Board of Management
Audit Committee

Date: 1 October 2019 **Time: 2 pm** **Room: 1074b**

AGENDA

				Presented by
1		Welcome and Apologies		HC
2		Declaration of Interest		HC
3		Minute of Meeting of 21 May 2019	(attached)	HC
4		Matters Arising not on the Agenda		
	4.1	Board Toolkit, from the National Cyber Security Centre	(attached)	AG
	4.2	Audit Committee Membership	(verbal)	HC
5		Audit Committee Evaluation	(verbal)	AW/HC
6		Internal Audit Plan – discussion and draft	(attached)	HC
7		*Internal Audit Reports		
	7.1	Internal Audit Annual Report	(attached)	PC
	7.2	Action Tracking Spreadsheet	(attached)	KH
8		Audit Scotland Reports		
	8.1	Scotland's Colleges 2019	(attached)	KH
	8.2	Fraud & irregularity update 2018-19	(attached)	KH
	8.3	Good Practice Note- Improving the Quality of Annual Reports and Accounts	(attached)	KH
	8.4	Technical Bulletin 2019-2	(attached)	KH
9		2018-19 Draft Audit Committee Annual Report	(attached)	HC/KH
10		Cyber-Security – update report	(attached)	AG
11		Strategic Risk Register	(attached)	JC
12		Any Other Business		
13		Date and Time of Next Meeting – Tuesday, 12 November 2019 at 2pm		
14		Good Governance - Annual discussion with internal auditors without members of college staff		HC

*Individual Internal audit reports are not published on the website; they are included in the published annual internal audit report

Board of Management-Audit Committee

Minute of the Meeting of the Audit Committee of the Board of Management of Dumfries and Galloway College held on 1 October 2019 at 2 pm in Room 1074b

Present:	Hugh Carr (Chair) Pat Kirby	Robbie Thomas (via skype) Naomi Johnson
In attendance:	Joanna Campbell (Principal) Karen Hunter (Head of Finance) David Eardley (Scott Moncrieff) Brian Johnstone (Regional Chair)	Andy Glen (Vice Principal) Ann Walsh (Board Secretary) Philip Church (RSM)
Minute Taker	Heather Tinning (Executive Assistant)	

1 Welcome and Apologies

The Chair welcomed all to the meeting. Apologies were received from Board Member Ros Francis, who planned to attend as an Observer, pending board approval to join the Audit Committee.

The Chair (Hugh Carr) advised that he was unable to stay for the full meeting and asked that Naomi Johnson chair the rest of the meeting after he leaves. This was agreed.

The Board Secretary confirmed the meeting was quorate.

NOTE: It was agreed to revise the order of the agenda, as noted within the table below - Hugh Carr leaving after item number 10 of the revised order, Internal Audit Plan. Naomi Johnson took over as Chair for this meeting from item number 11 of the revised order, Draft Audit Committee Report. To enable easy access to the committee papers, using the item numbers assigned to them, the minute is recorded in the order of the original agenda.

Revised Order of the Agenda	Original Agenda	
1	1	Apologies
2	2	Declaration of Interest
3	3	Minutes of the last meeting
4	4	Matters Arising
5	5	Audit committee evaluation
6	4.2	Audit committee membership
7	11	Strategic Risk Register
8	7, 14	Internal Audit annual report, with Good Governance discussion
9	7.2	Action tracking
10	6	Internal Audit plan
11	9	Draft Audit Committee Report
12	10	Cyber security update
13	4.1	NCSC toolkit
14	8	Audit Scotland reports (4)
15	12	AOCB

2 Declaration of Interest

Members agreed to indicate declarations of interest as appropriate throughout the meeting.

3 Minute of Meeting of 21 May 2019

The Minute of the meeting of 21 May 2019 was approved, with one minor amendment:

> **8 Audit Committee Membership**
>
> (Should read) with a quorate of three

4 Matter Arising not on the Agenda

4.1 Board Toolkit, from the National Cyber Security Centre

The Vice Principal Business Development & Corporate Services advised that the Cyber Security Toolkit for Boards report had been issued for information.

4.2 Audit Committee Membership

The Audit Committee membership currently consists of four members, with the aim to increase to six members. One additional member is being proposed for approval at the next Board meeting, Discussion followed regarding how to ensure a sufficient number of members for each committee and attendance at meetings

Action: Request for Members to come forward to join the Audit Committee to be taken to the Board Meeting on 8 October 2019

4.3 Strategic Risk Register

As curriculum development planning for the SoSEP Project is monitored through the Learning & Teaching Committee it was agreed to add the L&T Committee as having oversight of Risk Number 3.11.

Action: The Principal will amend the Risk Register as agreed

5 Audit Committee Evaluation

The Board Secretary reported that she had received returns from committee members. She gave early feedback that generally the feedback was positive. There were some areas where Board Members are unsure of the answers to some of the questions and feedback that the committee can only be as good as the information given, raising the issue of having timely and appropriate communication. The Board Secretary reported on the next steps, advising that she will collate the information and develop proposals recommendations from the findings. This to be presented at the next meeting and agreed actions will be included in the Board Development Plan

Action: The Board Secretary to produce a report for the next Audit Committee meeting

6 Internal Audit Plan 2019-20 – discussion and draft

Philip Church, Internal Auditor, spoke to the draft Internal Audit Strategy 2019/2022 which had been issued, advising that a meeting had taken place with the Principal and Head of Finance to develop the Internal Audit Plan for 2019-20. Members discussed the Audit Plan and PC's question to the committee asking if the areas proposed were appropriate.

During discussion Members asked for the plan to include an audit on specific financial processes and procedures to provide assurance that these are being managed and adhered to and also to provide an audit on governance. Changes agreed to the draft plan are as follows:

- Revised audit plan to include an audit of Petty cash, to also cover expenses, claims and payments. To check that controls are adequate and that the controls are being adhered to. This audit will be included within the currently planned Key Financial Controls Audit.

- To include a Governance Review - The scope of works will be issued and approved by the Audit Committee in November 2019. The Governance Review will replace the proposed audit of Marketing. The Principal was comfortable with this as there is a current review taking place.

David Eardley, External Auditor advised that there is already a process in place for reviewing and evaluating board effectiveness and governance and raised the question of value for money of this audit. The Board secretary advised that the next external review of Board Effectiveness is due in 2020. Philip Church, Internal Auditor will take account of the current process and content in place for reviewing and evaluating board effectiveness and governance when scoping the governance audit.

Actions:

- RSM to issue revised plan for members' comments.
- Revised plan to be approved by committee members via email, by the morning of Friday 4 October
- Approved revised plan to be issued to Board Members for the Board of Management meeting on 8 October 2019
- RSM to provide the proposed scope of work for the governance audit – to be discussed at the next audit committee meeting – November 2019.

Members approved the Internal Audit Strategy 2019/2022 which includes the Internal Audit Plan 2019-20, subject to the changes agreed. The revised document to be seen and approved by the committee.

7 Internal Audit Reports

7.1 Internal Audit Report

Philip Church spoke to the report, which provides an annual opinion based on work undertaken 2018-19. Philip advised that in terms of Risk Management the college received a positive assurance. The audit opinion is that the College has an adequate and effective framework for risk management, internal control and economy, efficiency and effectiveness. In terms of the six audits undertaken of the Control environment four reasonable and two substantial opinions were identified.

Members noted the report, and the reasonable assurance identified for the college.

7.2 Action Tracking Spreadsheet

The Head of Finance spoke to the Action Tracking Spreadsheet, reporting that the summary at the top of the spreadsheet should read that two are still in progress with sixteen completed. The Employer Engagement Strategy will be reported on at the next meeting. Pat Kirby confirmed that although the Strategy had been approved at the L&T Committee, it is being updated.

The Head of Finance reported that risk 4 is still in progress, with the delay in upgrading the virtual machines to Windows 10. The VP Business Development & Corporate Services confirmed that where there is a need for training identified by staff this will be progressed by the E Learning Manager.

All other recommendations are fully implemented.

Members noted the progress on the Action Tracking Spreadsheet.

8 Audit Scotland Reports

8.1 Scotland's Colleges 2019

Members discussed the report which had been issued. The Head of Finance reported on discussions at a recent Finance Network. She advised that each college has to give a clear instruction on how to address a deficit going forward. The Head of Finance has also been linking in with colleagues across the sector in terms of best practice. The FFR should be signed off in the next week or so. The Principal advised that the Transformation Plan will be brought to the Board to ensure that the college is addressing a deficit. The outline of the Transformation Plan will be discussed at the Board Strategy day on 29th October 2019.

The Principal reported that in terms of attainment, the college is 1% higher than last year on retention.

Members noted the report.

8.2 Fraud & Irregularity Update 2018-19
Members noted the Fraud & Irregularity Update 2018-19 report, issued to members for information.

8.3 Good Practice Note – Improving the Quality of Annual Reports and Accounts
Members noted the Good Practice Note – Improving the Quality of Annual Reports and Accounts, issued to members for information.

8.4 Technical Bulletin 2019-2
Members noted the Technical Bulletin 2019-2 report, issued to members for information.

9 2018-19 Draft Audit Committee Annual Report
The Chair (NJ) spoke to the Draft Audit Committee Annual Report for 2018-19 which had been issued.

Members discussed and agreed the following amendments:
- Section 3.4 – amend meeting date to 13.11.2018
- Include positive statements confirming that the committee are content that good governance is in place and being adhered to
- Section 8.2 – revise wording accordingly, in terms of materiality and proportionality

Action: The Head of Finance to revise the Draft Audit Committee Annual Report 2018-19 to bring back to the Audit Committee meeting in November 2019

Members noted the work of the Committee for period August 2018 to July 2019.

10 Cyber-Security – update report
The Vice Principal Business Development and Corporate Services spoke to the report which had been issued, providing members with an update on Cyber Security.

The VP reported that the college is applying for their second Cyber Security certificate by 31st October 2019. Cyber Security plus requires more working with the Central Information Services and will require more spend on infrastructure. All colleges are facing challenges around their ICT estate. The Principal advised that a review exercise is taking place, led by the Principal of Forth Valley College who is looking at types of technology for a progressive learning and teaching environment. The college is at risk of an ageing IT asset, impacting on what the college can deliver.

Members discussed their concerns over security of emails received and Board papers issued. Board Members were re-assured that using the Admincontrol programme to access Board Papers, was secure, with individual username and passwords, which also adheres to GDPR. As part of induction, new members undertake General Data Protection Regulations (GDPR) training. Board members should be using Admincontrol as this complies with Cyber Security and GDPR.

Members noted the report.

Action: The Vice Principal to progress key points for Board Members on basic ICT security principles for the next Audit Committee meeting

11 Strategic Risk Register
The Principal spoke to the Strategic Risk Register, reporting on the risks pertinent to the Audit Committee. The Risk Register has been updated to incorporate revised role titles and ownership.

With reference to risk 2.4 (Financial Fraud), in response to the recent Fraud element, the Vice Principal confirmed that robust controls are now in place. The Head of Finance has progressed increased Financial controls, in terms of processes and duplicate signatures. Internal Hospitality budgets are now authorised solely by designated budget holders

Actions:

- The Principal to amend Risk 2.4 to read "Public Interest Disclosure (Whistleblowing) Policy"
- The Principal to amend Risk 3.11 to include the L&T Committee in the Committee Oversight column

Members approved the Strategic Risk Register, subject to the amendments noted

12 Any other business
None.

13 Date and time of Next Meeting
The next meeting of the Audit committee is to take place on Tuesday 12 November 2019 at 2 pm.

14 Good Governance – Annual discussion with internal auditors without members of college staff
The Chair brought this confidential agenda item forward so that it could be held before he needed to leave the meeting, for discussion with the Auditors, asking that the college staff leave the meeting at this point.

The Chair invited Philip Church (Internal Auditor, RSM) and David Eardley (External Auditor, Scott-Moncrieff) to feedback to the committee on any issues or concerns they wished to draw to the committee's attention.

Philip spoke positively of the relationship between Internal Audit and Management and stated there were no issues or concerns to report to the committee. He had regular meetings and stated that engagement was very positive with all recommendations accepted and acted upon. He had met with the Principal and all information required by him was provided in a timely manner. Two of this year's internal audits had already been undertaken.

David reported that this was the second day of the final audit visit. He stated that he had been provided with excellent working papers and the team were available. He informed the committee that the early indications were good.

There was some discussion regarding the fraud issue over the summer and it was proposed that an audit to review controls should be undertaken. This to be discussed under the Internal Audit Plan agenda item.

(The college staff were invited to return to the meeting)

Board of Management-Audit Committee

Minute of the Meeting of the Audit Committee of the Board of Management of Dumfries and Galloway College held on 21 May 2019 at 2 pm in Room 2009

Present:	Hugh Carr (Chair) Pat Kirby	Robbie Thomas (via Facetime)
In attendance:	Andy Glen (Acting Principal) Karen Hunter, Head of Finance Rob Barnett (RSM)	David Eardley (Scott-Moncrieff) Ann Walsh (Board Secretary)
Minute Taker	Heather Tinning (Executive Assistant)	

1 Welcome and Apologies

The Chair welcomed all to the meeting. Apologies for absence were intimated on behalf of Naomi Johnson.

The Board Secretary confirmed the meeting was quorate.

2 Declaration of Interest

Members agreed to indicate declarations of interest as appropriate throughout the meeting.

3 Minute of Meeting of 19 February 2019

The Minute of the meeting of 19 February 2019 was approved.

4 Matter Arising not on the Agenda

4.1 Check to see if the security camera is connected to the college internet system

The Acting Principal confirmed that the security camera is not directly connected to the college internet system, however the security camera is linked to two named individuals within the organisation who have access to the camera.

4.2 Feedback request re: External Audit – completion of questionnaire

The Head of Finance reported on positive feedback from Audit Scotland.

4.3 Board Toolkit, from the National Cyber Security Centre

Following discussions, the Board Secretary suggested that the Acting Principal arrange for completion of the Board toolkit and feedback to the Board Members at the next Audit Committee meeting. The Acting Principal agreed that the ICT department would consider the answers to the questions and offer guidance to the Board on where they will find answers.

The Board toolkit consists of a range of questions that the National Cyber Security Centre believe will help generate constructive cyber security discussions between board members and their CISOs.
Action: The Acting Principal to bring back a brief report from the ICT department to the next Audit Committee

5 Internal Audit Contract – Tender Update

The Head of Finance provided a summary of the recent tender exercise for the College Internal Audit Contract. The advertisement was published on the Quick Quotes Hub using the APUC framework for internal audit, with four suppliers submitting quotes:

- BDO
- RSM
- TIAA
- Wyllie & Bisset

The Head of Finance reported that there was a substantial difference in the prices. BDO and RSM provided excellent tenders, giving a lot of assurance from tenders and timing. Start date for the successful Company is the 1st August 2019. Both RSM and BDO gave assurance from information in tender, with positive method statements and reports from both. TIAA papers lacked a lot of detail, and not a lot of confidence from tender papers submitted. Although a good tender had been received from Wyllie Bisset and they had addressed the questions, they had lacked detail in their response.

Price scoring tenders based on prices submitted using 3-year period price. Overall BDO and RSM received full marks for quality, however as BDO were such a high price, RSM received the best score. Members recommend awarding the contract to RSM as the Internal Auditors. RSM has been the college's Internal Auditors since 2009.

- BDO – 50 days quoted in tender
- RSM – 35 days quoted in tender

Decision: Members agreed to award a 3-year contract to RSM, where extension for another year will require a full change of personnel if an extension is exercised
Action: The Head of Finance to take forward

6 External Audit

6.1 External Audit Plan 2018-19

David Eardley (DE) spoke to the External Audit Plan 2018-19 which had been shared, advising that there were no main changes in the audit scope. The Plan before is similar to the structure content and focus to last year's plan. DE highlighted the revenue recognition and how the college recognise expenditure identified in the report. Also identified in the report is the financial statements in relation to the estate work, which will cover all aspects of estates development in terms of income and expenditure. In relation to financial sustainability GDPR is not included in the document, as this is not necessarily a financial risk.

Members noted a proposed Audit fee for 2018/19 of £17,410. Ongoing costs around £12m for financial sustainability, which was highlighted as one of the risks in the report. The Head of Finance confirmed 3% would provide the overall savings target.

The Head of Finance confirmed that Scott Moncrieff are the college's VAT advisor. Scott Moncrieff will be joining with Campbell Dallas as part of CogitalGroup. DE confirmed that there is no change to current terms and conditions and fees.

In terms of the SoSEP Project, DE advised that discussions will take place with the Head of Finance and the Team around October with regard to the Project, to look at the situation from 31 July onwards.
Action: The Head of Finance to forward documentation providing details of merger to Audit Committee members

Members approved the External Audit Plan 2018-19

7 Financial Regulations Update

The Head of Finance spoke to the report which had been issued, which provided a brief overview of the Financial Regulations.

The information is the same in terms of link to strategic objectives, incorporating internal audit recommendations. The draft Financial Regulations include examples of staff responsibilities, which were not included in the previous regulations. The Head of Finance reported that all Purchase Orders go through the Internal System. She advised that the college is looking to improve their internal processes and to reinforce this with staff to ensure that they comply with the processes.

Action: Members approved the draft Financial Regulations after the following change:

- The Head of Finance to amend the wording of Whistle Blowing to read Public Interest Disclosure throughout the document

8 Audit Committee Membership

The Chair reported that there are currently four members on the Audit Committee, with a quorate of four. He advised that to date he had received no interest from other Board members to join the Audit Committee. The Chair reminded members that whilst seeking interest, members cannot sit on both the Audit and Finance & General Purposes Committee, as per the Terms of Reference.

Decision: Members agreed to increase the membership to six Audit Committee Members

Action: The Chair to take the discussion to the Board of Management meeting on 4th June with regard to seeking a further two members for the Audit Committee and for approval by the Board

9 Internal Audit Reports

9.1 Action Tracking Spreadsheet

The Head of Finance reported that the Action Tracking Spreadsheet is presented and discussed at the monthly College Leadership Team meeting, when CLT report on their outstanding actions. The Head of Finance provided an update for the Committee, advising that recommendations will be taken into account when completing the next forecasting exercise:

- Ref 1 – Employment Engagement Strategy: The Strategy has been approved at the last Learning and Teaching Committee subject to benchmarking criteria, currently awaiting milestones
- Ref 3 – Induction Checklist: now available online, ready to roll out for induction
- Ref 4 – ICT: Windows 10 will be updated in all computers by the end of July
- Ref 12 – UWS Service Level Agreement: A Partnership Agreement has been drafted for discussion in terms of service delivery
- Ref 13 and 15 – Financial Regulations: To be revised and included on the system

Members noted the progress on the Action Tracking Spreadsheet.

9.2 Progress Report

Rob Barnett (RB) reported that the Progress Report has been presented to provide an update to the Committee against the 2018/19 Internal Audit Plan, which was approved by the Audit Committee on 17 May 2018. Members noted that four reports have been finalised since the last Committee, two with substantial assurances and one amber reasonable assurance. A reasonable progress was issued for the Follow up of Previous Internal Audit Management Actions. RB advised that the KPIs demonstrate the targets agreed at the start of year.

Members noted the Progress Report.

9.3 Equality and Diversity
Rob Barnett reported on a Substantial Assurance given as the Internal Audit Opinion. Within the detailed findings one medium and two low actions had been identified relating to the Equality and Impact Assessment. The Equality Impact Assessment had not been formed, however this has now been addressed and a suitable action plan is now in place. Overall there is a strong control framework showing that the controls are in place, an Equality and Diversity Policy is in place, together with an Equality and Diversity Framework. An Equality and Diversity Update had been provided at the recent HR Committee (12 February 2019) including a summary of progress against last year's action plan and a proposal of action plan for the coming year. RB advised that RSM will follow this up at their next visit.

Members noted the Progress Report.

9.4 Financial Planning and Forecasting
RB spoke to the Financial Planning and Forecasting reporting that two medium action points had been agreed with Management. RB reported on greater sensitive analysis needed around forecasting, and the need to get into Income and Expenditure variables. Rob suggested that in terms of testing, the college look at more variables. RB advised that some risks on the FFR did not have mitigating actions and reported from the Management Actions mitigating controls are now in place.

Members noted overall a good strong positive audit report.

9.5 Key Financial Controls – Creditors
RB reported that each year the Auditors review a different financial area. This year a Creditor Review was undertaken. Four medium and two low priority actions were identified. Medium Actions identified include:

- Financial Regulations – some missing information, out of date information
- Purchase Orders not consistently raised, 60% not been raised for orders placed, missing signatures
- Raised opportunities to strengthen cash advance process, to provide greater effort to recoup money. Actions have been taken to address this
- Weakness around completion including lack of details on forms and again missing Budget holder's signatures

The Head of Finance reported that the Finance Team are re-enforcing procedures with Budget holders and are tightening up on cash advances, including extra checking in place with the use of Credit Cards. She advised that there are two Credit Cards in use in the college, Human Resources and Finance. Managers have been undertaking Finance Training, and meetings are ongoing with regards Zero Based budgets moving forward.

Members noted the Creditor Payments Report

9.6 Follow-Up of Previous Management Actions
RB reported that from the thirteen medium actions, overall seven were implemented, with implementation ongoing for five. He advised that there is a revised action plan in place. One action

has been superseded. Members noted no great concern for the ongoing actions, where there are revised implementation dates in place.

Members noted reasonable progress for implementing agreed management actions.

9.7 Internal Audit Plan – draft

The Head of Finance spoke to the report which had been issued, seeking members approval for the initial works to be carried out early in the new Academic Year. RB spoke to the Internal Audit Strategy covering period 2018 – 2021. Following discussion on the Internal Audit Strategy for 2018/2021, with regard to a full audit needs assessment, this would be reviewed at a later date once the full Internal Auditor was in place. The Acting Principal confirmed that the Student Activity Data, detailed in the report as SUMs, is now measured in Credits. Following a question in relation to Appendix B and Core Assurance, the Acting Principal confirmed that the Curriculum Planning which will be looked at again in 20/21 is an annual ongoing process.

Members considered the outline for the 2019-20 Internal Audit and approved the Student Support Funds and Student Activity Data Reviews.

- Members noted that Individual reports are not published on the website; they are included in the published annual internal audit report

10 Strategic Risk Register

The Acting Principal spoke to the Strategic Risk Register, reporting on the risks pertinent to the Audit Committee, advising that there have been no changes to the four risks identified:

- Risk 2.4 – Financial Fraud
- Risk 3.6 – Failure to achieve ICT Strategy Ambitions
- Risk 3.8 – Breach of data security
- Risk 3.10 – Failure to meet compliance agreements

In answer to a question, the Acting Principal advised that the Strategic Risk Register is discussed at the monthly College Leadership Team meetings and regularly with the Executive Leadership Team. Members were assured that the Management Team were looking at the risks regularly.

Members approved the Strategic Risk Register, with no changes.

11 Audit Committee Evaluation

The Board Secretary reported on an Audit Committee Self-Assessment Checklist with regard to Audit Committee Training. It was also suggested to use as a part of Board Evaluation

Action: The Board Secretary to send information to Audit Committee members regarding the online training

12 Any other business

None.

13 Date and time of Next Meeting

The next meeting of the Audit committee is to take place on Tuesday 10 September 2019 at 2 pm.

National Cyber
Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Helping board members to get to grips with cyber security

Contents

Introduction

The vast majority of organisations in the UK rely on digital technology to function.

Good cyber security protects that ability to function, and ensures organisations can exploit the opportunities that technology brings. Cyber security is therefore central to an organisation's health and resilience, and this places it firmly within the responsibility of the Board.

New regulations (such as GDPR) as well as high profile media coverage on the impact of cyber incidents, have raised the expectations of partners, shareholders, customers and the wider public. Quite simply, organisations - and Board members especially - have to get to grips with cyber security.

Why have the NCSC produced a Cyber Security Toolkit for Boards?

Boards are pivotal in improving the cyber security of their organisations. **The Cyber Security Toolkit for Boards has been created to encourage essential discussions about cyber security to take place between the Board and their technical experts**.

What can this toolkit do for you?

Board members don't need to be technical experts, but they need to know enough about cyber security to be able to have a fluent conversation with their experts, and understand the right questions to ask.

The Cyber Security Toolkit or Boards therefore provides:

1. A general introduction to cyber security.
2. Separate sections, each dealing with an important aspect of cyber security. For each aspect, we will:
   - explain what it is, and why it's important
   - recommend what individual Board members should be doing
   - recommend what the Board should be ensuring your organisation is doing
   - provide questions and answers which you can use to start crucial discussions with your cyber security experts
3. Appendices summarising the legal and regulatory aspects of cyber security.

Getting started

Don't feel obliged to read the Cyber Security Toolkit in a single sitting. Think of it less of a manual to be read cover-to-cover, but more of a resource to be used to help you develop your own cyber security board strategy; one that can adapt to fit your own unique cultures and business priorities.

If you're not sure where to begin, we suggest you start with the Introduction to Cyber Security for Board members and Embedding cyber security into your structure and objectives.

About the Cyber Security Toolkit

The Cyber Security Toolkit is relevant for anyone who is accountable for an organisation in any sector. That could be a Board of Directors, a Board of Governors or a Board of Trustees. Additionally, technical staff and security practitioners may find it a useful summary of NCSC guidance, and can use the questions within the toolkit to frame discussions with the Board.

Cyber Security Toolkit: scope and structure

Good cyber security is all about managing risks. The process for improving and governing cyber security will be similar to the process you use for other organisational risks. It is a continuous, iterative process and comprises three overlapping components, summarised below:

1. Get the information you need to make well informed decisions on the risks you face.
2. Use this information to understand and prioritise your risks.
3. Take steps to manage those risks.

Crucially in order for these steps to be effective, you need to get the environment right, so we've included three sections that explain how to do this. The full structure of the Cyber Security Toolkit is summarised in the table below - click on a link to jump to the relevant section.

<table>
<tr><td colspan="3"><b>Getting the environment right</b>
Embedding cyber security in your organisation
Growing cyber security expertise
Developing a positive cyber security culture</td></tr>
<tr><td><b>1. Get the information you need to make well informed decisions on the risks you face.</b>
Establishing your baseline and identifying what you care about most
Understanding the cyber security threat</td><td><b>2. Use this information to evaluate and prioritise your risks.</b>
Risk management for cyber security</td><td><b>3. Take steps to manage those risks.</b>
Implementing effective cyber security measures
Collaborating with suppliers and partners
Planning your response to cyber incidents</td></tr>
</table>

Note: You will be familiar with this type of process, and may have your own approach to managing risk within your organisation. The Cyber Security Toolkit therefore focuses on the aspects of the process that are unique to cyber security and need additional consideration.

How to use the Cyber Security Toolkit

The NCSC is often asked 'what does good look like?' The simple answer is 'whatever protects the things you care about'. This means that, whilst there is some good practice that applies in most situations, 'good' cyber security for one organisation may not be 'good' for another. 'Good' cyber security has to work for you; it has to be appropriate to your systems, your processes, your staff, your culture and, critically, has to be appropriate for the level of risk you are willing to accept.

Each section within the toolkit addresses three questions:

1. **What should the Board do?**

   This provides specific actions for the Board.

2. **What should your organisation do?**

   This provides information on aspects that Boards should have oversight of but are unlikely to be actively taking action on (though this is dependent on your organisational structure).

3. **What does good look like?**

   This provides questions (and potential answers) designed to generate discussions with your experts that can help the Board identify what constitutes 'good' cyber security within your organisation. The questions are only the start of the story; you may find that simply getting the right people in the room, engaged in meaningful discussions, can throw a light on what works (and doesn't work) within your organisation.

How we built the Cyber Security Toolkit

This toolkit was created by:

- listening to what Boards have told us they want to know
- applying the NCSC's unique insights into cyber security, and how attacks happen

How you can help

We want to keep adding to this toolkit as you encounter new cyber security challenges, so we'll need your practical experiences of the challenges and opportunities you encounter. Please let us know how this toolkit could be improved, what you liked (or didn't like), and suggestions for what could be added next. You can use the contact us form or email us directly at enquiries@ncsc.gov.uk .

Introduction to cyber security for Board members

What is cyber security?

Cyber Security is the protection of devices, services and networks - and the information on them - from theft or damage via electronic means.

What do I need to know about cyber security?

There are three common myths concerning cyber security. Understanding why they're incorrect will help you understand some key aspects of cyber security.

Myth #1: Cyber is complex, I won't understand it.

Reality: You don't need to be a technical expert to make an informed cyber security decision.

We all make security decisions every day (whether to put the alarm on, for example) without necessarily knowing how the alarm works. Boards regularly make financial or risk decisions without needing to know the details of every account or invoice. The Board should rely on its cyber security experts to provide insight, so that the Board can make informed decisions about cyber security.

Myth #2: Cyber attacks are sophisticated, I can't do anything to stop them.

Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to your organisation.

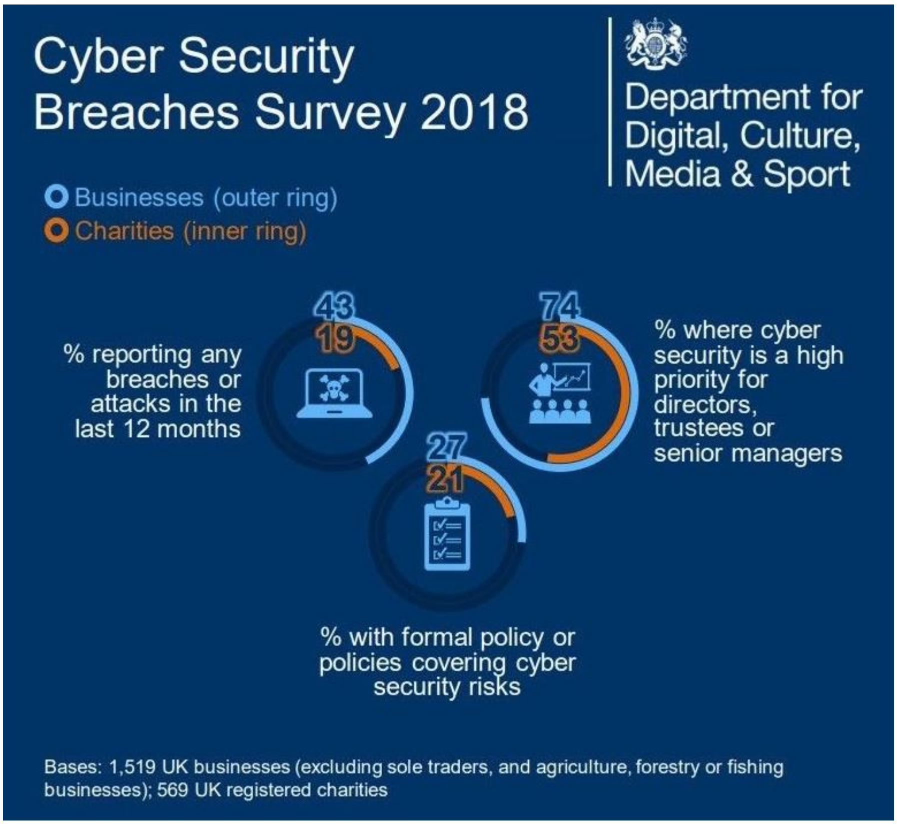
The vast majority of attacks are still based upon well known techniques (such as phishing emails) which can be defended against. Some threats can be very sophisticated, using advanced methods to break into extremely well defended networks, but we normally only see that level of commitment and expertise in attacks by nation states. Most organisations are unlikely to be a target for a sustained effort of this type, and even those that are will find that even the most sophisticated attacker will start with the simplest and cheapest option, so as not to expose their advanced methods.

Myth #3: Cyber attacks are targeted, I'm not at risk.

Reality: Many cyber attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

The majority of cyber attacks are untargeted and opportunistic in nature, with the attacker hoping to take advantage of a weakness (or vulnerability) in a system, without any regard for who that system belongs to. These can be just as damaging as targeted attacks; the impact of WannaCry on global organisations - from shipping to the NHS - being a good example. If you’re connected to the internet then you are exposed to this risk. This trend of untargeted attacks is unlikely to change because every organisation - including yours - will have value to an attacker, even if that is simply the money you might pay in a ransomware attack.

The findings from the Cyber Security Breaches Survey below show just how many organisations are coming under cyber attack and how organisations are responding to this risk. Further information is provided in the full report.



Cyber Security Breaches Survey 2018

Department for Digital, Culture, Media & Sport

Bases: 1,519 UK businesses (excluding sole traders, and agriculture, forestry or fishing businesses); 569 UK registered charities

How do cyber attacks work?

A good way to increase your understanding of cyber security is to review examples of how cyber attacks work, and what actions organisations take to mitigate them. Reviewing incidents that have occurred within your organisation is a good place to start.

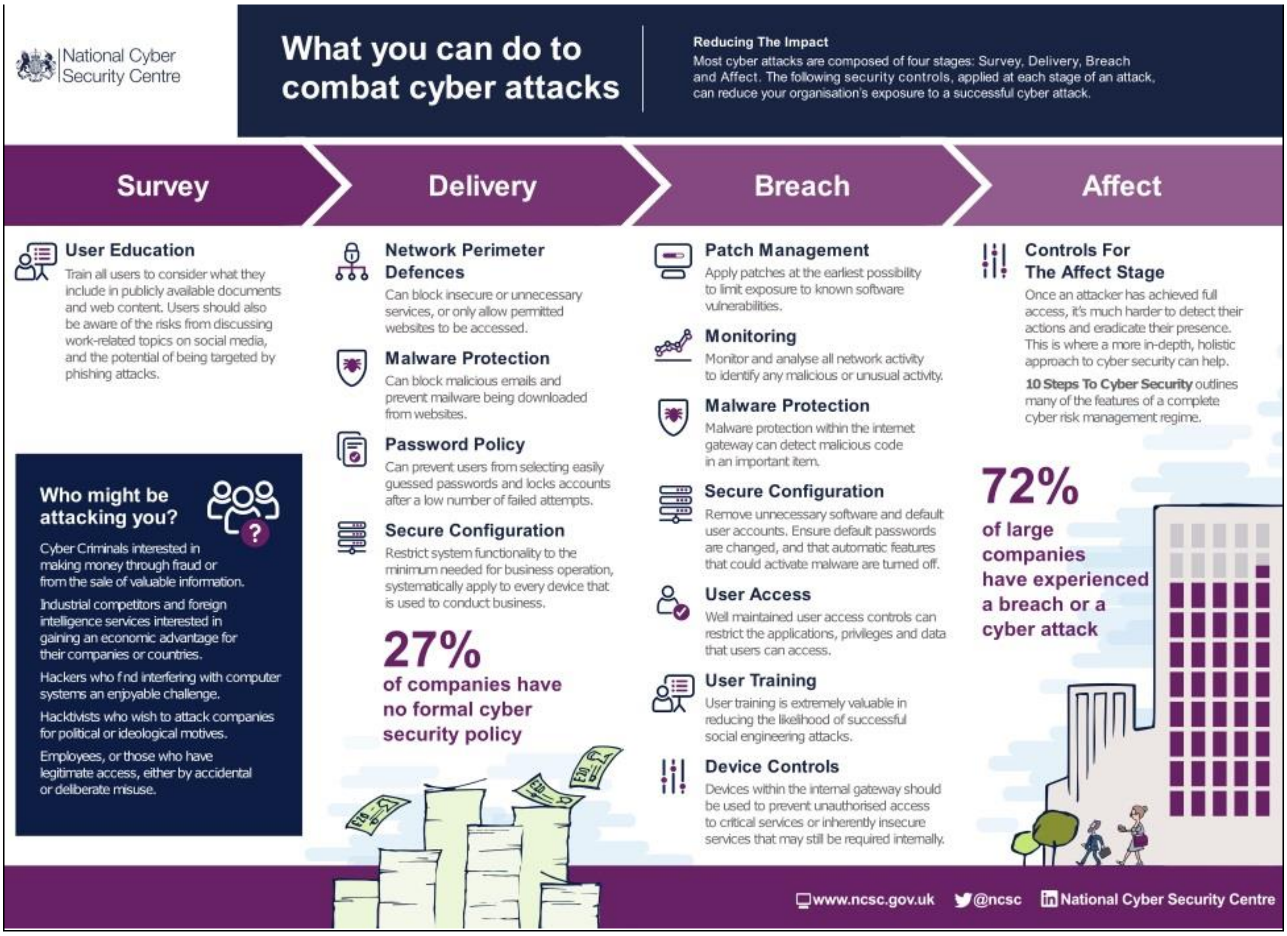
In general, cyber attacks have 4 stages:

- **Survey** - investigating and analysing available information about the target in order to identify potential vulnerabilities.
- **Delivery** - getting to the point in a system where you have an initial foothold in the system.
- **Breach** - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.
- **Affect** - carrying out activities within a system that achieve the attacker’s goal.

Defending against cyber attacks

The key thing to understand about cyber security defences is that they need to be layered and include a range of measures, from technology solutions to user education to effective policies. The infographic below gives examples of defences that will help your organisation to combat common cyber attacks. Our section on Implementing effective cyber security measures provides further detail and questions that you can use to understand more about your own organisation's defences.

The following infographic summarises the security controls you can apply to reduce your organisation’s exposure to a successful cyber attack.



National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact
Most cyber attacks are composed of four stages: Survey, Delivery, Breach and Affect. The following security controls, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education
Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences
Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection
Can block malicious emails and prevent mailware being downloaded from websites.

Password Policy
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration
Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

27%
of companies have no formal cyber security policy

Breach

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

Controls For The Affect Stage
Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

72%
of large companies have experienced a breach or a cyber attack

www.ncsc.gov.uk @ncsc National Cyber Security Centre

As a Board member, you will be targeted

Senior executives or stakeholders in organisations are often the target of cyber attack, because of their access to valuable assets (usually money and information) and also their influence within the organisation.

Attackers may try and directly target your IT accounts, or they may try and impersonate you by using a convincing looking fake email address, as the NCSC’s Technical Director found out. Once they have the ability to impersonate you, a typical next step is to send requests to transfer money that may not follow due process. These attacks are low cost and often successful as they exploit the reluctance of staff to challenge a non-standard request from someone higher up in the organisation.

Good cyber security awareness throughout your organisation, security policies that are fit for purpose and easy reporting processes will all help to mitigate this risk. It is also critical that Board members understand and follow their organisation's security policies, so that when an impersonator tries to circumvent them, staff can identify that something is unusual.

You should also consider how information about you (that is publicly available) could assist an attacker who is trying to impersonate you.

What support can the NCSC provide on cyber security?

The NCSC is the UK government's technical authority and therefore takes the lead role in providing guidance and advice on cyber security for UK organisations. The NCSC:

- understands cyber security, and distils this knowledge into practical guidance that we make available to all
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK
- uses industry and academic expertise to nurture the UK's cyber security capability
- helps organisations navigate the cyber security marketplace
- reduces risks to the UK by providing sector-specific guidance and engagement for public and private sector organisations

If you want to find out more about how you can work with the NCSC, please get in touch via enquiries@ncsc.gov.uk .

There is also government support on cyber security available from:

- Centre for Protection of National Infrastructure (CPNI) - provides advice on a range of security matters. Start with: Passport to Good Security for Senior Executives
- Department for Digital, Culture, Media and Sport (DCMS) - provides insight into the state of cyber security within the UK. Start with: FTSE350 Cyber Governance Healthcheck and the Cyber Security Breaches Survey
- National Cyber Crime Unit (NCCU) - part of the National Crime Agency and leads on investigating and prosecuting cyber crime. Start with: Cyber Threat to UK Business.

Embedding cyber security into your structure and objectives

The role of cyber security is to enable the organisation's objectives and, increasingly, enable competitive advantage. It should be adding value to your organisation rather than hindering progress. This requires a positive cyber security culture and appropriate investment and management of cyber security.

What should the Board do?

Integrate cyber security into your organisation's objectives and risks

There are two reasons why this is so important.

Firstly, cyber security impacts on every aspect of your organisation. Therefore to manage it properly it must be integrated into organisational risk management and decision making. For example:

- Operational risk will likely be underpinned by cyber security because of the reliance on the security of digital services that you use (email services, bespoke software, etc).
- Some legal risk will be tied in with cyber security risk (such as contractual requirements to protect data or partnerships, regulatory requirements to handle data in particular ways).
- Financial risk is impacted by cyber security (such as money lost through fraud enabled by cyber, revenue lost when services are taken offline by cyber attack).
- Good cyber security will also allow you to take some risk in using new technology to innovate. An overly cautious approach to risk can lead to missed business opportunities or additional (and unnecessary) costs.

Secondly, cyber security needs to be integrated for it to be successful. Good cyber security isn't just about having good technology, it's about people having a good relationship with security, and having the right processes in place across the organisation to manage it.

For example, in order to protect against an attacker accessing sensitive data (whilst ensuring that only those with a current and valid requirement can see it), you will need:

- a good technical solution to storing the data
- appropriate training for staff handling the data
- a process around managing the movement of staff, aligned with access management

Reflect this in your structure

Don't leave it to one person; Cyber security is the responsibility of the entire Board.

A cyber security incident will affect the whole organisation - not just the IT department. For example, it may impact on online sales, impact on contractual relationships or result in legal or regulatory action. There should be sufficient expertise within the Board in order to provide direction on cyber security strategy and hold decisions to account. However every member of the Board needs enough expertise to understand how it impacts specifically upon their area of focus, and to understand the broad implications for the organisation as a whole.

> **Cyber security outside the UK**: When trying to understand the impact of cyber security on your organisation and your risks, an important consideration is which countries your organisation operates in. For those organisations who operate outside the UK or have partners outside the UK, the CPNI Smart Business Guidance highlights how this may impact your security considerations, including your cyber security. The Collaborating with suppliers and partners section of this toolkit provides guidance on how to mitigate the cyber security risk associated with these relationships.

Engage with your experts

Consider whether your reporting structure enables the Board to have the engagement with cyber security that it needs. If the CISO reports to an intermediary to the Board who has a focus on only one aspect - be that finance or legal or technology - this can potentially hinder the ability for the Board to see cyber security's wider implications. In the majority of FTSE350 organisations the CISO now reports directly to the Board.

A good place to start on improving cyber security in your organisation is to consider the communication between experts and members of the Board. Getting the structure right can help, but we also often see a reluctance from both parties to engage, because:

- technical staff think that the Board won't understand them
- the Board think that the technical staff are unable to explain the issues in the context of the strategic aims of the organisation

Improving the communication between these two groups requires effort from both sides:

- **Boards** need a good enough understanding of cyber security that they can understand how cyber security supports their overall organisational objectives
- **technical staff** need to appreciate that communication of cyber risk is a core component of their job, and ensure they understand their role in contributing to the organisation's objectives

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **embedding cyber security into your structure and objectives**.

Q1. As a Board, do we understand how cyber security impacts upon our individual and collective responsibilities?

You might want to consider:

- Does every Board member have enough expertise to understand the potential impact and value of cyber security?
- Is there someone responsible for delivering the organisation's cyber security?
- Who is responsible for oversight of cyber security?
- Have we been clear about what information both the Board and our wider stakeholders need?

Q2. As an organisation, who currently has responsibility for cyber security?

This could be a person or a function, e.g. an audit committee. You might want to consider:

- How they engage with the Board - do they report directly to the Board or do they fit into another reporting process? Does this encourage the Board to actively participate in discussions on cyber security?
- What their objectives are and who sets them - do these objectives drive cyber security to be an enabler for the organisation?
- Do they have access to all the people they need to ensure effective cyber security - this could be just in terms of the resource required to meet your cyber security objectives, but could also be the teams that they need to be linked in with e.g. HR, policy, finance.

Q3. As a Board, how do we assure ourselves that our organisation's cyber security measures are effective?

You might want assurance that:

- The organisation is employing an appropriate suite of technical assurance activities and the output of this is conveyed in a meaningful way to the Board. Assurance activities might include reviewing defensive measures against suitable frameworks, such as Cyber Essentials or 10 Steps to Cyber Security.
- Threat assessments and defensive priorities are regularly reviewed and defensive measures updated accordingly.
- The focus of your cyber security measures is aligned with the risks you have identified and prioritised.

Q4. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

An example of this would be where a risk from one part of the organisation has been balanced against another. For example, an organisation may assess that introducing a Bring Your Own Device (BYOD) policy brings substantial benefit to the organisation in terms of flexible working. As part of the case for change, including assessing the business risk of not implementing a BYOD model, you would also want to:

- Assess the increase in risk associated with the increased number of devices connected to your network.
- Assess the risk associated with not owning, and therefore not being in control of, devices connected to your network.
- Consciously balance the business risks and benefits with the technical risks and benefits of BYOD.
- Consider other models, such as Corporate Owned, Personally Enabled (COPE) and compare the risks and benefits.
- Assess the suitability of planned security measures to ensure that they support rather than constrain the aims of flexible working.
- In this example, the cyber risk of introducing the new service (BYOD) has been integrated into the business risk. Those who are accountable for a service should be receiving the best possible advice, so that they can clearly balance cyber risks with other risks (and benefits) in their decision making.

Growing cyber security expertise

Cyber skills are already in high demand, and the Global Information Security Workforce study estimates that by 2022 there will a shortfall of 350,000 appropriately trained and experienced individuals in Europe. Organisations must take steps now to ensure they can draw on cyber security expertise in the future.

What should the Board do?

Baseline your current skills

The Board should have an understanding of what cyber expertise there is in the organisation and what you need. Do you have a CISO? An information security team? Incident managers? If not, should you?

This information will give you an insight into the resilience of cyber security efforts (are you currently reliant on one person?) and also will help you to understand the provenance of the cyber security information you receive.

You might also want to consider the expertise on the Board itself. Do you currently have sufficient specialist knowledge to ensure that the Board is able to make appropriate strategic decisions about cyber security? Are you likely to be able to keep pace as advances in technology bring new security challenges?

What should your organisation do?

Make an organisational plan

Given the lack of suitably skilled individuals and an increasing reliance on digital services that need to be secured, organisations that do not embrace cyber security will soon fall behind.

1. Work out what specific cyber security expertise you need. 'Cyber security' covers a range of different skills, from network security to risk management to incident response. It may be useful to first consider what skills you need to manage your highest priority objectives or risks and then assess which (if any) of these you cannot outsource and so must have in house.
2. Establish how urgently you need these skills. If you are considering developing existing staff, don't underestimate what this entails. Putting someone through a training course does not make them a cyber security expert: they must also have the opportunity to develop hands-on, practical skills and so will require support for this from within the organisation. If you need expertise in the shorter-term, it might be better to recruit a consultant or specialist.
3. Consider how you might recognise professional cyber security skills. As yet, there is no professional body for cyber security expertise (although the NCSC is working on it). This could mean that validating the ability or quality of a new hire and/or developing training plans, is difficult. Consider how you might be able to work with trusted partners or industry specialists to give you the necessary assurance.

MAKE THE BEST USE OF THE SKILLS YOU HAVE

The best way to make use of the skills you have is to identify and focus on the things that are unique to you (or the things that only people within your organisation are most qualified to do). This can be enabled by making use of established, commodity technologies. For example, you might choose to allow cloud vendors to build and secure your infrastructure, which frees your experts to spend time exploiting the unique insight they have into your organisation.

Build your best workforce: equal, diverse and inclusive

Due to the cyber security skills shortfall, your organisation must draw and nurture talent from the largest possible pool. The cyber security industry is subject to the same skills challenges as all technology-focused industries. Organisations may find it hard to recruit and retain high-calibre staff from all demographic groups. In fact there are many talented women and minorities working in cyber security, but they are often less visible. They may experience hostile working environments that slow or stop their career, or avoid the industry altogether. Working together to overcome these challenges will give your organisation a competitive edge.

LOOK BEYOND TECHNICAL SKILLS

When designing job roles and desired candidate profiles, particularly at entry level, be imaginative. Protecting our organisations relies on bringing together many different skills, technical and non-technical, to deliver security that aligns with the organisation's objectives. Recruit for broader business skills, aspiration and potential as much as for current technical skills.

LOOK AFTER YOUR EXISTING TALENT

When trying to make our organisations more diverse and inclusive, we often focus on bringing in new talent, while ignoring the issues that prevent your current staff staying and thriving once they are in. The talent available may be beyond your own direct control, but you can control how much cyber security talent you lose because of difficult policies and processes, and unwelcoming workplace cultures. As much as strong security cultures, you should focus on fully inclusive workplace cultures.

Train, buy-in, or develop for the future

Broadly there are 3 options to increase cyber expertise within your organisation.

TRAIN EXISTING STAFF

Don't just consider the staff who are already in security-related jobs. The NCSC has had huge success training staff from a variety of backgrounds, skills and experience. After all, there are many different aspects to cyber security and someone who is expert at designing a network architecture might have a very different skill set to the person working with staff to make sure security policies are practical and effective.

Depending on your organisation's needs and your staff, training could take the form of on-the-job training, professional qualifications or placements. Do remember that developing cyber security expertise is no different to many other professional areas: staff will require continuous investment, training and development opportunities to hone their expertise and also to keep up with changes in the industry.

- There are many companies who offer cyber security training. NCSC provides a list of accredited training courses.
- You could also offer time for study on an NCSC certified degree, or time for a placement on the Industry100 programme.

BUY IN EXPERTISE

There are several complementary routes available for introducing external expertise. A large organisation will probably take advantage of all of them.

1. Recruit a skilled non-executive director to your Board.
2. Employ a consultant to provide specific cyber security advice.
3. Identify specific cyber security services which can be fulfilled by a 3rd party.
4. Recruit employees who already have the skills you need.

> **Note:** good place to look for external expertise is NCSC's certified cyber professionals.

DEVELOP FUTURE STAFF: SPONSORSHIP, APPRENTICESHIPS AND WORK EXPERIENCE

Supporting young people to pursue an education in cyber security can be a brilliant way of ensuring a future pipeline of employees with the right skills. There are many schemes aimed at school and university-age students and almost all of them involve some industry participation or support, including apprenticeships, site visits and speaker opportunities.

> **NCSC** runs CyberFirst events and apprenticeships and is looking for company sponsors and placements. You could also forge links with universities through involvement in the CyberInvest scheme which enables organisations to fund and support cyber security research.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **growing cyber security expertise**.

Q1. As an organisation, what cyber expertise do we need, and what do we have?

You should find out:

- What expertise do we need to manage our cyber risk? What do we need to keep in-house and what can we outsource?
- Are each of our requirements continuous? For example, you might only need a penetration testing team to come in a few times a year, but you might need someone to monitor your systems all year round.
- What expertise is the minimum for all staff? How can you ensure a healthy cyber security culture in the organisation? How well and how frequently are you training staff in your security policies and any particular threats your organisation might be vulnerable to?
- How many staff do we currently have with cyber security expertise and what gaps are they telling us we have in our provision?

Q2. As an organisation, what is our plan to develop what we don't have?

You should find out:

- Which skills are a priority?
- Who owns the plan to develop cyber expertise, and how are they responsible for delivering against it?
- How you will find people with the right aptitude for the different cyber security skills? Remember that people from all backgrounds, and with technical and non-technical skills, may be well suited to this field.
- What support the Board can give to this work, both in terms of investment or broader resources?

Q3. As a Board member, do I have the right level of expertise to be accountable for cyber security decisions?

- Do I understand enough about the decisions being made on cyber security in my organisation to be accountable to shareholders?
- If not, what plan do I have in place to increase my expertise? The Introduction to Cyber Security section of this Toolkit is a good place to start. There are also many training providers who run sessions specifically for Board level.

Q4. As an organisation, are we building an equal, diverse and inclusive workforce to tackle our cyber security skills challenges?

- Do we have a champion for EDI (Equality, Diversity and Inclusion)?
- Do we have the right policies in place, and do they work well in practice as well as looking good on paper?
- Are we gathering the right data and interpreting it correctly? Are we then having the right conversations with individuals all around the organisation, to supplement this data and create a richer picture on less tangible measures?
- Are we making active, meaningful efforts to recruit from all communities, to reflect the society we operate in?
- Do we use a range of recruitment methods, to help overcome unconscious bias and ensure we fully explore candidate strengths?
- Are we confident that we are recruiting and developing staff to meet the challenges our organisation will face in the future, not just complete the tasks of today?
- Are we creating the right environment and culture to make staff feel confident, safe and comfortable in flagging issues?

Developing a positive cyber security culture

Establishing and maintaining a healthy culture, in any part of the business, is about putting people at the heart of structures and policies. However, when it comes to cyber security, there is sometimes a tendency to focus almost exclusively on the technical issues and to overlook the needs of people and how they really work.

This rarely results in success. We know, for example, that when official policy makes it hard for someone to do their job, or when a policy is no longer practical, that people find workarounds and ‘unofficial’ ways of carrying out particular tasks.

Without a healthy security culture, staff won't engage with cyber security so you won't know about these workarounds or unofficial approaches. So not only will you have an inaccurate picture of your organisation's cyber security, but you will also miss the opportunity for valuable staff input into how policies or processes could be improved.

What should the Board do?

Lead by example

You set the tone when it comes to cyber security. Lead by example and champion cyber security within your organisation.

We often hear stories of senior leaders ignoring security policies and processes, or of asking for 'special treatment' in some way (such as requesting a different device to those issued as standard). This tells everyone else in the organisation that perhaps you don't consider the rules fit for purpose, and/or that it is acceptable to try to bypass them.

If policies don't work for you as a Board member (that is, if you find yourself doing something different to get your job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it.

Culture takes time and concerted effort to evolve. Don't assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

What should your organisation do?

Put people at the heart of security

Ultimately, the role of security should be to enable your organisation to achieve its objectives. It follows that if your cyber security measures aren’t working for people, then your security measures aren’t working.

Some organisations fall into the trap of treating people as the 'weak link' when it comes to cyber security. This is a mistake. Effective security means balancing all the different components, not expecting humans always to bend to meet the technology. More importantly, the organisation can't function with people, so staff should be supported so they can get their job done as effectively and securely as possible.

Security and leadership need to make the most of what people’s behaviour is telling them. Whilst technical monitoring can look for anomalies, people can act as an early-warning system and intuitively spot something that looks unusual. Ensuring staff know who to report any concerns to can save the organisation a huge amount of time and money in the long run. If staff are working around a set procedure, this may highlight a particular policy or process that needs reviewing.

Develop a 'just culture'

Developing a 'just culture'[1] will enable the organisation to have the best interaction with staff about cyber security. Staff are encouraged to speak up and report concerns, appropriate action is taken, and nobody seeks to assign blame. This allows staff to focus on bringing the most benefit to the organisation rather than focusing on protecting themselves.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **developing a positive cyber security culture**.

Q1. As a Board member, do I lead by example?

You might do this by:

- Ensuring staff feel empowered, and have a suitable mechanism to raise security concerns, at any level in the organisation.
- Engaging with and respecting security decisions and working with decision makers to highlight ineffective policies.
- Taking responsibility for your own role in cyber security by recognising the risk you pose as a likely target for attackers and acting accordingly.
- Speaking openly and positively to staff about why cyber security is important to the organisation.

Q2. As an organisation, do we have a good security culture?

Some signs that an organisation has a good approach would be:

- Staff know how to report any concerns or suspicious activity, and feel empowered to do so.
- Staff don't fear reprisals when they report concerns or incidents.
- Staff feel able to question processes in a constructive manner.
- Staff input is demonstrably used to shape security policy.
- Staff understand the importance of cyber security measures and what it means for the organisation.

Q3. As an organisation, what do we do to encourage a good security culture?

This can vary hugely depending on the size of your organisation. Some examples we have seen include:

- Properly resourced staff awareness .
- Ensuring that staff input is included when creating new policies or system designs.
- Sharing security metrics which focus on success rather than failure (for example, how many people identified phishing emails rather than how many people clicked on them).
- Support from senior leadership on the importance of security.

[1] "A just culture is a culture of trust, learning and accountability. A just culture is particularly important when an incident has occurred, when something has gone wrong. How do you respond to the people involved? How do you minimise the negative impact and maximise learning?" – Sidney Dekker

Establishing your baseline and identifying what you care about most

There are two tasks in this section, but we examine them side-by-side as the results of one will impact on the other, and vice versa. The two tasks are:

- working out which components of your 'technical estate' (that is, your systems, data, services and networks) are the most critical to your organisation's objectives
- understanding what your technical estate comprises, so that you can establish a baseline which will inform both your risk assessments and the deployment of your defensive measures

Whilst these two tasks have separate purposes, you will need to have some baseline of your technical estate in order to understand which parts of it are mission critical. At the same time, you will need some way to prioritise which areas to baseline, as doing this for your entire technical estate would be a very resource intensive task.

What should the Board do?

Work out what you care about the most

As with any other business risks, your organisation will not be able to mitigate all cyber security risks at all times. So the Board will need to communicate key objectives (it might be 'providing a good service to customers and clients', for example) in order for the technical experts to focus on protecting the things that ensure these objectives are fulfilled.

The Board should also consider what is most valuable to the organisation. For example, the Board might know that a specific partner is crucial to the organisation and that a compromise of their data would be catastrophic. This should be communicated to technical teams, so that they can prioritise protecting these 'crown jewels'.

It is **critical** that this is an active and ongoing discussion between Boards and their experts:

- Boards will have business insight that technical teams may not have (such as which particular partner relationship must be to be prioritised)
- technical teams will have insight into the enablers for key objectives (such as which networks or systems do particular partners rely upon)

Only by bringing these two together can you get a full picture of what is important to protect. Once you have this picture it is likely the Board will still need to prioritise within that list. This understanding will not only help focus the aim of your cyber security, but will also inform the assessment of the threat your organisation might be facing.

What are your crown jewels? Your crown jewels are the things most valuable to your organisation. They could be valuable because you simply couldn't function without them, or because their compromise would cause reputational damage, or it would incur financial loss. Some examples could be:

- bulk personal data
- intellectual property
- your public-facing website
- industrial control systems

What should your organisation do?

Work out where you are starting from

This provides information that underpins your risk decisions in two ways.

Firstly, it influences the options you have. Knowing which systems are connected to each other, who and what has access to particular data, and who owns which networks are all critical to setting good defences. This information will also be required in an incident to make an assessment of the damage an attacker could be inflicting, or the impact of any remedial actions you might decide to take.

Secondly, it might influence your risk assessment. Sometimes a risk comes not from a threat to an important asset, but from a vulnerability in your organisation's systems. Many incidents are the result of vulnerabilities in older, legacy systems, and the incidents arise not because the vulnerability can't be defended against, but because the organisation didn't have a good enough understanding of their systems to realise they were exposed.

Understanding the entirety of your estate can be a daunting, or impossible, task - especially for organisations whose networks and systems have grown organically - but even a basic understanding will help, and a good understanding of your priorities can help focus this task.

Identify critical technical assets

Based on the Board's priorities you need to identify what parts of the technical estate are critical to delivering those top-level objectives. This could be systems, data, networks, services or technologies. For example, maintaining a long-term customer base may be a priority objective. There are lots of ways that good cyber security could enable this. It could be:

- securing a customer database to protect their data
- ensuring resilience of the order processing system to ensure deliveries go out on time
- ensuring availability of the website so that customers can contact you easily

It can sometimes be difficult to identify these dependencies as they are such an integral part of your operation that they can be taken for granted, but the questions below can help. Doing this in conjunction with baselining your technical estate will also help to potentially identify assets that you weren't even aware of, and are actually critical to providing certain services.

> **Working with suppliers and partners** Most organisations will have suppliers or partners with whom they receive, provide or share information, systems or services. You must consider this in your baseline of your estate as these are potential entry points to your organisation.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **establishing your baseline and identifying what you care about most**.

Q1. As an organisation, do we have a clear understanding of how technical systems, processes or assets are contributing to achieving our objectives?

Some questions to consider that may help in identifying these dependencies include:

- What are our 'crown jewels' (that is, the things our organisation could not survive without) ?
- What requirements must we meet (such as legal or contractual requirements) ?
- What do we not want to happen, how could that come about ?

Q2. As a Board, have we clearly communicated our priority objectives and do we have assurance that those priorities guide our cyber security efforts?

Cyber security strategy should be integrated into your organisation's strategy and your strategic priorities should guide defensive efforts. A good organisation should have a process for ensuring these strategies remain aligned and should be able to demonstrate how investment is focused on those priorities.

For example, if a promise to customers about their privacy is a priority then you might:

- identify what could jeopardise this promise e.g. the loss of their credit card details
- identify what technical assets are required to secure those details e.g. database, access management system
- prioritise defending these assets when implementing cyber security measures
- audit measures regularly

Q3. As an organisation, how do we identify and keep track of systems, data or services that we are responsible for?

If you are a large organisation and your systems have grown organically, understanding the detail of your systems, devices and networks may be impractical. At a minimum you should be aware of what level of understanding you do have and the potential risks that any undocumented systems might pose. Ideally you want to start with a good idea of what your technical estate looks like and then have a process to ensure any changes are considered and recorded to keep the baseline up to date. This baseline might include information such as:

- inventory of the hardware and software used across the organisation
- an up to date register of systems, including all internet-connected, partner-facing, systems and networks
- details of data sets; which services, systems and users have access to them, where are they stored, how are they managed

Understanding the cyber security threat

The type of threat faced is shaped by the nature of organisation and the services an organisation provides. For example, the vast majority of organisations won't be targeted specifically by nation states and so may focus on the threats posed by cyber criminals. However, organisations who form part of, or are providing services to, our Critical National Infrastructure and defence sector may be at risk from nation states.

Understanding the threats faced by your organisation, either in its own right or because of who you work with, will enable you to tailor your organisation's approach to cyber security investment accordingly. You need to consciously make the decision about what threat you are trying to defend against, otherwise you risk trying to defend against everything, and doing so ineffectively.

What should the Board do?

Get an understanding of the threat

An understanding of the cyber security threat landscape will be key to helping the Board make well-informed governance decisions. For example, you may prepare differently for a merger with a company if you know that they provide important products or services to Critical National Infrastructure and therefore may be a target for a nation state. The Board will already have insight into the threats or challenges facing their sector. This should be complemented by an awareness of the motivations of attackers, and a mechanism for staying up to date with key cyber security developments (for example, the growth of ransomware).

Collaborate on security

One of the best sources of information on good practice and relevant threats can be your sector peers. Attackers often target a number of organisations in the same sector in a similar manner. Cultivating these collaborative relationships on security has two major benefits. Firstly, it can help make your own organisation more resilient, through early warning of threats and improved cyber security practice. Secondly, it helps make the sector as a whole more resilient, which can reduce the appeal to potential attackers.

> **Cyber Security Information Sharing Portal**: The NCSC's Cyber Security Information Sharing Partnership provides a secure forum where companies and government can collaborate on threat information. Access to CISP not only provides the opportunity to securely share intelligence with trusted partners in your sector, but also gives access to sensitive threat reports and the full breadth of NCSC advice.

Assess the threat

Working out the 'threat actors' (the groups or individuals capable of carrying out a cyber attack) relevant to your organisation can help you make decisions on what you are actively going to defend against. Whilst investing in a good baseline of cyber security controls will help defend your organisation from the most common threats, implementing effective defences against a more targeted or sustained attack can be costly. So dependent on the likelihood and impact of that threat, you may decide that it is not worth that additional investment.

Ongoing discussion between the Board and experts will help you to prioritise the threats to actively defend against. The experts will have an in-depth understanding of the threat, and the Board will be able to identify the features of the organisation that might make it an attractive target to attackers. It is also critical to have this discussion in advance of any decision that will significantly change the threat profile of the organisation, in order to give technical staff the time to suitably adapt the organisation's cyber security.

Working with suppliers and partners

When assessing the threat, you should consider not only the value that you might have as a standalone organisation, but also the value you may represent as a route into another, possibly larger organisation. For example, you may supply important services to an organisation involved in Critical National Infrastructure, in which case, a nation state may want to attack your organisation in order to access their ultimate target.

What should your organisation do?

Don't underestimate the impact of untargeted attacks

An untargeted attack is where an attacker uses a 'scattergun' approach to reach thousands of potential victims at once, rather than targeting a specific victim. Attackers often use automated, widely available tools that scan public-facing websites for known vulnerabilities. This same tool will then, once a vulnerability has been found, exploit that website automatically, regardless of who it belongs to. This could have just as much impact on your organisation as a targeted attack. A good baseline of basic cyber security controls and processes will protect your system from the majority of these attacks.

Obtain good intelligence - and use it

You will need different types of threat intelligence for different purposes. A good overall threat picture is needed for governance decisions and timely threat intelligence for day-to-day and tactical decisions. Many industry and government partners offer threat intelligence, from annual reports on general trends, right down to highly technical reports on a specific type of malware. You therefore need a mechanism for identifying what intelligence your organisation needs, for what purpose and for sharing that intelligence internally. Critically you then need to use that intelligence to inform business decisions, including procurement, outsourcing, training, policy and defence of your networks.

You can also gather threat intelligence internally. You will likely have experience of attacks on your own organisation which can provide strategic insight into activities of threat actors, as well as tactical details on the methods of the threat actors. These specific details will likely come from logging or monitoring within your organisation.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **understanding the cyber security threat to your organisation**.

Q1. As an organisation, which threats do we assess are relevant to our organisation, and why?

This assessment should:

- identify potential motivation for those threats and the likelihood of them targeting your organisation
- inform which risks you are willing to tolerate
- be enriched by collaboration with key partners in your sector
- be supported by evidence from the attacks you have experienced to date

Q2. As an organisation, how do we stay up to date with the cyber threat?

You might:

- seek to discover evidence of any attacks in system logs you may hold
- subscribe to a number of threat intelligence feeds
- be part of a sector-specific intelligence sharing group
- have mechanisms for sharing key cyber threat updates internally

Q3. As an organisation, how do we use threat intelligence to inform business as usual (BAU)?

This should be a continuous cycle with threat assessments informing BAU decisions, and BAU experience informing the threat assessments. Examples might be:

- assessing the likelihood and impact of threats to inform risk assessments and appetite
- educating staff on the key threats they face so that they can make informed decisions
- taking lessons from previous incidents to inform threat assessments
- using threat intelligence to focus defensive measures
- including threat consideration in change or procurement decisions (for example, when choosing a new enterprise IT provider, considering a potential merger or designing a new product)

Risk management for cyber security

Most organisations will already be taking steps to assess and manage their cyber security risk. However it is worth considering what the driver is for that activity. Often, organisations conduct risk management exercises for 'compliance' reasons, which could include:

- obligations from external pressures (such as regulatory requirements)
- customers' demands
- legal constraints

When done for these reasons, there is a danger of risk management becoming a tick-box exercise. This can lead to organisations believing they have managed a risk, when in reality they have merely complied with a process which may have (albeit unintended) negative consequences.

Compliance and security are not the same thing. They may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices. Good risk management should go beyond just compliance. Good risk management should give insight into the health of your organisation and identify opportunities and potential issues.

What should the Board do?

Integrate cyber security into organisational risk management processes

Many of your organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated with your organisational approach to risk management. Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for you to recognise the wider implications of those cyber security risks, or to consider all the other organisational risks that will have an impact on cyber security.

The role of cyber security should be to support and enable the business, and it should do this by managing its risks without blocking essential activities, or slowing things down, or making the cost of doing business disproportionately expensive.

Don't make reducing risk levels the measure of success

It can be difficult to measure the success of your organisation's cyber security efforts. A typical output of good cyber security is the absence of a failure, which can be hard to measure, and since cyber security is still a relatively new field there aren't yet many established metrics to draw on.

It is common for risk assessments to deliver some kind of assessment level, be that high medium low, or a number, and so it could be tempting to use this as a performance metric for your cyber security efforts. However, they are a poor metric of your internal security efforts as they are influenced by external factors that are outside of your control - factors which change extremely rapidly. New vulnerabilities are being discovered every day and the number of actors seeking to use cyber means to achieve their aims is increasing.

Driving performance through reduction of a number associated with the cyber security risk will likely incentivise risk assessors and reviewers to underestimate the risks, leading to less informed decisions. Some considerations on what 'good metrics' look like is provided in Implementing effective cyber security measures.

What should your organisation do?

Be realistic about the risks

Similar 'good practice' risk management principles will apply for managing cyber risk as they would for managing any other organisational risk. However, there are two things to bear in mind.

Firstly, solutions and technologies in cyber security are advancing so quickly that it is easy to get caught out using outdated assessments of cyber risks. So you may need to review cyber security risks more regularly than other risks.

Secondly, because cyber security is still a relatively new field, the organisation won't have as intuitive an understanding of cyber security risks, as it might for say, financial risk. As new technologies emerge, there might not be a huge evidence base to draw on to form a risk assessment. This is worth bearing in mind when considering the confidence you have in an assessment of cyber security risk, especially if that assessment is going to be directly compared to assessments of more well-established risks.

A good example of this is cloud security. The NCSC see many organisations hesitant to use cloud services because they intuitively assume it is high risk, informed mainly by the belief that storing something valuable with a third party is more risky. In reality, the third party (so in this case a cloud service provider) may have better security measures within their data centres than your own on-site storage. So the overall risk may actually be lower. A decision to adopt recent technologies - like cloud storage - would need to be based on a comprehensive understanding of all the risks, rather than an intuitive assessment.

> **Managing risk for newer technologies** The NCSC has produced guidance on Cloud security and Software as a Service which can help identify and assess the associated risks.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **managing cyber security risk**.

Q1. As an organisation, do we have a process that ensures decision makers are as well informed as possible?

The primary focus of your process should be that decision makers can make the most well-informed decisions. The decision makers might be the Board (who have to set a risk appetite based on an understanding of a technical or operational risk) or it might be the practitioners who need to decide how to implement a specific course of action fed down from the Board. Both need to be as well informed as possible (in an understandable format) to allow those decisions to be made well. This means the output of risk assessments needs to **meaningfully** articulated. Qualified outputs are usually the most effective and are preferable to meaningless results where sometimes arbitrary numbers are added or multiplied to derive a score.

Q2. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

Any decision maker in your organisation should have an awareness of the importance of cyber security risk and enough expertise (or access to expertise) to consider cyber security risk in the decisions they make. To begin with you might want to:

- consciously build in consideration of cyber security risk to any decision making processes you have
- focus on educating people on cyber security

A way to check if this is working is to look at a decision taken in your organisation and review whether cyber security risk has been balanced with other business risks. For example, an organisation may assess that introducing a Bring Your Own Device (BYOD) policy brings substantial benefit to the organisation in terms of flexible working. There are many different things you would expect to be considered in this decision, including:

- the potential improvement in staff productivity
- the potential security implications of having devices the organisation does not control connecting to the organisation's networks
- the cost implications
- the liability implications

Were these considered jointly when making the decision, or was security only discussed once the decision was already made?

Q3. As an organisation, do we have an effective and appropriate approach to manage cyber risks?

Both the Board and the practitioners should be able to clearly and simply articulate the process in a few minutes. The details of this framework might include:

- how risks are escalated
- what the threshold is for Board involvement in a risk decision
- how we convey the confidence in a particular risk assessment
- how often risks are reviewed
- who owns which risks
- who is responsible for the framework itself and for ensuring it is fit for purpose (for example, ensuring that the output of the risk assessment process genuinely reflects the assessment of the risk)

Q4. As a Board, have we clearly set out what types of risks we would be willing to take, and those which are unacceptable?

- Support decision makers if they make risk decisions within the parameters you set.
- Be clear on the process and the threshold for escalating the risk.
- Be as specific as you can in terms of the types of risk and the amount of risk. For example, you might be unwilling to tolerate any significant risk to personal data but would be willing to accept email being unavailable for a day.
- Consider the cumulative risk you are accepting; it's possible that all your cyber risk could be realised at the same time. In a single incident, you might lose email for a day, the public website might be unavailable and financial data you hold might be stolen. Whilst you may have accepted some risk of all those things happening, you may not have considered whether the organisation could tolerate them all happening at once.

Implementing effective cyber security measures

Implementing good cyber security measures is not only a key part of meeting your regulatory requirements but will also help reduce the likelihood of a significant incident. Implementing even very basic cyber security controls will help reduce the chance of an incident.

> **5 questions for the boardroom agenda** If you'd like more details about how to generate constructive cyber security discussions between board members and technical experts, refer to the NCSC's original 'Board toolkit: five questions for your board's agenda' guidance.

What should the Board do?

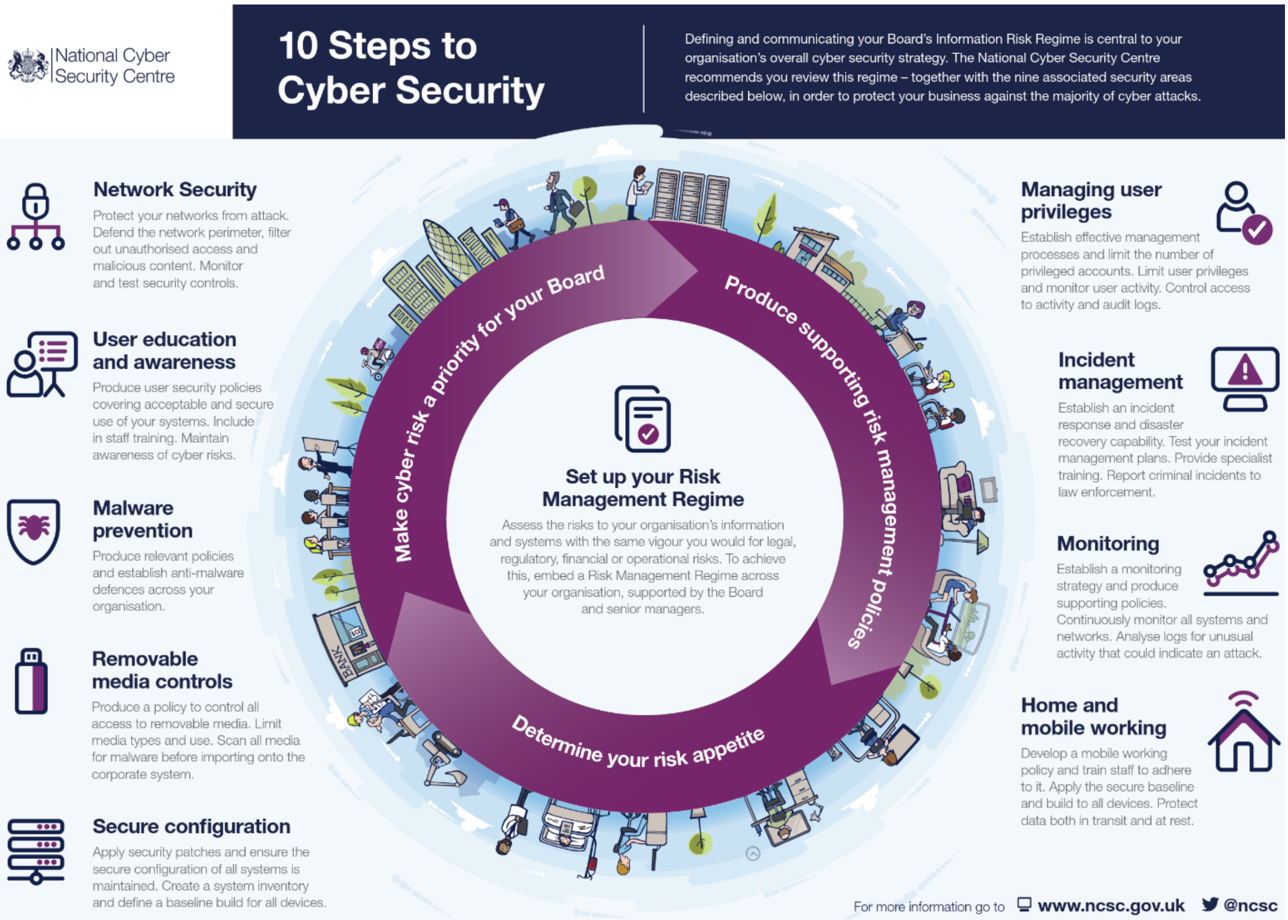
Get a little bit technical

Having a basic understanding of cyber security can help you to ask the right questions to seek assurance about your organisation's cyber resilience - just as you would need to have a certain level of understanding of finance to assess the financial health of your organisation. A good place to begin is to discuss your existing cyber security measures with your experts, and the questions below suggest a starting point for what to ask.

What should your organisation do?

Start with a cyber security baseline

Attackers often use common methods to attack a network. A lot of these methods can be mitigated against by implementing basic cyber security controls. There are several frameworks that outline what good cyber security controls look like. These include ISO/IEC 27002, the NIST Cyber Security Framework and the NCSC's 10 Steps to Cyber Security, a summary of which is shown below.



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

If you are an SME or a charity with fewer resources available to combat cyber security, you may want to instead use the Small Business Guide or Small Charity Guide.

Tailor your defences to your highest priority risks

The basic cyber security controls will help mitigate against the most common cyber attacks, but once you have that baseline in place, you then need to tailor your defences to mitigate your highest priority risks. Your measures will be tailored both to your technical estate (protecting the things you care about the most) and to the threat (protecting against methods used by specific threat actors).

NCSC guidance can help you address these priorities. For example, if you know that one of your critical systems has external connections, you might consider the specialised guidance on how to safely import data into that system.

Layer your defences

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) help reduce the chances of single point of failure. This approach is commonly referred to as 'defence in depth'. Each measure provides a layer of security and deployed collectively, greatly reduce the likelihood of a cyber incident. Once you have your cyber security baseline in place you can focus on layering your defences around those things that are most important to you - or particularly valuable to someone else.

Defend against someone inside your network

Defences do not stop at the border of your network. A good defence assumes that an attacker will be able to access your system and works to minimise the harm that they can do once they are inside it. One of the key things you can do to limit the damage they can inflict is to restrict their movement and access. Effectively managing user privileges and segregating your network are common approaches. Identifying an attacker inside your system as soon as possible will also help limit the damage they can do. Monitoring and logging are key to being able to spot any signs of malicious activity.

These measures will also help mitigate the threat from a malicious insider; somebody who has legitimate access to your systems but then uses that access to do harm. This threat ranges in capability and intent, from a disgruntled employee through to corporate espionage.

Review and assess your measures

Good cyber security is a continuous cycle of having the right information, making informed decisions and taking action to reduce the risk. You will need to be continuously assessing and adapting your defences as the needs of your organisation and the profile of the threat changes. To do this it's important to have some way to assess whether your defences are effective.

There are several mechanisms available to technically assess the effectiveness of your security controls. This may include things like testing the security of your networks (pen-testing) through to certification of products or services. You may want to use a combination of internal mechanisms and objective assessment provided by an external source.

Engaging with staff will also help you gain a more accurate picture of your organisation’s defences. It will also give you the opportunity to get valuable staff input into how policies or processes could be improved. Metrics or indicators can also tell you where you need to change your approach or adapt to new circumstances. Understanding exactly what an indicator is telling you may require further investigation of the situation. An example is the trend in people reporting suspicious emails. A decline in the number of people reporting can either mean fewer malicious emails are getting through to people’s inboxes, or it could mean fewer people are reporting any concerns because they don't receive feedback when they do, and therefore believe nothing is ever done afterwards.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing your organisation's cyber security measures**.

Q1. As an organisation, how do we assure ourselves that our measures are effective?

You might seek this assurance through:

- Penetration testing carried out by an external organisation, and action taken on the back of their results.
- Automated testing of your defences and monitoring of activity on your networks by your IT security team.
- Reviewing defensive measures against suitable frameworks, this could be an internal review or an independent consultant. Suitable frameworks might be Cyber Essentials, 10 Steps to Cyber Security, ISO/IEC 27002 or the NIST Cyber Security Framework.
- Ensuring threat assessments and defensive priorities are regularly reviewed and defensive measures updated accordingly.
- Ensuring that the focus of your cyber security measures is aligned with the risks you have identified and prioritised.

Q2. As an organisation, what measures do we take to minimise the damage an attacker could do inside our network?

You might consider:

- How you authenticate and grant access to users or systems. You want to ensure that these measures are not easy to bypass and that you don't afford access unless necessary.
- How you would identify an attacker's presence on your networks - normally done through monitoring.
- How you separate your network so that if an attacker gets access to one device they do not have access to the full range of your technical estate.

Further details on these three points are provided in NCSC guidance on preventing lateral movement.

Q3. As an organisation, do we implement cyber security controls to defend against the most common attacks?

As an organisation, how do we defend against phishing attacks?

- We filter or block incoming phishing emails.
- We ensure external mail is marked as external.
- We stop attackers 'spoofing' our own emails.
- We help our staff to identify and report suspicious emails.
- We limit the impact of phishing attacks that get through.

As an organisation, how do we control the use of privileged IT accounts?

- We use 'least privilege' when setting up staff accounts.
- We reduce the impact of attacks by controlling privileged accounts.
- We have strong links between our HR processes and the IT account function.

As an organisation, how do we ensure that our software and devices are up to date?

- We have defined processes to identify, triage, and fix any exploitable vulnerabilities within our technical estate.
- We've created an 'End of life plan' for devices and software that are no longer supported.
- Our network architecture minimizes the harm that an attack can cause.
- We make appropriate use of 3rd party or cloud services and focus on where we can have most impact.

As an organisation, what authentication methods are used to control access to systems and data?

- We take measures to encourage the use of sensible passwords.
- We ensure passwords don't put a disproportionate burden on staff.
- We implement two factor authentication (2FA) where possible.

Collaborating with suppliers and partners

There are four reasons why cyber security is a key consideration when collaborating with suppliers and partners:

1. You increase the number of routes and external touchpoints in your organisation. So if any of them are compromised, you are also at risk.
2. You may be targeted as a way into the organisation you are supplying.
3. Your suppliers may be targeted as a route into your organisation.
4. You may be sharing sensitive or valuable data or information that you want suppliers to protect.

Being able to demonstrate a good level of cyber security is increasingly a key component of supplier and provider contracts, and is already a requirement for many government contracts.

What should the Board do?

Build cyber security into every decision

All organisations will have a relationship with at least one other organisation, be that the provider of your email service, or the developers of the accounting software you use, through to your traditional procurement supply chain. Most organisations will be reliant on multiple relationships. Each of these relationships will have a level of trust associated with them, normally some form of access to your systems, networks or data. There are three key things you therefore need to ensure:

1. That this access doesn't provide a route for an attacker to gain access to your organisation, either through deliberate action or unintentional consequence.
2. That any partner or supplier is handling any sensitive data appropriately and securely.
3. That any product or service you buy has the appropriate security built in.

Cyber security risk should be a key consideration in any decision on new relationships or collaborations. This includes decisions on suppliers, providers, mergers, acquisitions and partners.

What should your organisation do?

Identify your full range of suppliers and partners, what security assurances you need from them, and communicate this clearly

Review your current supply chain arrangements to ensure you are setting out your security needs clearly and identifying the actions you need to take as a result. If you yourself are a supplier, ensure you meet the security requirements set for you by your customer as a minimum.

Ensure that the security requirements you set are justified and proportionate and match the assessed risks to your operations. Also be mindful of the current security status of your suppliers to give them time to make the necessary improvements. It might be useful to include references to the following NCSC guidance that can help to establish a baseline of cyber security:

- 10 Steps to Cyber Security
- Small Business Guidance
- Cyber Essentials

The following NCSC guidance can help you to assess your own security needs from suppliers:

- Supply chain guidance
- Cloud services guidance
- Software as a Service guidance

Get assurance

Security should be built into all agreements from the start, and you should have confidence that your security needs are being met. Dependent on your relationship with the supplier or provider and your resources, you could seek assurance of this through testing, auditing or adherence to accreditation standards.

Consider the implications if your supplier is compromised

No matter how comprehensive your security agreements with your partners are, and no matter how well they implement their controls, you should assume that your partners will be compromised at some point. You should plan the security of your networks, systems and data accordingly with this assumption in mind. This is also worth considering in your security agreements; what are you expecting of them and their response? Do they have to notify you? Do they have to assist you if you are consequently also compromised?

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing your organisation's cyber security measures**.

Q1. As an organisation, how do we mitigate the risks associated with sharing data and systems with other organisations?

You should:

- Have a good understanding of your suppliers, what data and networks they have access to and have a process for keeping this up to date.
- Set clear expectations of how your partners protect your data and access your systems.
- Build security into all relationships and agreements from the start.

To do this you might:

- If you have a very large number of supply chain companies, agree processes with your main suppliers on how they sub-contract any work, specifically what obligations they have to inform you.
- Choose organisations that can demonstrate the security of their defences. For example, larger organisations will have carried out regular pen tests and responded to the findings to understand their residual vulnerability. SME's might have been certified under the government's Cyber Essentials Scheme.
- Limit services exposed and information exchanged with other organisations to the minimum necessary.
- Implement user and system authentication and authorisation before access is granted.
- Audit any sensitive actions or data exchange/access.

Q2. As an organisation, how do we ensure that cyber security is considered in every business decision?

Security should be embedded in your culture and strategy, and should therefore be consciously considered in any decision regarding procurement, mergers or acquisitions. If there is a process for making those decisions, security can be explicitly identified as a relevant consideration and any conclusions recorded.

Q3. As an organisation, are we confident that we are fulfilling our security requirements as a supplier?

If you are a supplier to other organisations you are exposed to an increased risk. Both a reputational risk (if your product causes your customer to be compromised) and also operational risk (since you now provide access to more, and potentially more valuable, organisations). You should:

- Know how you would respond should your organisation be compromised, putting at risk partner networks you are connected to, or customer data you may hold.
- Have a good understanding of your customers and the impact they may have on your threat profile (for example, if you are in the supply chain for UK Critical National infrastructure you may be at increased risk from foreign state actors).

Q4. As a Board, do we have a clear strategy for using suppliers, and have we communicated it?

If procurement and supplier decisions are devolved below the Board, have you clearly described:

- What risk you are willing to accept in using suppliers? For example, if your organisation is compromised through a supply chain attack, you may not be exposed to the same level of reputational risk as if you were directly compromised, but you may be exposed to the same level of financial risk.
- What are your expectations of suppliers' security, and how much you are willing to pay for better security? For example, if company A is more expensive but also more secure, how much cheaper would company B need to be to make it the better option?
- What opportunities you are trying to exploit? This should be supported by an awareness of what you are able to cater within your organisation and what you will outsource. For example, if you assess it's not feasible to support your own data storage, do you take advantage of the competitive cloud data storage market?
- What your appetite is for working with partners or suppliers overseas? Some jurisdictions are incompatible with UK security and regulatory requirements or may bring very different continuity of supply issues. For further considerations see CPNI's Secure Business guidance.

Planning your response to cyber incidents

Incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. Being prepared to detect and quickly respond to incidents will help to prevent the attacker from inflicting further damage, so reducing the financial and operational impact. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on your reputation.

Experiencing an incident? If you are currently experiencing an incident, you can contact the NCSC.

What should the Board do?

Ensure you have a plan

1 in 10 organisations don't have an incident management plan. If you're one of these organisations, then you should address this immediately.

Understand your role in incident management

Incidents often occur at inopportune moments and most people's decision making is compromised in times of crisis. For these reasons, everyone must have a clear understanding of their role and the organisational response in advance, especially Board members who would likely be representing the organisation in the media.

The Board also needs to be explicit about who it is willing to devolve authority to (especially outside core working hours), and exactly what that authority covers. For example, does that cover calling in a contracted incident response company, or taking down a public facing website? The Board also needs to be explicit about when it wants to be informed of an incident, both in terms of at what stage of the incident, and in terms of what significance of incident they need to know about.

Get involved in exercises

The best way to test these processes and thresholds (and to get a good understanding of the Board's role) is through exercising the incident management plan. If you would be involved during a real incident, then you should be involved in an exercise. Doing this in conjunction with operational staff can also help to highlight issues around authority for critical decisions. Even if you do not have a direct role in responding to an incident, running an exercise can be a good way to understand the realities of how an incident would impact on your organisation.

Drive a 'no blame' culture

Post-incident analysis provides insight that can help you reduce the likelihood of incidents occurring in the future and reduce their potential impact. Crucially in order to get this insight you need to be able to be honest and objective about what has happened. This can only happen in a no blame culture, such as you would use when investigating health and safety incidents. Critically for the Board, new regulation, such as GDPR, is clear that responsibility for incidents or data breaches sits with the organisation and not an individual. Therefore the Board is ultimately responsible for any cyber security incident as the governing body. Apportioning blame to a specific individual within the organisation will be treated as poor cyber security practice.

What should your organisation do?

Work out what an incident would look like

One of the most common things overlooked is being able to identify what constitutes an incident. There's two aspects to this:

- working out how you would spot an event in the first place
- working out at what point an event (something happening on your networks or systems) becomes an incident

HOW WOULD YOU SPOT AN EVENT?

Depending on their motives, an attacker is unlikely to tell you when they have successfully compromised your organisation, so you need your own methods to identify an intruder or an attack. This normally takes the form of monitoring. Monitoring refers to observing data or logs collected from your networks or systems to identify patterns or anomalies that could indicate malicious activity. Even if you don't have monitoring to identify the incident, it is still useful to collect system or network logs (especially those relevant to your critical assets) so that you can retrospectively review them once you know an incident has occurred.

WHEN DOES AN EVENT BECOME AN INCIDENT?

This is often not a clear cut decision. You can try and gather as much information as possible to inform your assessment of an 'event', but you probably won't have a complete picture of what has happened. Beginning an incident response might have implications for cost, reputation and productivity, so you will want to consider who has the authority to make this decision, and what the thresholds are for an incident in advance.

WHAT IS A CYBER SECURITY INCIDENT?

A breach of the security rules for a system or service - most commonly:

- attempts to gain unauthorised access to a system and/or to data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owner’s consent
- malicious disruption and/or denial of service

Use the information you already have

All the information you have previously gathered on what's important to protect, the threat and your technical estate will provide critical insight in two key areas:

- It will give you insight into the impact of incident. If the attacker has accessed a particular user device, what could they access? Could they access those things you care about the most?
- It will help you determine your operational response. If the attacker is on a specific network can you isolate that network? If you can, what would the impact be on your organisation?

Take pre-emptive measures

Put measures in place to help reduce the harm that an attacker could do. This could be:

- introducing measures that restrict their movement once they are inside your network
- pre-emptively reducing the impact of attacks (for example, backing up your data will help to reduce the impact of a ransomware incident)

As with any other defensive measures, these should be focused on protecting what is most important to you.

Make an Incident Management plan

Cyber Incident Response is a complex subject as no two incidents are ever the same. However, as with all business continuity planning, you can develop a plan that will outline the key elements of your response. Your plan should not only cover the technical elements, but also:

- the people and process elements such as media, customer and stakeholder handling
- reporting to regulators
- dealing with legal actions

For more common incidents (such as DDOS) it may be helpful to develop a specific 'playbook' setting out your organisation's response.

Test your plan

Rehearsing your response to different scenarios is key to ensuring your plans are effective and remain current. There are various exercising packages you can use. This will be a critical part of the role for any staff involved directly in incident management, but every Board member also needs to understand their specific area of responsibility during an incident.

Learn lessons

An often overlooked aspect of incident management is the post-incident review. An incident can provide valuable insight into your cyber readiness, including:

1. The threat your organisation faces.
    - Who carried out the attack and was it targeted?
    - Did they go about it in the way you expected?
    - Did they go after the things you expected?
2. The effectiveness of your defensive measures.
    - What did your defences protect against?
    - What didn't they?
    - Could they be improved?
3. The effectiveness of your incident response measures.
    - What would you have done differently?
    - Did your response help to reduce the impact of the incident?
    - Did it make some aspects worse?

> **Working with suppliers and partners** Your plan should also consider how you mitigate the impact on any partners or customer organisations if you were compromised. When do you inform them? What mechanisms are in place to limit the damage it could do to them? You should also consider what you would do in the event that a supplier is compromised; you may not have control over how they deal with the incident. What would you be able to do independently to reduce the impact on your organisation? The best way to mitigate this risk is to have a collaborative approach to your security with your partners and suppliers.

What does good look like?

The following questions can be used to generate productive discussions with your technical team. The aim is to identify what constitutes 'good' cyber security in terms of **responding to cyber incidents**.

Q1. As an organisation, do we have an incident management plan and how do we ensure it is effective for cyber incidents?

A basic plan should include:

- Identifying the key contacts* (incident response team or provider, senior management, legal, PR, and HR contacts, insurance providers).
- Clear escalation routes (for example to senior management) and defined processes for critical decisions.
- Clear allocation of responsibility (specifically whether this is for normal working hours or 24/7).
- Basic flowchart or process for full incident lifecycle .
- At least one conference number which is available for urgent incident calls.
- Guidance on regulatory requirements such as when incidents need to be reported and when to engage legal support.
- Contingency measures for critical functions.

Q2. As an organisation, do we know where we can go for help in an incident?

This might include:

- Incident response providers (you might want to consider NCSC Certified Incident Response companies)
- NCSC Incident Management team, or if you believe you have been the victim of online fraud, via ActionFraud.
- Intelligence sharing groups, for details of other companies experiencing the same incident (consider joining CISP).

Q3. As an organisation, do we learn from incidents and near misses?

It's important to learn lessons from incidents as well as from 'near-misses'. These will give you valuable insight into the threat you're facing, the effectiveness of your defence, and potential issues with your policies or culture. A good organisation will use this insight to respond better to future incidents, and not seek to apportion blame. The Board may decide it doesn't need to know the details of every incident, just the most significant lessons learned from the incidents experienced.

Q4. As an organisation, how would we know when an incident occurred?

This incorporates two aspects; what are the triggers that can tell us an incident has happened, and how do we then share that information within the organisation?

When considering what might trigger an incident, you need to consider:

- What monitoring is in place around critical assets (like personal data) that would have an impact if compromised, lost or changed?
- Who examines the logs and are they sufficiently trained to identify anomalous activity?
- What reporting mechanisms are there in place for staff to report any suspicious activity?
- Are the thresholds for alerts set to the right level - are they low enough to give suitable warning of potential incidents and high enough that the team dealing with them are not overloaded with irrelevant information?

When considering how an incident will be shared internally, consider:

- What constitutes an incident?
- Who has the authority to make that decision?
- Who needs to know the details of the incident?
- Has the Board explicitly conveyed the threshold for when it wants to be informed of an incident?

Q5. As a Board, do we know who leads on an incident and who has the authority to take any decisions?

This will depend on your organisational structure. It might sit with the one member of the Board, or one of the executives, or it might be divided out into different roles. Ideally you should:

- Specify exactly who is able to take decisions on which aspects.
- Have backup plans in place if those decision makers are unable to fulfil that duty (for example, out of hours).
- Test this decision-making process, with a focus on potential areas of overlapping responsibility.

Q6. As a Board member, do I understand what's required of my role during an incident, and have I had training to equip me for that role?

Consider:

- Do I have the understanding required to make decisions potentially out of hours, and under time pressures?
- Do I need training to support my specific role in an incident, such as understanding relevant regulation, or dealing with the media?

Appendices

Appendix 1: Cyber security regulation

The regulation summarised below outlines the need for organisations to demonstrate and implement cyber security standards. The NCSC has contributed to the setting of cyber security standards to ensure they reflect good cyber security practice. By following and implementing NCSC guidance, organisations will be 'on their way' to meeting the cyber security requirements regulation.

General Data Protection Regulation (GDPR)

The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The Regulation does not mandate a specific set of cyber security measures, but rather expects you to take ‘appropriate’ action. In other words you need to manage risk. What is appropriate for you will depend upon your circumstances, as well as the data you are processing and therefore the risks posed.

However, there is an expectation you have minimal, established security measures in place. The security measures must be designed into your systems at the outset (referred to as Privacy by Design) and maintained effective throughout the life of your system.

The NCSC have worked with the ICO to develop a set of GDPR Security Outcomes. This guidance provides an overview of what the GDPR says about security, and describes a set of security related outcomes that all organisations processing personal data should seek to achieve.

Networks and Information Systems (NIS) Directive

The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the EU. It applies to companies and organisations identified as operators of essential services (OES). The regulatory responsibilities are carried out by Competent Authorities (CAs). The criteria for identifying OES and the list of CAs in the UK can be found within the NIS Regulations.

The NCSC is providing technical support and guidance to other government departments, Devolved Adminstrations, CAs and OES through:

- a set of cyber security principles for securing essential services
- a collection of supporting guidance
- a Cyber Assessment Framework (CAF) incorporating indicators of good practice
- implementation guidance and support to CAs to enable them to:
    - adapt the NCSC NIS principles for use in their sectors
    - plan and undertake assessments using the CAF and interpret the results

What is the NCSC's role in regulation?

The NCSC is not a regulator. However, as the UK technical authority for cyber security, the NCSC provides support and advice to companies and regulators to help minimise the risk of incidents and respond to them effectively if/when they do occur. The NCSC looks to ensure that any requirements are in line with best practice, and that frameworks are consistent across different pieces of regulation.

The NCSC also has a role to provide support during significant incidents, and these incidents may fall under specific regulation. We will encourage victims to consider their regulatory obligations, but recognise that any regulatory reporting or co-operation must be led by the victim.

It is also important to recognise that cyber security is only one aspect of security and business practice, and so there is wider regulation (such as Foreign Direct Investment, or EU restrictions on offshoring data) that must be considered in cyber security decisions.

Appendix 2: Help with cyber incidents

During an incident:

- If you are reporting fraud or cyber crime, please refer to the Action Fraud website.
- If you have been subject to a personal data breach that is required to be reported under the GDPR, please contact the ICO (Information Commissioner's Office). If there is malicious cyber activity related to this which you wish to report (either for information or for action), please complete an the NCSC Incident Form.
- If you are an Operator of Essential Services (OES) under the NIS Directive, please complete an NCSC Incident Form in addition to reporting to your Competent Authority (CA). This is applicable for any cyber incident which you feel requires NCSC's support (for action) or is for wider interest (for information).

Note that depending on the size of your organisation and the nature of the incident, you may receive support from the NCSC, the National Crime Agency or your Regional Organised Crime Units (ROCU).

For ongoing support and guidance:

The NCSC publishes all of its guidance on www.ncsc.gov.uk, and the NCSC twitter feed and LinkedIn page are good ways to keep up to date with new publications. If you want to receive more targeted information and a higher classification of threat intelligence, you should join an industry group in CISP.

Appendix 3: About the NCSC

The NCSC was set up to help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK internet through technological improvement and advice to citizens and organisations. Our vision is to help make the UK the safest place to live and do business online.

The NCSC supports the most critical organisations in the UK, the wider public sector, industry, SMEs, homes and families. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

The NCSC is the UK government's technical authority and therefore takes the lead role in providing guidance and advice on cyber security for UK organisations. We may also work with Law Enforcement when resolving or investigating an incident, or be asked to contribute to discussions on cyber security policy by government departments such as Cabinet Office or DCMS.

National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Cyber Security Toolkit for Boards: April 2019 **NCSC_CSTFB_G_02**

DUMFRIES AND GALLOWAY COLLEGE

Internal Audit Strategy 2019 / 2022

Presented at the Audit Committee meeting of: 1 October 2019

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

EXECUTIVE SUMMARY

Our Internal Audit Plan for 2019 / 2020 is presented for consideration by the Audit Committee.

The key points to note from our plan are:

2019 internal audit priorities: internal audit activity for 2019 / 2020 is based on analysing your corporate objectives, risk profile and assurance framework, as well as other factors affecting you in the year ahead including changes within the sector. Our detailed plan for 2019 / 2020 is included at section one.

The internal audit priorities have been discussed and agreed with the following individuals of the College:

- Principal;
- Head of Finance; and
- Audit Committee.

Level of resource: The level of resource required to deliver the plan is consistent with our tender proposal with the agreement made upon our appointment.

Core assurance: the key priorities and changes within the College during the period have been reflected within the proposed audit coverage for 2019 / 2020 and beyond. During the development of the internal audit plan the following key areas at the College were discussed:

Financial sustainability

The College has received its outcome agreement from the Scottish Funding Council for 2019 / 2020 that remains at a flat £9,000,000.

The College's staff costs represent 80% of its expenditure and this is currently under review by the College's management team.

A key issue for the sector is financial sustainability and the Scottish Funding Council now requests a financial forecast over a five year period (2018 / 2019 to 2023 / 2024). As part of this forecasting process, the College has identified an operating deficit of circa £700,000 by the end of 2023 / 2024. The College is in the process of identify financial efficiencies, so a balanced budget is achieved.

Capital

The College is currently building a STEM centre at both its Dumfries and Stranraer campuses. This is funded by the South of Scotland Economic Partnership and is currently on budget and on schedule to open at the start of the academic year.

Commercial activity

The College's commercial arm, Complete Training Solutions (CTS), income generation targets are under review and will be increased to reduce the College's reliance on Scottish Funding Council funding.

Risk register

The College has revised the format of its risk register and further revisions are planned for 2019 / 2020. As part of the discussions held with the Principal and Head of Finance the key risks facing the College were discussed.

CONTENTS

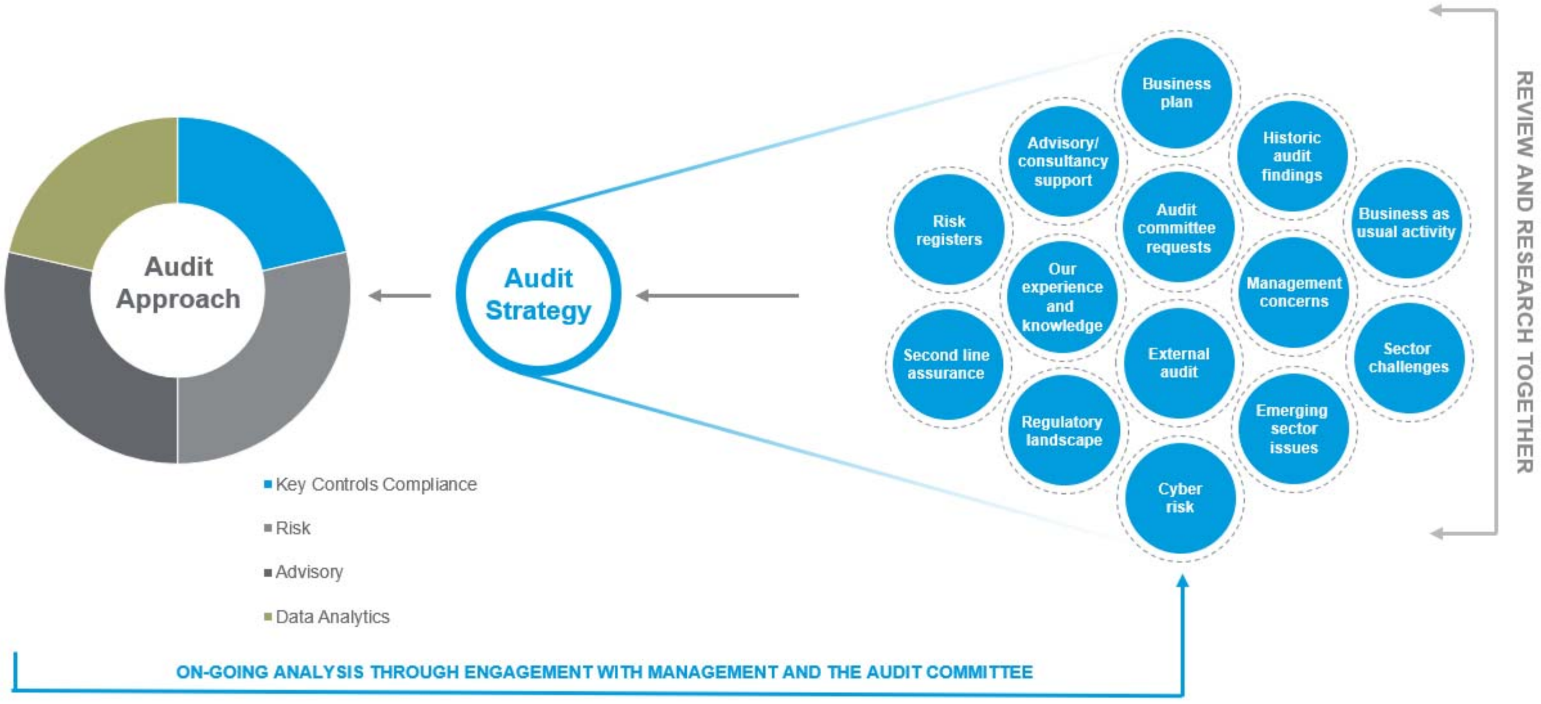
1. YOUR INTERNAL AUDIT PLAN 2019 / 2020

Our approach to developing your internal audit plan is based on analysing your corporate objectives, risk profile and assurance framework as well as other, factors affecting Dumfries and Galloway College in the year ahead, including changes within the sector.

Risk management processes

We have evaluated your risk management processes and consider that we can place reliance on your risk registers / assurance framework to inform the internal audit strategy. We have used various sources of information (see Figure A below) and discussed priorities for internal audit coverage with senior management and the Audit Committee

Figure A: Audit considerations – sources considered when developing the Internal Audit Strategy.



Based on our understanding of the College, the information provided to us by stakeholders, and the regulatory requirements, we have developed an annual internal plan for the coming year and a high level strategic plan (see section two and appendix B for full details).

2. INTERNAL AUDIT PLAN 2019 / 2020

The table below shows each of the reviews that we propose to undertake as part of the internal audit plan for 2019 / 2020. The table details the strategic risks which may warrant internal audit coverage. This review of your risks allows us to ensure that the proposed plan will meet the College's assurance needs for the forthcoming and future years. As well as assignments designed to provide assurance or advisory input around specific risks, the strategy also includes: time for tracking the implementation of actions and an audit management allocation.

Objective of the review (Strategic risk)	Fee (Days)	Proposed timing	Proposed Audit Committee
Staff Development *(Risk 3.1) Legal actions, serious accident, incident or civil / criminal breach.* This review will consider the staff development programme in place for mandatory and non-mandatory courses, and the linkages to staff roles and responsibilities.	6 days / £2,820	Week commencing 25 November 2019	February 2020
Marketing *(Risk 3.2) Reputational Risk – Loss of reputation with key stakeholders.* This review will consider whether the College has robust systems in place to ensure that value for money is achieved in regard to its marketing activities and use of resources in this area, and is clearly aligned to the delivery of the College's strategic objectives. We will specifically consider the use of social media including how it can be used going forward to promote the College.	8 days / £3,760	Week commencing 2 December 2019	February 2020
Core Assurance			
Credit Guidance Review of the Scottish Funding Council's Credit Guidance to ensure all income due to the College is maximised. We will also consider the wider curriculum planning process.	6 days / £2,820	Week commencing 30 March 2020	May 2020
FES Return An annual review of the College's FES return which has been prepared by the College under the 'Credits' Guidance. This audit will examine the procedures and controls relevant to the collection and recording of student data. Our review will evaluate the adequacy of these controls in ensuring the accuracy of the data. It will also include examination, on a test basis, of evidence relevant to the figures recorded in the student data returns.	6 days / £2,820	Week commencing 9 September 2019	November 2019
Student Support Fund Our review will examine the books and records of the College, including evidence of checks of five per cent of applications and payments, with a minimum sample size of five students.	6 days / £2,820	Week commencing 26 August 2019	November 2019

Objective of the review (Strategic risk)	Fee (Days)	Proposed timing	Proposed Audit Committee
Key Financial Controls: Asset Management Key financial control review considering the management and accounting of College capitalised assets. This review will also consider the allocation and tracking of assets identified as desirable.	5 days / £2,350	Week commencing 10 February 2020	May 2020
Other Internal Audit Activity			
Follow Up of Previous Internal Audit Management Actions To meet internal auditing standards, and to provide assurance on action taken to address recommendations previously agreed by management.	2 days / £940	Week commencing 10 February 2020	May 2020
Management This will include: • Annual planning; • Preparation for, and attendance at, the Audit Committee; • Regular liaison and progress updates; • Liaison with external audit and other assurance providers; and • Preparation of the annual opinion.	5 days / £2,350	Throughout the year	-
Total	44 days / £20,680		

A detailed planning process will be completed for each review, and the final scope will be documented in an assignment planning sheet. This will be issued to the key stakeholders for each review.

2.1 Working with other assurance providers

The Audit Committee is reminded that internal audit is only one source of assurance and through the delivery of our plan we will not, and do not, seek to cover all risks and processes within the College.

We will however continue to work closely with other assurance providers, such and external audit to ensure that duplication is minimised, and a suitable breadth of assurance obtained.

APPENDIX A: YOUR INTERNAL AUDIT SERVICE

Your internal audit service is provided by RSM Risk Assurance Services LLP. The team will be led by Rob Barnett as your Head of Internal Audit, supported by Philip Church as your Client Manager.

Fees

Our fee to deliver the plan is in line with our tender proposal and detailed in section two of this report.

Core team

The delivery of the 2019 / 2020 audit plan will be based around a core team. However, we will complement the team with additional specialist skills where required.

Conformance with internal auditing standards

RSM affirms that our internal audit services are designed to conform to the Public Sector Internal Audit Standards (PSIAS).

Under PSIAS, internal audit services are required to have an external quality assessment every five years. Our risk assurance service line commissioned an external independent review of our internal audit services in 2016 to provide assurance whether our approach meets the requirements of the International Professional Practices Framework (IPPF) published by the Global Institute of Internal Auditors (IIA) on which PSIAS is based.

The external review concluded that ""there is a robust approach to the annual and assignment planning processes and the documentation reviewed was thorough in both terms of reports provided to audit committee and the supporting working papers." RSM was found to have an excellent level of conformance with the IIA's professional standards.

The risk assurance service line has in place a quality assurance and improvement programme to ensure continuous improvement of our internal audit services. Resulting from the programme, there are no areas which we believe warrant flagging to your attention as impacting on the quality of the service we provide to you.

Conflicts of interest

We are not aware of any relationships that may affect the independence and objectivity of the team, and which are required to be disclosed under internal auditing standards.

APPENDIX B: INTERNAL AUDIT STRATEGY 2019 / 2020

The table below shows an overview of the audit coverage to be provided through RSM's delivery of the internal audit strategy. This has been derived from the process outlined in Section 1 above, as well as our own view of the risks facing the sector as a whole.

Assurance Provided	
🟥	Red - Minimal Assurance / Poor Progress
🟧	Amber/red - Partial Assurance / Little Progress
🟨	Amber/green - Reasonable Assurance / Reasonable Progress
🟩	Green - Substantial Assurance / Good Progress
⬛	Advisory / AUP
🟦	IDEA

	Internal Audit – Third Line of Assurance (Independent review / assurance)					
Audit Area	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22
Strategic risks						
(Risk 2.2) Failure to achieve institutional sustainability			🟩 Financial Planning / Forecasting			✓
(Risk 3.1) Legal actions; serious accident; incident or civil/criminal breach.			🟨 Health and Safety	✓		✓
(Risk 3.2) Reputational Risk – Loss of reputation with key stakeholders.	🟨 Marketing and Communication			✓		
(Risk 3.3) Disasters – e.g. Fire, MIS Failure, Failure of Emergency Procedures.					✓	
(Risk 3.4) Failure to meet Prevent and related obligations	🟩 Safeguarding including the Prevent Agenda					

Assurance Provided	
🟥	Red - Minimal Assurance / Poor Progress
🟧	Amber/red - Partial Assurance / Little Progress
🟨	Amber/green - Reasonable Assurance / Reasonable Progress
🟩	Green - Substantial Assurance / Good Progress
⬛	Advisory / AUP
🟦	IDEA

Internal Audit – Third Line of Assurance

(Independent review / assurance)

Audit Area	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22
(Risk 3.7) Breach of ICT/Cyber security.	🟨 IT Cyber Security	⬛ GDPR				
(Risk 3.9) Failure to reach aspirational standards in learning, teaching and service delivery						✓
(Risk 3.10) Failure to achieve/maintain compliance arrangements, e.g. contracts; awarding bodies; audit.			🟨 Health and Safety			
Core Assurance						
Income Generation	🟩	🟨 Complete Training Solutions			✓	
Student Journey		🟨				
Equality and Diversity			🟩			
Estates	🟨 Reactive Maintenance					✓
Human Resources Management		🟨 Sickness Absence		✓		

Assurance Provided	
🟥	Red - Minimal Assurance / Poor Progress
🟧	Amber/red - Partial Assurance / Little Progress
🟨	Amber/green - Reasonable Assurance / Reasonable Progress
🟩	Green - Substantial Assurance / Good Progress
▨	Advisory / AUP
🟦	IDEA

	Internal Audit – Third Line of Assurance (Independent review / assurance)					
Audit Area	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22
Key Financial Controls		🟨 Procurement	🟨 Creditors	✓	✓	
FES Return	🟩	🟩	🟩	✓	✓	✓
Student Support Fund	🟩	🟨	🟩	✓	✓	✓
Follow Up of Previous Internal Audit Management Actions	🟨	🟨	🟨	✓	✓	✓

APPENDIX C: INTERNAL AUDIT CHARTER

Need for the charter

This charter establishes the purpose, authority and responsibilities for the internal audit service for Dumfries and Galloway College. The establishment of a charter is a requirement of the Public Sector Internal Audit Standards (PSIAS) and approval of the charter is the responsibility of the Audit Committee.

The internal audit service is provided by RSM Risk Assurance Services LLP ("RSM").

We plan and perform our internal audit work with a view to reviewing and evaluating the risk management, control and governance arrangements that the College has in place, focusing in particular on how these arrangements help you to achieve its objectives. The PSIAS encompass the mandatory elements of the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) as follows:

- Core principles for the professional practice of internal auditing;
- Definition of internal auditing;
- Code of ethics; and
- The Standards.

Mission of internal audit

As set out in the PSIAS, the mission articulates what internal audit aspires to accomplish within an organisation. Its place in the IPPF is deliberate, demonstrating how practitioners should leverage the entire framework to facilitate their ability to achieve the mission.

> *"To enhance and protect organisational value by providing risk-based and objective assurance, advice and insight".*

Independence and ethics

To provide for the independence of internal audit, its personnel report directly to the Rob Barnett (acting as your Head of Internal Audit). The independence of RSM is assured by the internal audit service reporting to the Principal, with further reporting lines to the Head of Finance.

The head of internal audit has unrestricted access to the Chair of Audit Committee to whom all significant concerns relating to the adequacy and effectiveness of risk management activities, internal control and governance are reported.

Conflicts of interest may arise where RSM provides services other than internal audit to Dumfries and Galloway College. Steps will be taken to avoid or manage transparently and openly such conflicts of interest so that there is no real or perceived threat or impairment to independence in providing the internal audit service. If a potential conflict arises through the provision of other services, disclosure will be reported to the Audit Committee. The nature of the disclosure will depend upon the potential impairment and it is important that our role does not appear to be compromised in reporting the matter to the Audit Committee. Equally we do not want the College to be deprived of wider RSM expertise and will therefore raise awareness without compromising our independence.

Responsibilities

In providing your outsourced internal audit service, RSM has a responsibility to:

- Develop a flexible and risk based internal audit strategy with more detailed annual audit plans. The plan will be submitted to the audit committee for review and approval each year before work commences on delivery of that plan.
- Implement the internal audit plan as approved, including any additional tasks requested by management and the Audit Committee.
- Ensure the internal audit team consists of professional audit staff with sufficient knowledge, skills, and experience.
- Establish a quality assurance and improvement program to ensure the quality and effective operation of internal audit activities.
- Perform advisory activities where appropriate, beyond internal audit’s assurance services, to assist management in meeting its objectives.
- Bring a systematic disciplined approach to evaluate and report on the effectiveness of risk management, internal control and governance processes.
- Highlight control weaknesses and required associated improvements together with corrective action recommended to management based on an acceptable and practicable timeframe.
- Undertake follow up reviews to ensure management has implemented agreed internal control improvements within specified and agreed timeframes.
- Report regularly to the Audit Committee to demonstrate the performance of the internal audit service.

For clarity, we have included the definition of ‘internal audit’, ‘senior management’ and ‘board’.

- Internal audit: a department, division, team of consultant, or other practitioner (s) that provides independent, objective assurance and consulting services designed to add value and improve an organisation’s operations. The internal audit activity helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.
- Senior management: who are the team of individuals at the highest level of organisational management who have the day-to-day responsibilities for managing the organisation.

- Board: the highest-level governing body charged with the responsibility to direct and/or oversee the organisation's activities and hold organisational management accountable. Furthermore, "board" may refer to a committee or another body to which the governing body has delegated certain functions (e.g. an audit committee).

Client care standards

In delivering our services we require full cooperation from key stakeholders and relevant business areas to ensure a smooth delivery of the plan. We proposed the following KPIs for monitoring the delivery of the internal audit service:

- Discussions with senior staff at the client take place to confirm the scope four weeks before the agreed audit start date.
- Key information such as: the draft assignment planning sheet are issued by RSM to the key auditee four weeks before the agreed start date.
- The lead auditor to contact the client to confirm logistical arrangements at least 10 working days before the commencement of the audit fieldwork to confirm practical arrangements, appointments, debrief date etc.
- Fieldwork takes place on agreed dates with key issues flagged up immediately.
- A debrief meeting will be held with audit sponsor at the end of fieldwork or within a reasonable time frame.
- Draft reports will be issued within 10 working days of the debrief meeting and will be issued by RSM to the agreed distribution list / Sharefile.
- Management responses to the draft report should be submitted to RSM.
- Within three working days of receipt of client responses the final report will be issued by RSM to the assignment sponsor and any other agreed recipients of the report.

Authority

The internal audit team is authorised to:

- Have unrestricted access to all functions, records, property and personnel which it considers necessary to fulfil its function.
- Have full and free access to the Audit Committee.
- Allocate resources, set timeframes, define review areas, develop scopes of work and apply techniques to accomplish the overall internal audit objectives.
- Obtain the required assistance from personnel within the College where audits will be performed, including other specialised services from within or outside the College.

The Head of Internal Audit and internal audit staff are not authorised to:

- Perform any operational duties associated with the College.
- Initiate or approve accounting transactions on behalf of the College.
- Direct the activities of any employee not employed by RSM unless specifically seconded to internal audit.

Reporting

An assignment report will be issued following each internal audit assignment. The report will be issued in draft for comment by management, and then issued as a final report to management, with the executive summary being provided to the Audit Committee. The final report will contain an action plan agreed with management to address any weaknesses identified by internal audit.

The internal audit service will issue progress reports to the Audit Committee and management summarising outcomes of audit activities, including follow up reviews.

As your internal audit provider, the assignment opinions that RSM provides the College during the year are part of the framework of assurances that assist the board in taking decisions and managing its risks.

As the provider of the internal audit service we are required to provide an annual opinion on the adequacy and effectiveness of the College’s governance, risk management, control and value for money arrangements. In giving our opinion it should be noted that assurance can never be absolute. The most that the internal audit service can provide to the board is a reasonable assurance that there are no major weaknesses in risk management, governance and control processes. The annual opinion will be provided to the College by RSM Risk Assurance Services LLP at the financial year end. The results of internal audit reviews, and the annual opinion, should be used by management and the Board to inform the College’s annual governance statement.

Data protection

Internal audit files need to include sufficient, reliable, relevant and useful evidence in order to support our findings and conclusions. Personal data is not shared with unauthorised persons unless there is a valid and lawful requirement to do so. We are authorised as providers of internal audit services to our clients (through the firm’s terms of business and our engagement letter) to have access to all necessary documentation from our clients needed to carry out our duties.

Quality Assurance and Improvement

As your external service provider of internal audit services, we have the responsibility for maintaining an effective internal audit activity. Under the standards, internal audit services are required to have an external quality assessment every five years. In addition to this, we also have in place an internal quality assurance and improvement programme, led by a dedicated team who undertake these reviews. This ensures continuous improvement of our internal audit services.

Any areas which we believe warrant bringing to your attention, which may have the potential to have an impact on the quality of the service we provide to you, will be raised in our progress reports to the Audit Committee.

Fraud

The Audit Committee recognises that management is responsible for controls to reasonably prevent and detect fraud. Furthermore, the Audit Committee recognises that internal audit is not responsible for identifying fraud; however internal audit will be aware of the risk of fraud when planning and undertaking any assignments.

Approval of the internal audit charter

By approving this document, the internal audit strategy, the Audit Committee is also approving the internal audit charter.

FOR FURTHER INFORMATION CONTACT

Rob Barnett
Head of Internal Audit

RSM Risk Assurance Services LLP
1 St. James Gate, Newcastle Upon Tyne, NE1 4AD

T: +44 (0)191 2557000 | **M:** +44 (0)7809 560103 | **W:** www.rsmuk.com

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **Dumfries and Galloway College**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

DUMFRIES AND GALLOWAY COLLEGE

Annual Internal Audit Report and Opinion - Year ended 31 July 2019

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.

CONTENTS

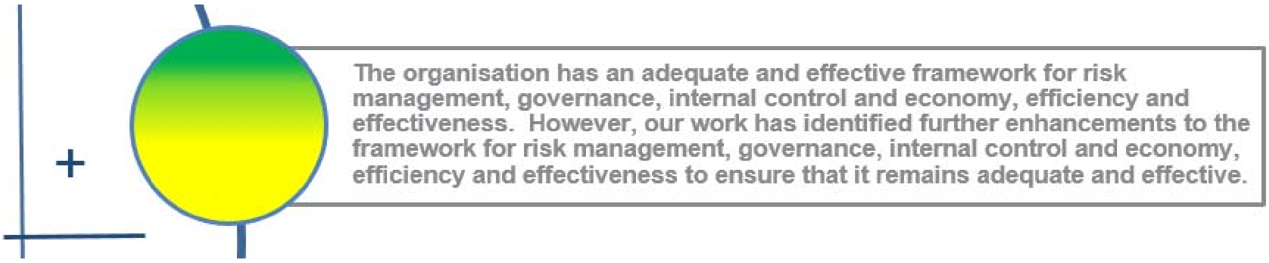
1 THE ANNUAL INTERNAL AUDIT OPINION

This report provides an annual internal audit opinion, based upon and limited to the work performed, on the overall adequacy and effectiveness of the College's risk management, control, governance and value for money processes. The opinion should contribute to the College's annual governance reporting.

1.1 The opinion

For the 12 months ended 31 July 2019, the Head of Internal Audit Opinion for Dumfries and Galloway College is as follows:

Head of Internal Audit Opinion 2018/19



The organisation has an adequate and effective framework for risk management, governance, internal control and economy, efficiency and effectiveness. However, our work has identified further enhancements to the framework for risk management, governance, internal control and economy, efficiency and effectiveness to ensure that it remains adequate and effective.

Please see appendix A for the full range of annual opinions available to us in preparing this report and opinion.

1.2 Scope and limitations of our work

The formation of our opinion is achieved through a risk-based plan of work, agreed with management and approved by the Audit Committee, our opinion is subject to inherent limitations, as detailed below:

- the opinion does not imply that internal audit has reviewed all risks and assurances relating to the College;

- the opinion is substantially derived from the conduct of a risk-based plan generated from a robust and organisation-led assurance framework. As such, the assurance framework is one component that the Board takes into account in completing its annual governance reporting;

- the opinion is based on the findings and conclusions from the work undertaken, the scope of which has been agreed with management;

- the opinion is based on the testing we have undertaken, which was limited to the area being audited, as detailed in the agreed audit report;

- where strong levels of control have been identified, there are still instances where these may not always be effective. This may be due to human error, incorrect management judgement, management override, controls being by-passed or a reduction in compliance;

- due to the limited scope of our audits, there may be weaknesses in the control system which we are not aware of, or which were not brought to our attention; and
- it remains management's responsibility to develop and maintain a sound system of risk management, internal control and governance, and for the prevention and detection of errors, loss or fraud. The work of internal audit is not and should not be seen as a substitute for management responsibility around the design and effective operation of these systems.

1.3 Factors and findings which have informed our opinion

Based on the work we have undertaken on the systems of internal control, governance, risk management and value for money at the College, our opinion has been informed by the following:

Governance

We did not perform a specific governance review at the College, however we confirmed sufficient reporting had been undertaken in the following areas: Financial Planning and Forecasting and Equality and Diversity.

We concluded that the governance arrangements in place were adequate and effective.

Risk Management

We did not undertake a specific review of risk management within the 2018/19 internal audit plan. We have however attended all Audit Committee meetings throughout the year and confirmed the College's risk management arrangements continued to operate effectively and were adequately reported and scrutinised by committee members, with regular updates provided and copies of the risk register shared and reviewed.

Our risk management opinion is informed by the assessment of the risk mitigation procedures undertaken in the areas covered by our risk-based reviews in the following areas:

- Financial Forecasting and Planning;
- Student Activity Data; and
- Student Support Funds.

Our student funding reviews, Student Activity Data and Student Support Funds, concluded that **substantial assurance** could be taken that the controls were both adequately designed and applied consistently. We raised two medium and two low management actions across both areas to improve the application of the College's control framework

Financial Forecasting and Planning continues to be a key focus for the Scottish Funding Council (SFC), and we confirmed the College has an appropriate control framework in place that resulted in a **substantial assurance** opinion. We did raise two medium management actions to improve the financial forecasting framework in place at the College.

Control

We undertook six audits of the control environment that resulted in formal assurance opinions. These six reviews concluded that two **reasonable (positive) assurance** and four **substantial (positive) assurance opinions** could be taken. We identified the College had established control frameworks in place for a number of the audits undertaken.

Furthermore, the implementation of agreed management actions raised during the course of the year are an important contributing factor when assessing the overall opinion on control. We have performed a follow up and during the year which concluded in **reasonable progress** being made towards the implementation of those actions.

Value for Money

The Scottish Further and Higher Education Funding Council requires internal audit to provide an appraisal each year on the College's arrangements for value for money.

We have considered the College's creditor payments process and undertook substantive testing to confirm its application, this resulted in a **reasonable assurance** opinion.

A summary of internal audit work undertaken, and the resulting conclusions, is provided at appendix B.

1.4 Topics judged relevant for consideration as part of your annual governance reporting

Colleges are required to include a Statement of Corporate Governance and Internal Control within their financial statements. As your internal audit provider, the assignment opinions and advisory reviews that we undertake and report on during the year are part of the framework of assurances that assist the Board (through the audit committee) to prepare an informed statement and provide the opinions required.

Our overall opinion may be used by the Board in the preparation of the 2018/19 Statement.

2 THE BASIS OF OUR INTERNAL AUDIT OPINION

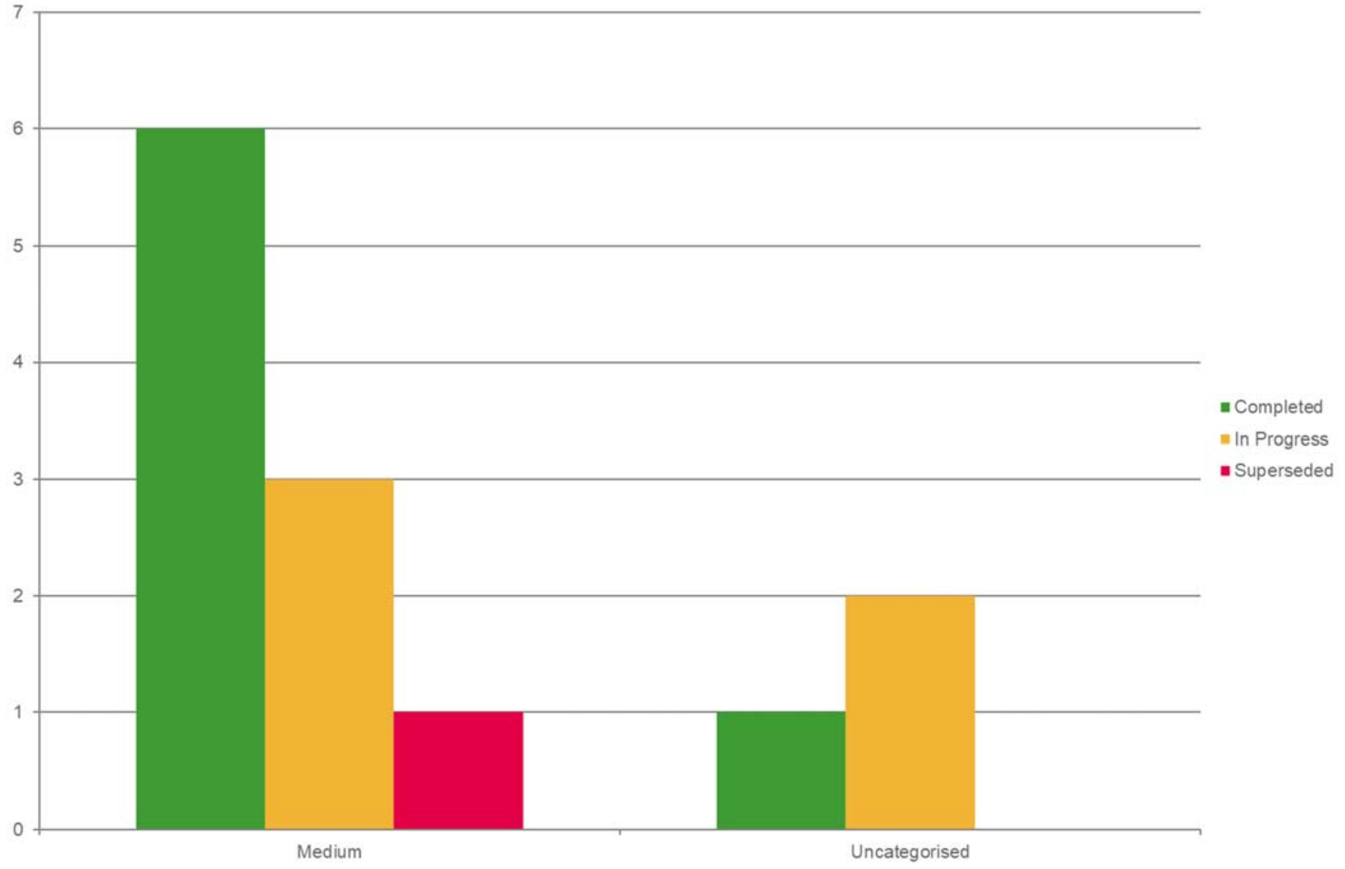
As well as those headlines discussed at paragraph 1.3, the following areas have helped to inform our opinion. A summary of internal audit work undertaken, and the resulting conclusions, is provided at appendix B.

2.1 Acceptance of internal audit management actions

Management has agreed actions to address all of the findings reported by the internal audit service during 2018/19.

2.2 Implementation of internal audit management actions

Our follow up of the actions agreed to address previous years' internal audit findings shows that the College had made **reasonable progress** in implementing the agreed actions.



A summary of internal audit work undertaken, and the resulting conclusions, is provided at appendix B.

2.3 Working with other assurance providers

In forming our opinion we have not placed any direct reliance on other assurance providers.

3 OUR PERFORMANCE

3.1 Conflicts of interest

RSM has not undertaken any work or activity during 2018/19 that would lead us to declare any conflict of interests.

3.2 Conformance with internal auditing standards

RSM affirms that our internal audit services are designed to conform to the International Standards for the Professional Practice of Internal Auditing and the International Professional Practices Framework (IPPF) as published by the Global Institute of Internal Auditors (IIA).

Under the standards, internal audit services are required to have an external quality assessment every five years. Our Risk Assurance service line commissioned an external independent review of our internal audit services in 2016 to provide assurance whether our approach meets the requirements of the IPPF.

The external review concluded that “there is a robust approach to the annual and assignment planning processes and the documentation reviewed was thorough in both terms of reports provided to audit committee and the supporting working papers.” RSM was found to have an excellent level of conformance with the IIA’s professional standards.

3.5 Performance indicators

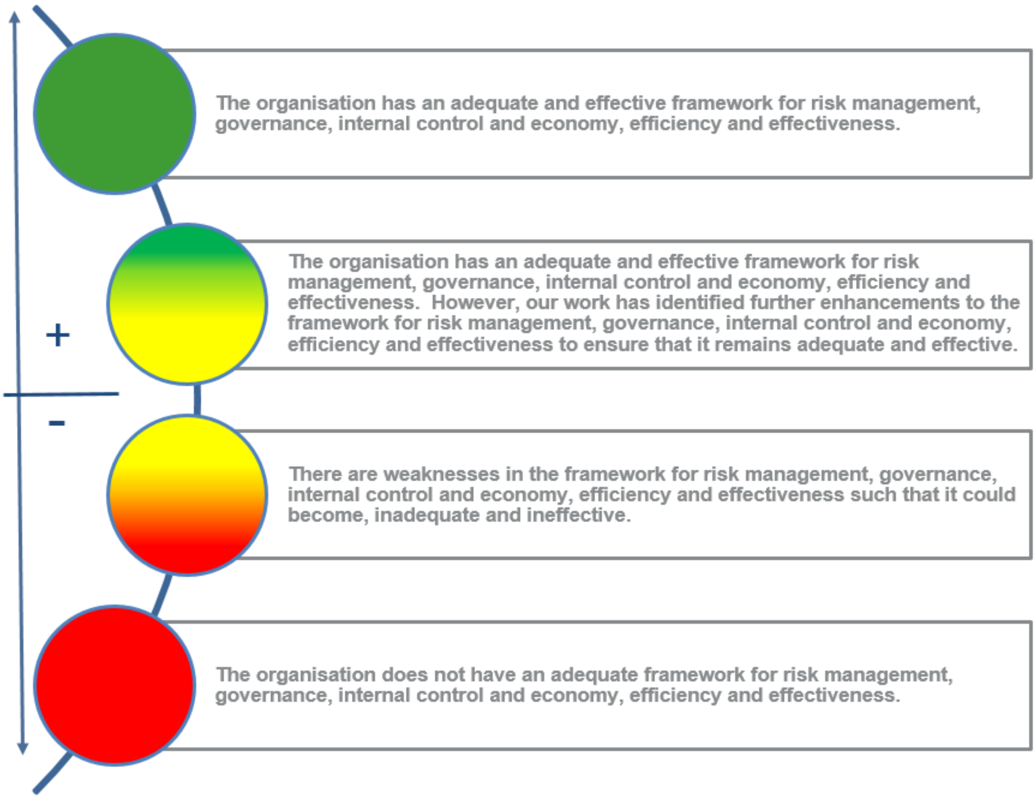
A number of performance indicators were agreed with the Audit Committee. Our performance against those indicators is as follows:

Delivery			**Quality**		
	Target	**Actual**		**Target**	**Actual**
Draft reports issued within 10 working days of debrief meeting	10 working days	*10 working days (average)*	Conformance with PSIAS and IIA Standards	Yes	*Yes*
			Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	*As and when required*
Final report issued within 3 working days of management response	3 working days	*1 working day (average)*	% of staff with CCAB/CMIIA qualifications	>50%	*71%*
			Turnover rate of staff	<10%	*No staff turnover in 2018 / 2019*
			Response time for all general enquiries for assistance	2 working days	*2 working days (average)*
High and Medium recommendations followed up	Yes	*Yes*	Response for emergencies and potential fraud	1 working day	*N/A*

APPENDIX A: ANNUAL OPINIONS

The following shows the full range of opinions available to us within our internal audit methodology to provide you with context regarding your annual internal audit opinion.

Annual opinions



The organisation has an adequate and effective framework for risk management, governance, internal control and economy, efficiency and effectiveness.

The organisation has an adequate and effective framework for risk management, governance, internal control and economy, efficiency and effectiveness. However, our work has identified further enhancements to the framework for risk management, governance, internal control and economy, efficiency and effectiveness to ensure that it remains adequate and effective.

There are weaknesses in the framework for risk management, governance, internal control and economy, efficiency and effectiveness such that it could become, inadequate and ineffective.

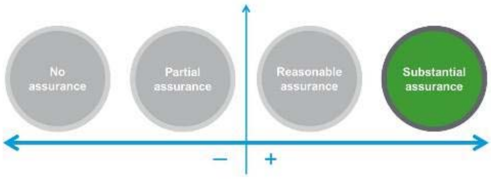
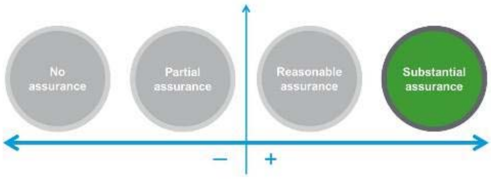
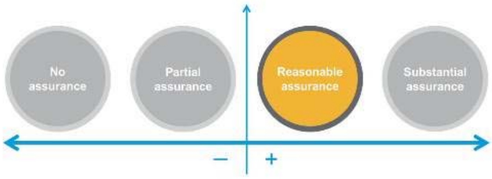
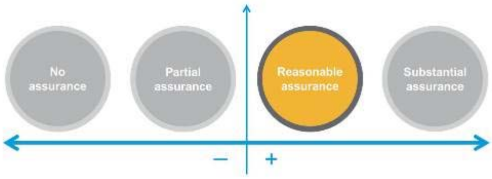
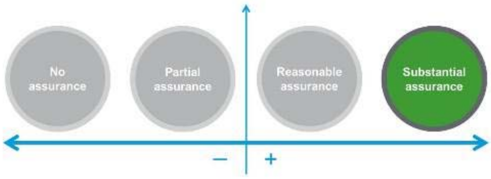
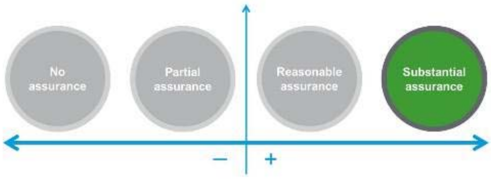
The organisation does not have an adequate framework for risk management, governance, internal control and economy, efficiency and effectiveness.

Factors influencing our opinion

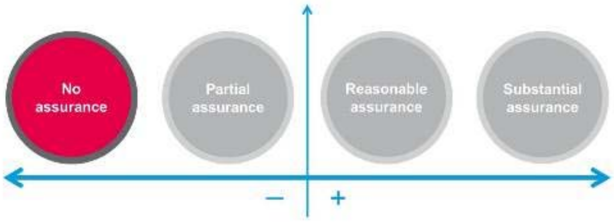
The factors which are considered when influencing our opinion include:

- inherent risk in the area being audited;
- limitations in the individual audit assignment reports;
- the adequacy and effectiveness of the risk management, governance, control and/or economy, efficiency and effectiveness framework;
- the findings from any advisory work undertaken;
- the impact of weakness identified;
- the level of risk exposure; and
- the response to management actions raised and timeliness of actions taken.

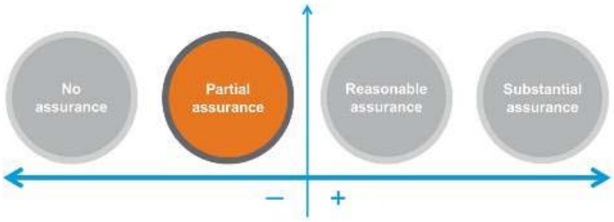
APPENDIX B: SUMMARY OF INTERNAL AUDIT WORK COMPLETED 2018/19

Assignment	Assurance level	Actions agreed		
		L	M	H
Student Support Funds		2	0	0
Student Activity Data		0	2	0
Health and Safety		2	2	0
Creditor Payments		2	4	0
Follow Up	Reasonable Progress	1	2	0
		2 uncategorised management actions (GDPR)		
Equality and Diversity		3	1	0
Financial Planning and Forecasting		0	2	0

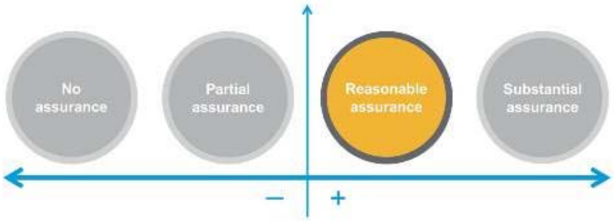
We use the following levels of opinion classification within our internal audit reports. Reflecting the level of assurance the Board can take:



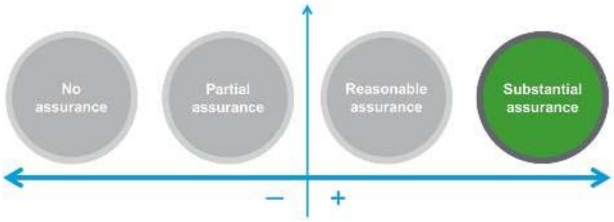
Taking account of the issues identified, the Board **cannot take assurance** that the controls upon which the College relies to manage this risk are suitably designed, consistently applied or effective.
Urgent action is needed to strengthen the control framework to manage the identified risk.



Taking account of the issues identified, the Board can take **partial assurance** that the controls to manage this risk are suitably designed and consistently applied.
Action is needed to strengthen the control framework to manage the identified risk.



Taking account of the issues identified, the Board can take **reasonable assurance** that the controls in place to manage this risk are suitably designed and consistently applied.
However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.



Taking account of the issues identified, the Board can take **substantial assurance** that the controls upon which the College relies to manage the identified risk are suitably designed, consistently applied and operating effectively.

FOR FURTHER INFORMATION CONTACT

Robert Barnett
RSM
1 St. James Gate,
Newcastle Upon Tyne,
NE1 4AD

T +44 191 255 7000
M +44 (0)7791237658
Robert.Barnett@rsmuk.com

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **Dumfries and Galloway College**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

Agenda Item No. 7.2
Audit 01.10.19

OUTSTANDING AUDIT RECOMMENDATIONS

- Review of Medium and High Risk Recommendations to be followed-up

Updated 20.08.19

		Number:	
KEY:	**Complete, to be included in Follow-up review**	12	🟩
	In progress	6	🟧
	Added to report from recent audit review	0	🟦
		18	

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
1	Feedback from external events to inform courses is not formally documented, and without an employment engagement strategy, the College may fail to engage with appropriate employers and be able to provide courses to them, resulting in a missed opportunity for income.	Follow-Up 02.19	A documented employer engagement strategy will be developed	Revised to October '19	Vice Principal Learning and Skills	Employer Engagement Strategy has now been approved by the Learning & Teaching Committee, with the proviso that Milestones are added. L&T Committtee will be asked for their input.
2	The TSR system is capable of producing performance indicators; however, currently the performance indicators the system produces only show how many requests have been received and how many have been completed in a month. The performance indicators on the system are not used by the Estates team to monitor performance of completing reactive maintenance requests.	Follow-Up 02.19	We will discuss which key performance indicators the Estates team should have in place and what the target level is for each of these indicators. The Maintenance Foreman will review and discuss KPIs with janitorial staff on a monthly basis, to identify the reasons why any KPIs have not been achieved and any areas they need to improve on as a team, and also to highlight what they are doing well. An update on reactive maintenance KPIs will be provided to the Finance and General Purposes Committee as part of the general performance update on estates and facilities.	March '19	Facilities Manager	KPI's now in place, to run alongside of SLA. TSR Performance is now included as a standing item in monthly Team catch-ups, and is being minuted, with a monthly report sent to the Head of Corporate Services.
3	There is no central point for induction checklists to be uploaded to, these are retained by the individual tutors on individual student files. Without a central point for the storage of induction checklists, there is a risk that the College is unable to evidence that inductions have taken place.	Follow-Up 02.19	All induction checklists will be uploaded to the Adminnet system.	July '19	Heads of Curriculum	Online Induction Checklists content has been reviewed and checklists have now been implemented across all curriculum areas in time for 2019-20 enrolement.

OUTSTANDING AUDIT RECOMMENDATIONS

- Review of Medium and High Risk Recommendations to be followed-up

Audit 01.10.19

Updated 20.08.19

		Number:	
KEY:	**Complete, to be included in Follow-up review**	12	🟩
	In progress	6	🟧
	Added to report from recent audit review	0	🟦
		18	

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
4	ICT management will ensure that software updates are applied consistently to IT assets such as servers and desktops in accordance with the patch procedure.	Follow-Up 04.18	ICT management will consistently apply the Windows 10 program update to all of the College's desktops.	Revised date - October '19	IT Manager	All physical PC's have now been upgraded to Windows 10. There is a delay in upgrading the 'virtual machines' which the IT team are working to resolve.
5	Procedures for dealing with student withdrawals - the required date for attendance had been input incorrectly on the SITS system.	Student Activity Data 09.18	The College will ensure that the required attendance date is correctly calculated on the SITS calculator	November '18	Business Systems Manager / Student Records Manager	All now fully implemented/ dates all now checked
6	The required date for part-time students had been calculated based on the student being full-time - without accurate required attendance dates, there is a risk that students could be included in the credit return without attending 25% of their part-time course.	Student Activity Data 09.18	The College will ensure that the required attendance date is correctly calculated on the SITS calculator for all part-time courses. The Student Records Manager will conduct a manual calculation of part-time courses required attendance dates to ensure they are accurate. This check will be conducted quarterly	November '18	Business Systems Manager / Student Records Manager	All now fully implemented/ dates all now checked
7	For staff working in specific areas e.g. engineering and construction, specific health and safety training may be required to use certain machinery.	Health & Safety 11.18	Heads of Department will be requested to produce lists of equipment and machinery within their department which requires additional safety training as well as identifying the staff who operate this machinery within their role. Also Health and safety audits will now include a review of these equipment lists and a review of training records against these lists to ensure staff operating machinery are appropriately trained.	March '19	Head of Corporate Services	A new internal checklist has been revised to include the recommendations from the audit. This has been issued to all managers for awareness before any checks are carried out.

OUTSTANDING AUDIT RECOMMENDATIONS **Audit 01.10.19**

- Review of Medium and High Risk Recommendations to be followed-up

Updated 20.08.19

		Number:	
KEY:	**Complete, to be included in Follow-up review**	12	🟩
	In progress	6	🟧
	Added to report from recent audit review	0	🟦
		18	

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
8	Roles and responsibilities for RIDDOR reporting are clearly defined.	Health & Safety 11.18	The Health and Safety Policy is due to be updated shortly by the newly formed Health and Safety Committee, RIDDOR requirements and guidance will be included as part of this review.	February '19	Head of Corporate Services	The policy has been revised with the inclusion of the wording for RIDDOR.
9	Health and safety is monitored at the Health and Safety Committee where information regarding statistics, trends and other relevant health and safety issues are discussed	Health & Safety 11.18	A new Health and Safety Committee is being recruited and will meet on a quarterly basis. Its first meeting will develop a Terms of Reference and present to the Board for approval.	January '19	Head of Corporate Services	New members have come forward for the committee, and the first meeting was held in February.
10	Health and safety statistics, as well as details of compliance against legislation, are not reported at board level on a frequent basis.	Health & Safety 11.18	Health and safety will become a standing item on the monthly senior management team meeting where the Health and Safety Manager will present an update on key details relating to health and safety.	January '19	Head of Corporate Services	Now fully implemented/ included as a standing item on the CLT Agenda
11	We recommend that the College investigates the finance system capabilities and whether electronic journal authorisation of journals is possible. In whatever system is used, the College should ensure there is clear evidence of approval for all manual journals.	External Audit 11.18	We will liaise with our software provider to investigate if an approval procedure could be set up within the finance system. If that isn't possible we will include a manual check for authorisation of all journals as part of the monthly process.	November '18	Head of Finance	Civica have advised that this isn't possible using the finance software. A process has been set up using the Nominal ledger daybook and this will be carried out as part of the monthly accounts completion
12	The billing arrangements with UWS for staffing re-charges should be agreed in sufficient detail that the College is able to estimate the amount of income it will receive	External Audit 11.18	We will liaise with the University of the West of Scotland to establish a formal agreement for the teaching contract	Revised to October '19	Head of Finance	HoF is liaising with UWS to set up a Service Level Agreement
13	The College should complete the review of the Financial regulations and authorised signatory listing and ensure these are appropriately authorised by the Finance and General Purposes Committee.	External Audit 11.18	We will complete the update of the Financial Regulations and authorised signatories as per of the 2019-20 budget planning process.	Revised to June '19	Head of Finance	The Financial Regulations have now been updated
14	It was noted during out testing that an EIA had not been carried out on the Equality and Diversity Policy.	Equality and Diversity 02.19	The Equality and Diversity Officer will carry out an Equality Impact Assessment (EIA) on the Equality and Diversity Policy, update the policy with the date of the EIA and re-issue.	February '19	Equality and Diversity Officer	Now completed

OUTSTANDING AUDIT RECOMMENDATIONS **Audit 01.10.19**

- Review of Medium and High Risk Recommendations to be followed-up

Updated 20.08.19

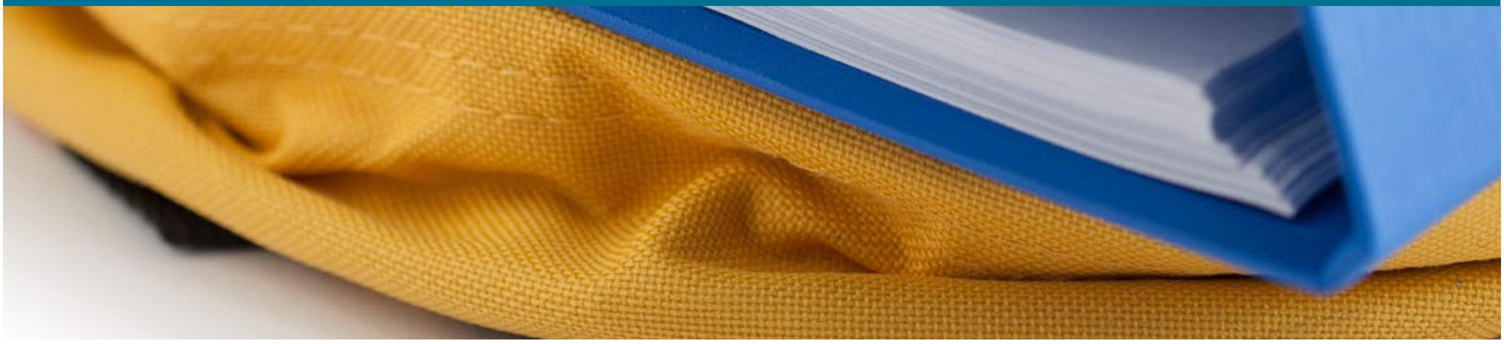
KEY:		Number:	
	Complete, to be included in Follow-up review	12	🟩
	In progress	6	🟧
	Added to report from recent audit review	0	🟦
		18	

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
15	We confirmed the Financial Regulations provide guidance on the general management of funds within the college; however, they do not provide full guidance on the administration of petty cash or credit cards. They do not stipulate that purchase orders should be issued in advance of ordering goods, only that they should be issued. We also found no reference to procurement legislation.	Creditor Payments 02.19	The Financial Regulations will be reviewed and updated, within them we will incorporate reference to procurement legislation, tendering processses and procedures for petty cash, use of credit cards and purchase orders	June '19	Head of Finance	The Financial Regulations have now been updated
16	Budgets can become overspent where goods are ordered without appropriate authorisation. The Purchase orders provide confirmation that the budget holder has sanctioned the purchase and there is sufficient budget to honour payment, and not all invoices are supported by a Purchase Order	Creditor Payments 02.19	Steps will be taken to put more suppliers on PECOS. Where a supplier is on PECOS the use of a purchase order cannot be avoided.	March '19	Head of Finance	A review of suppliers has been completed and additional suppliers are now being added to Pecos
17	Cash advances from the petty cash should be supported by documentary evidence and receipts, but these are not always chased up.	Creditor Payments 02.19	A form will be devised to record cash advances. This form will require the staff member to sign for the amounts given; and advise a payback date. The staff member will be required to return the balance of the cash advance along with all receipts to substantiate the expenditure. The Finance Department will monitor the return of the form, cash and receipts, and an annual breakdown of expenditure given to students in regards of cash shortfalls will be provided to the Finance and General Purposes Committee. A budget will be	March '19	Head of Finance	A form has been drafted and is now being used for any cash advances
18	A payment request form is completed and approved by the budget holder prior to any purchase being made. Credit cards are used for appropriate expenditure which cannot easily be made by another means of payment. Valid VAT receipts are retained to support all expenditure made via the credit card.	Creditor Payments 02.19	The budget holders will be reminded to ensure appropriate authorisation is given prior to making purchases via the credit card. The payment request form will be adapted so the requesting officer signs to confirm the credit card is being used because other method of payment is possible and that an appropriately authorised purchase order accompanies the request. The specimen signature list will be updated and reviewed at least annually.	February '19	Head of Finance	Forms updated on Adminnet. The Specimen Signature list has now been updated

Scotland's colleges 2019

AUDITOR GENERAL

Prepared by Audit Scotland
June 2019



Auditor General for Scotland

The Auditor General's role is to:

- appoint auditors to Scotland's central government and NHS bodies
- examine how public bodies spend public money
- help them to manage their finances to the highest standards
- check whether they achieve value for money.

The Auditor General is independent and reports to the Scottish Parliament on the performance of:

- directorates of the Scottish Government
- government agencies, eg the Scottish Prison Service, Historic Environment Scotland
- NHS bodies
- further education colleges
- Scottish Water
- NDPBs and others, eg Scottish Police Authority, Scottish Fire and Rescue Service.

You can find out more about the work of the Auditor General on our website:
www.audit-scotland.gov.uk/about-us/auditor-general

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively.

Contents

Audit team

The core audit team consisted of: Mark MacPherson, Mark McCabe, Yoshiko Gibo, Angus Brown and Sanya Ahmed, with support from other colleagues and under the direction of Angela Canning.

Links

PDF download

Web link

Key messages

1 The college sector reported a small, but improved, underlying financial surplus in 2017-18. Colleges are operating within an increasingly tight financial environment and the sector-wide position masks particular financial challenges for some colleges. The gap between colleges' income and expenditure is widening and this is forecast to continue, with 12 incorporated colleges forecasting recurring financial deficits by 2022-23.

2 Colleges face increasing cost pressures. The increase in Scottish Government revenue funding for 2019/20 covers only the additional costs of harmonising pay and conditions across the sector (excluding cost of living increases and increases in employers' pension contributions). Current Scottish Government capital funding falls short of the estimated costs of maintaining the college estate. The proportion of non-government income that colleges generate has reduced over time, and cash balances and money held by arm's-length foundations fell.

3 Student numbers increased, and the sector exceeded its learning activity targets. Over the past three years, colleges have been providing less learning to students aged 16-24 and more to students aged 25 and over. Colleges are widening access to disabled, ethnic minority and care-experienced students. After several years of increasing learning delivered to students from deprived areas, the proportion of learning delivered to this group fell slightly in 2017-18.

4 There is considerable variation across colleges in terms of student attainment and retention and those going on to positive destinations. Average attainment rates for students in full-time education have remained relatively static in recent years. The attainment rate for full-time further education, at 66 per cent, is some distance from the Scottish Funding Council's (SFC) target of 75 per cent by 2020-21. Attainment gaps still exist for students from the most deprived areas, students with disabilities and for care-experienced students.

5 There is scope for the SFC to work with individual colleges and their boards to improve financial planning and to achieve greater transparency in the sector's financial position. The SFC can also be more transparent in how it reports colleges' performance against outcome agreements and student satisfaction data. The SFC has agreed aspirational and stretching targets with colleges in their latest outcome agreements. Based on recent performance trends, achieving some of these targets will be very challenging for colleges.

Recommendations

Colleges should:

- agree their underlying financial position with the SFC prior to finalising their accounts (paragraph 5)
- improve data collection and response rates for student satisfaction and publish results (paragraphs 52–53)
- use *How good is our college?* effectively to drive improved performance and enhance the quality of service provision (paragraphs 55–57).

College boards and regional bodies should:

- agree medium-term financial plans that set out the mitigating actions to ensure their college's financial sustainability (paragraphs 17–19)
- submit agreed medium-term financial plans to the SFC along with financial forecast returns (FFRs) (paragraphs 17–19).

The SFC should:

- work with colleges to agree their underlying financial position prior to finalising their accounts (paragraph 5)
- require colleges to submit medium-term financial plans to support FFRs in assessing financial sustainability across the sector (paragraphs 17–19)
- publish college region performance against all outcome agreement measures (paragraph 44)
- publish good-quality student satisfaction data for every college (paragraph 52).

The SFC and Scottish Government should:

- agree and publish a medium-term capital investment strategy that sets out sector-wide priorities (paragraph 24)
- review whether targets for college provision and student outcomes, including for students from deprived areas, remain relevant and realistic, based on current performance trends (paragraph 31) (paragraphs 41–42)
- work with colleges to deliver the necessary improvements in performance to meet agreed outcome agreement targets (paragraph 45).

Part 1

Financial health

Key messages

1 The college sector reported a small, but improved, underlying financial surplus in 2017-18. Colleges are operating within an increasingly tight financial environment and the sector-wide position masks particular financial challenges for some colleges.

2 The Scottish Government has been providing colleges with real-terms increases in revenue funding since 2016/17. The most recent increase for 2019/20 covers only the additional cost of harmonising staff terms and conditions. Colleges also need to fund cost of living pay increases and any unfunded element of increases in employers' pension contributions. The proportion of non-government income, such as education contracts and other commercial income, has reduced. Colleges' ability to access other sources of funding, such as cash and arm's-length foundation (ALF) balances, is also reducing.

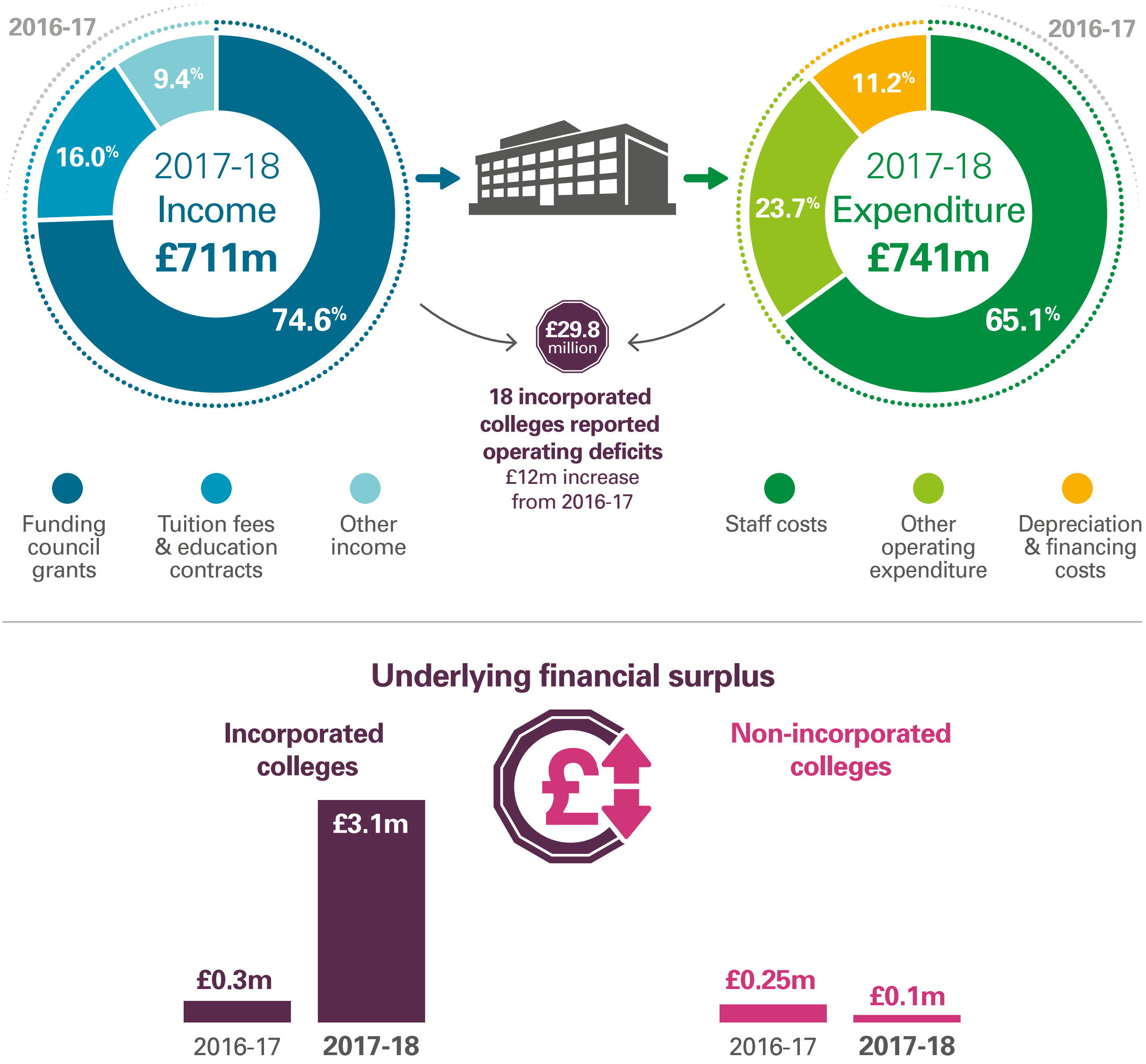
3 The gap between colleges' income and expenditure is widening. Twelve incorporated colleges were forecasting recurring financial deficits by 2022-23. At the time of their annual audits, ten of these were still to determine the specific actions needed to achieve financial sustainability.

4 Scottish Government capital funding falls short of what is needed to meet the estimated costs of maintaining the college estate. The Scottish Government is working with the Scottish Futures Trust and SFC to identify an appropriate revenue funding model for future investment in the college estate.

The underlying financial position for the college sector improved slightly in 2017-18, but the gap between income and expenditure is widening

1. Income remained unchanged across the sector in 2017-18 at £711 million. This represents a 1.9 per cent reduction in real terms from 2016-17. Scottish Government funding (provided through grants from the Scottish Funding Council) increased by 1.0 per cent in real terms. The proportion of income from other sources, such as education contracts and other commercial income, fell, meaning that colleges are increasingly dependent on Scottish Government funding (Exhibit 1, page 7).

Exhibit 1
Colleges have achieved an underlying surplus but the gap between income and expenditure is widening



Source: College accounts/SFC

2. Colleges' expenditure increased by £11.8 million (0.3 per cent in real terms) to £741 million in 2017-18, widening the gap between income and expenditure. As a result, the sector's operating deficit increased to £29.8 million. Eighteen of the 20 incorporated colleges reported operating deficits.

3. Adjusting the operating position for technical accounting factors that are beyond a college's immediate control, such as pensions and net depreciation, helps to provide a clearer picture of a college's short-term financial health. After such adjustments, incorporated colleges reported an underlying surplus of £3.1 million. While the underlying surplus is £2.8 million higher than in 2016-17, it represents a very small percentage of sector expenditure (0.4 per cent).

4. The overall underlying surplus for the six non-incorporated colleges is £0.1 million, equivalent to 0.4 per cent of their expenditure of £25.6 million and less than half the surplus in 2016-17 (£0.25 million).

5. In calculating and reporting their underlying operating positions, colleges continue to interpret the SFC's accounts direction inconsistently. While the differences between colleges' and the SFC's calculations are small overall (around £1.4 million), differences in individual college figures can be significant.

6. As public bodies, colleges are expected to operate with balanced budgets, but they are operating within an increasingly tight financial environment. The underlying positions of individual colleges are shown on (Exhibit 6, page 12), together with other indicators of financial health.

The latest increase in Scottish Government revenue funding is only enough to cover the costs of harmonising staff terms and conditions

7. Scottish Government revenue funding to the sector reduced in the period leading up to college reorganisation. Revenue funding for the sector has increased year-on-year since 2016/17 in real terms, mainly due to the Scottish Government funding the costs of harmonising staff terms and conditions. All of the increase in funding in 2019/20 is to fund these costs (Exhibit 2, page 9).

8. The SFC and Colleges Scotland have calculated the additional cost from harmonising staff terms and conditions at £50 million per annum from 2019-20. This includes £12 million allocated over the next two years to fund the harmonisation of terms and conditions for support staff. Colleges and the Educational Institute of Scotland (EIS) are in dispute over the cost of living pay claim for lecturers, over and above the harmonisation of pay, terms and conditions. This has resulted in several periods of industrial action and they have yet to reach agreement. The additional costs of the settlement will have further implications for colleges' costs and financial sustainability.

9. There is no additional Scottish Government revenue funding to cover other cost increases over this period, such as cost of living increases and increases in employer pension contributions. Scottish ministers have committed to pass on any specific UK funding made available to help meet planned increased employer pension contributions to the Scottish Teachers Superannuation Scheme. There still may be a significant element that remains unfunded for colleges (Exhibit 3, page 9).

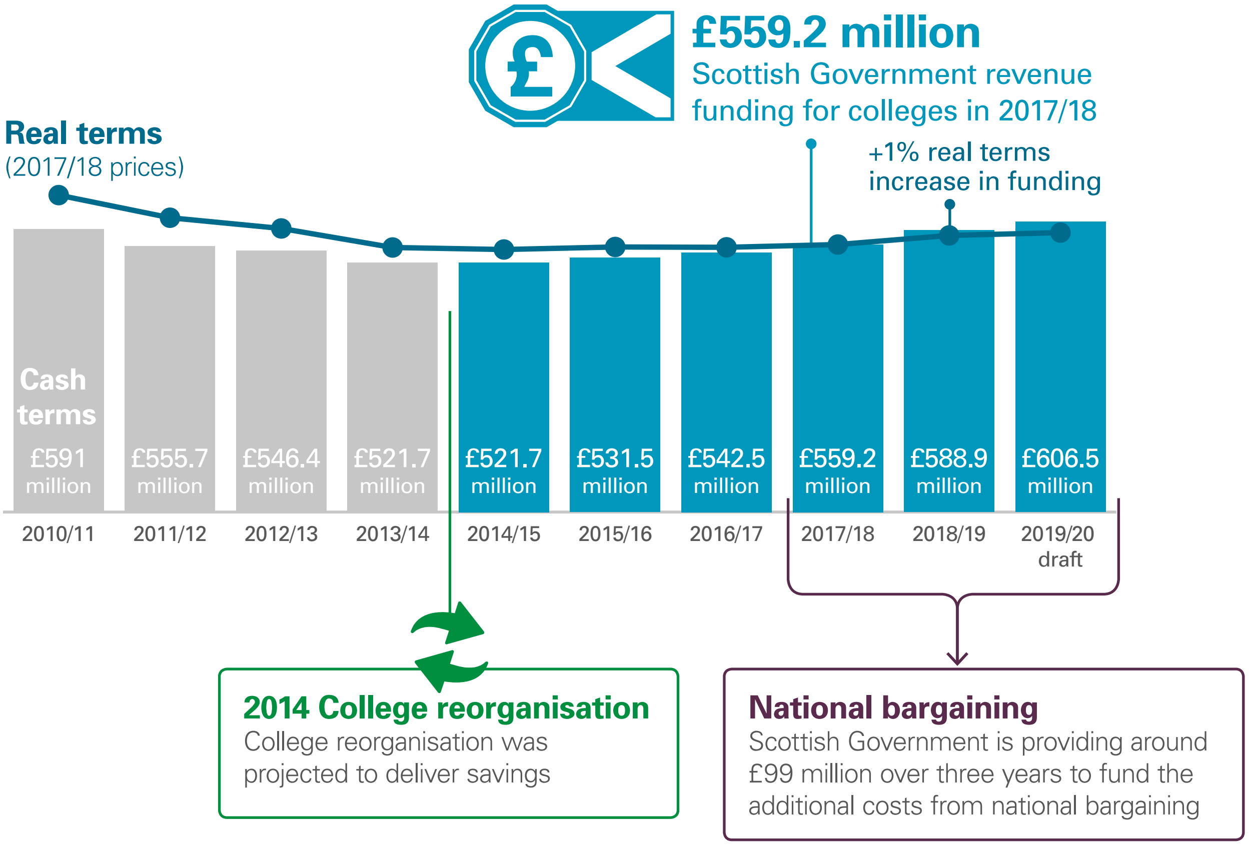
Staffing changes will affect SFC funding for harmonising terms and conditions

10. Total staffing numbers across the sector in 2017-18 remained unchanged, but the staffing profile across the sector has changed.[1] The number of non-teaching staff fell, while the number of teaching staff increased by the same proportion. The proportion of full-time permanent teaching staff with a recognised teaching qualification fell by one percentage point to 87.9 per cent.

11. Small changes at sector level mask noticeable changes within some colleges:

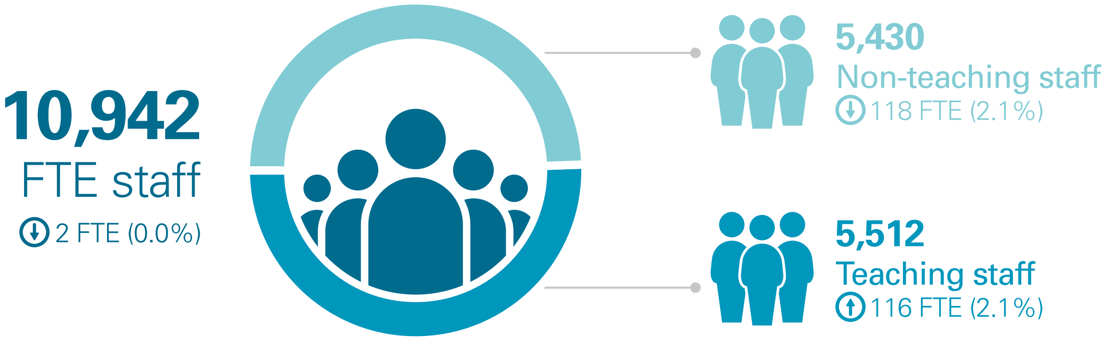
- Twelve incorporated colleges increased their teaching staff numbers. Of these, seven reduced their non-teaching staff.
- Seven incorporated colleges reduced teaching staff. Of these, three increased their non-teaching staff.
- Three incorporated colleges increased both teaching and non-teaching staff numbers, while four reduced both teaching and non-teaching staff.

Exhibit 2
Scottish Government revenue funding for colleges



Source: Scottish Government

Exhibit 3
Colleges staffing 2017-18



Note: Staffing numbers fluctuate depending at the point in the year they are recorded.

Source: College staffing returns to the SFC

12. Current funding allocations for harmonisation of terms and conditions are based on the number of staff in April 2018. The SFC will consider changes in staff numbers when determining future funding allocations.

Some sector-level financial health indicators improved in 2017-18 but the ability to draw on cash balances and ALF income has reduced for most colleges

13. Performance across the sector varied against financial health indicators. The sector's access to cash reduced. Its current net asset/liabilities position improved (ie, the sector's ability to pay its debts), with a reduction in net liabilities. Net assets more than doubled in 2017-18, mainly due to factors outside colleges' direct control. (Exhibit 4).

Exhibit 4

College sector financial health indicators

	2016-17		2017-18	
Cash	£49.2m	↘	£42.1m	Cash held by colleges fell by 16 per cent in 2017-18. Twelve colleges had a reduction in cash, totalling £12.5 million. Eight colleges increased cash balances by almost £5.9 million. Cash balances will fluctuate throughout the year and some cash will already be committed to planned expenditure.
Net assets	£230m	↗	£484m	Comparing the value of the assets an organisation holds against its financial liabilities – its net asset or liabilities position – gives an indication of its financial health. Net assets increased by £254 million, more than doubling the £230 million we reported in 2016-17. But £240 million of the increase was as a result of favourable revaluations of pensions and buildings.
Net current assets (liabilities)	(£33.9m)	↘	(£31.3m)	Current net assets/liabilities are an indication of colleges' ability to pay off current debts. Net liabilities across the sector have reduced. In only five colleges are current assets greater than current liabilities.

Source: Incorporated college 2017-18 accounts

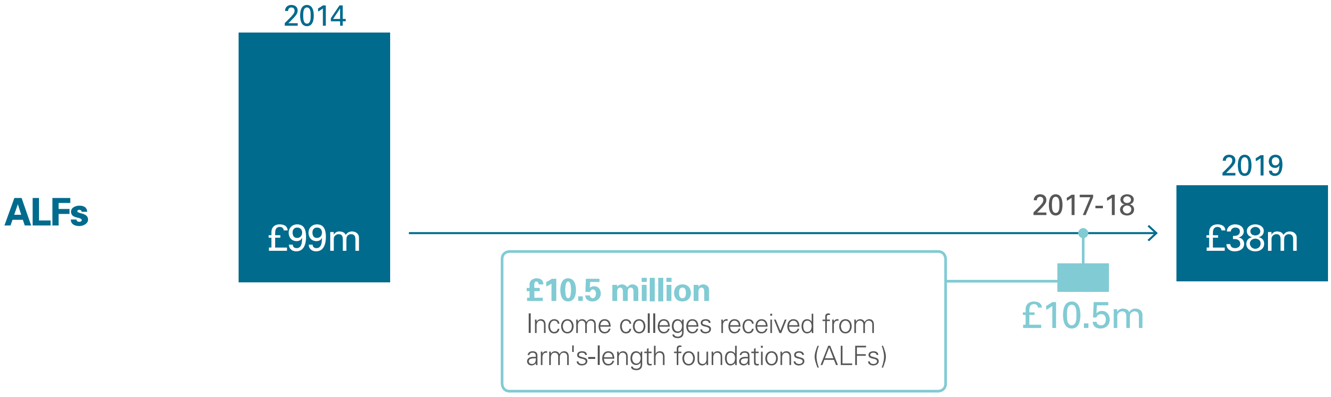
Arm's-length foundations continue to be a reducing source of funds for colleges

14. Fifteen colleges received funding from arm's-length foundations (ALFs) in 2017-18. Around 80 per cent (£8.4 million) of the total sector income from ALFs was provided to Ayrshire, City of Glasgow, Glasgow Clyde and Glasgow Kelvin colleges. ALFs are independent, charitable bodies that were set up when colleges were reclassified as public bodies and could no longer retain significant cash reserves. Colleges can donate money into ALFs and can apply to ALFs for funding. Colleges have typically used income from ALFs to fund voluntary severance, capital works and investment in equipment and digital infrastructure.

15. Balances held by ALFs are reducing, with colleges planning to apply to use a further £6.25 million of ALF funding in 2018-19. ALF balances vary significantly, with some colleges having little or no scope to access any ALF income. For the remainder of colleges, the ability to apply for income from ALFs is becoming increasingly limited as balances reduce (Exhibit 5).

Exhibit 5

The balances of arm's-length foundations (ALFs) are reducing



Source: College accounts and ALF accounts or SFC – ALF balances not in college accounts

There is significant variation in the financial positions of individual colleges

16. There is significant variation in the financial indicators at individual college level. Taken on their own, each indicator is not a reliable measure of financial health. But, taken together, the indicators provide a broad indication of the extent to which each college is exposed to financial risk (Exhibit 6, page 12).

Exhibit 6
Financial indicators

Colleges	Underlying surplus/deficit	Operating surplus/deficit	Cash	Net assets	Net current assets/liabilities
Ayrshire College	-1.9%	-4.9%	3.3%	78.5%	-8.1%
Borders College	1.6%	-0.6%	19.9%	0.5%	10.5%
City of Glasgow College	0.7%	-2.5%	7.6%	29.7%	-4.8%
Dumfries and Galloway College	-0.5%	-8.1%	5.5%	82.7%	-6.7%
Dundee and Angus College	0.3%	-4.6%	2.7%	77.7%	-6.3%
Edinburgh College	0.6%	-3.4%	1.4%	111.5%	-8.7%
Fife College	0.2%	-6.6%	4.2%	61.3%	-3.1%
Forth Valley College	1.9%	-2.3%	15.6%	-14.0%	1.6%
Glasgow Clyde College	0.3%	-1.0%	5.3%	138.8%	-5.0%
Glasgow Kelvin College	1.5%	1.0%	4.6%	41.9%	-10.3%
Inverness College	1.4%	-5.2%	14.6%	-10.2%	-5.0%
Lews Castle College	1.9%	-5.1%	2.7%	48.0%	-4.9%
Moray College	1.2%	-3.5%	5.9%	90.6%	-5.9%
New College Lanarkshire	0.9%	-4.3%	1.8%	53.9%	-8.7%
North East Scotland College	-2.2%	-8.1%	4.9%	85.0%	5.5%
North Highland College	0.4%	-6.0%	3.0%	22.1%	2.3%
Perth College	0.0%	-5.7%	8.6%	103.0%	-8.4%
South Lanarkshire College	4.0%	0.2%	3.9%	56.0%	-5.5%
West College Scotland	0.0%	-4.7%	6.2%	101.9%	0.0%
West Lothian College	0.9%	-5.0%	3.9%	-16.6%	-4.4%
Scotland	0.4%	-4.0%	5.7%	65.2%	-4.2%

Quartile: Highest 1 2 3 4 Lowest

Notes:
1. Financial indicators are shown as of the proportion of each college's expenditure
2. For each indicator, we have shown colleges' performance broken down into quartiles, with the highest performance shown in Quartile 1 and the lowest performance in Quartile 4.

Source: College accounts

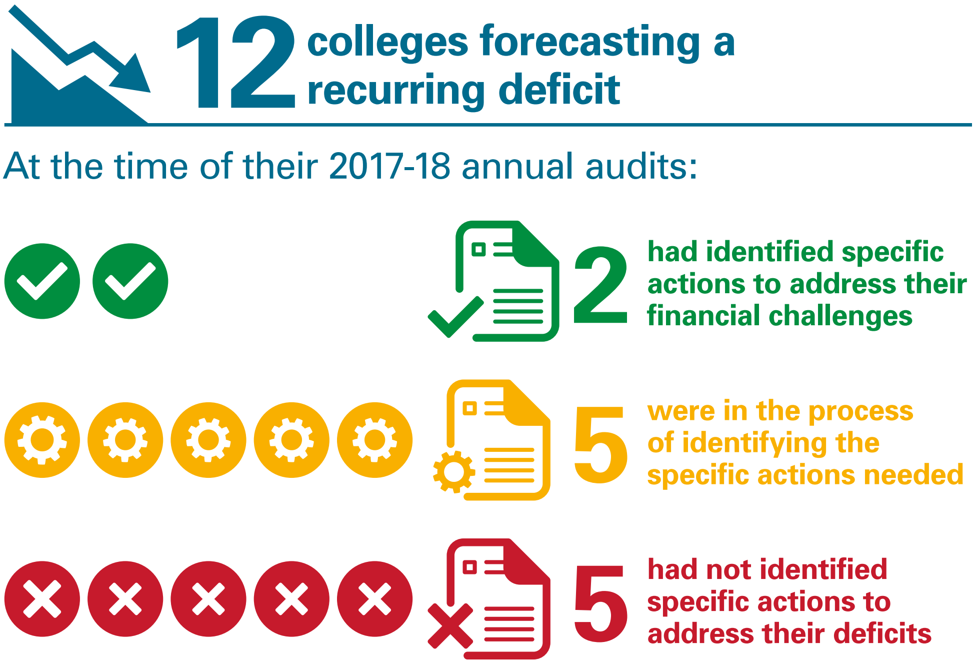
Twelve incorporated colleges are forecasting recurring deficits during the next five years

17. The SFC requires colleges to submit five-year financial forecast returns every year, and provides colleges with common financial planning assumptions to use when preparing their forecasts. Although colleges did apply the SFC's common assumptions, the SFC identified that colleges had not been consistent in compiling their most recent financial forecasts.[2] Colleges had broadly adopted one of two approaches: making forecasts that incorporated actions to address potential deficits; or forecasting their future financial position based on how they currently operate. Twelve colleges are forecasting recurring deficits during the next five years. Of the six non-incorporated colleges, only Orkney College is not projecting a recurring deficit during the next five years.

Only two of the 12 incorporated colleges forecasting recurring deficits had identified specific actions to address their financial challenges

18. At the time of their annual audit, only two of the 12 colleges forecasting a recurring deficit had identified the specific actions needed to address their financial challenges. A further five colleges were in the process of developing specific actions. Of the ten colleges still to determine agreed actions to address recurring deficits, six are forecasting a deficit position by the end of the next academic year: Inverness, North Highland and West Lothian colleges are forecasting deficits from 2018-19; and Forth Valley, Glasgow Clyde and Glasgow Kelvin colleges are forecasting deficits from 2019-20 (Exhibit 7).

Exhibit 7
Status of colleges' responses to forecasted recurring deficits



12 colleges forecasting a recurring deficit

At the time of their 2017-18 annual audits:

✓ ✓ **2** had identified specific actions to address their financial challenges

⚙ ⚙ ⚙ ⚙ ⚙ **5** were in the process of identifying the specific actions needed

✗ ✗ ✗ ✗ ✗ **5** had not identified specific actions to address their deficits

Source: SFC/colleges' external auditors

19. The SFC asked colleges that are projecting deficits to identify the actions needed to achieve financial sustainability. Additional financial pressures have emerged since colleges prepared their financial forecasts, including reduced capital funding and additional employer pension contributions. Unless funding increases, or colleges change how they operate, these are likely to result in future forecasts showing a worsening financial picture.

Three colleges face particular challenges to their financial sustainability

20. Auditors have highlighted that increasing operating deficits present challenges to financial sustainability in many colleges. Three colleges face particular challenges.

Ayrshire College

Ayrshire College reported an underlying deficit of £1 million in 2017-18 and was forecasting increasing deficits over the next five years, with a cumulative deficit of around £12 million (equivalent to 23 per cent of its current expenditure) by 2022-23. The college faces a number of cost pressures. It has identified annual PFI payments of £1.4 million until 2024-25 as its highest risk.

In February 2019, the SFC agreed the college's two-year financial sustainability plan. The SFC will provide the college with an additional £1.3 million in 2018-19 to fund a voluntary severance scheme and additional revenue funding support of £0.7 million in both 2019-20 and 2020-21.

The college anticipates its severance scheme will contribute to financial sustainability by generating savings of £1.66 million a year, reducing its projected cumulative deficit by 2022-23 to £5 million. Like other colleges, Ayrshire will need to continue to manage its costs, and to develop the necessary actions to balance its operating position from 2021-22 onwards.

New College Lanarkshire

Last year, the Auditor General for Scotland prepared a statutory report on the college, which highlighted the financial challenges facing the college and the potential impact on its longer-term financial sustainability. The college reported an underlying surplus of £0.6 million for 2017-18.

During the year, the SFC provided the college with £1.1 million for voluntary severance and a short-term cash advance of £1.3 million to address cash-flow difficulties.

The Lanarkshire Regional Board has agreed a five-year regional business plan with the SFC. This forecasts an underlying surplus for the college by 2019/20. The college anticipates receiving a further repayable advance of £2.6 million from the SFC in 2018-19, subject to maintaining progress and achieving the milestones in its plan.

To achieve financial sustainability, the college is reducing staffing costs. The SFC will provide £645,000 for the next voluntary severance scheme proposed in the plan. The college also intends to increase non-SFC income and to pursue opportunities for shared services with South Lanarkshire College.

North Highland College

The college reported a small underlying surplus of £0.1 million in 2017-18 but faces several key risks to its financial sustainability.

The college has previously required cash advances from its regional body, the University of the Highlands and Islands (UHI). It is forecasting a cumulative underlying deficit of £2.5 million by 2022-23 (equivalent to around 16 per cent of current costs) and a negative cash-flow position from 2019-20 onwards.

The college has loans of £1.3 million and in 2017-18 relied on waivers from its bank to avoid breaching loan covenants. At the time of the annual audit, the college did not have an agreed financial plan in place to achieve the required savings in both the short and longer term.

The auditor highlighted the need for more detailed interaction between the college and UHI as savings plans are developed. The college has since began a curriculum review, with a view to achieving savings for the 2019-20 budget. However, the college anticipates that it may require financial support from UHI, in the form of cash advances, for 2019-20.

21. Staff costs are the largest area of college expenditure and those colleges that have produced financial plans to address their underlying financial deficits are planning or currently implementing voluntary severance schemes as part of their plans.

Scottish Government capital funding is insufficient to address colleges' maintenance requirements

22. Capital funding is needed for the maintenance and improvement of buildings and investing in digital infrastructure. The Scottish Government provided £76.7 million of capital funding for the sector in 2018/19. Of this, £43.1 million related to existing capital commitments, including Forth Valley College's new campus project, £27 million was allocated for very high-priority backlog maintenance identified in the SFC's estates survey in 2017.[3] The SFC is monitoring whether funding for backlog maintenance has been spent as planned.

23. In 2019/20, capital funding for the sector has fallen to £47.6 million. Of this, £22.7 million is for Forth Valley College's new campus. After other specific capital commitments,[4] the SFC is allocating £21 million to address lifecycle and backlog maintenance needs.[5] Colleges and the SFC have calculated annual lifecycle maintenance costs to be around £22 million, over and above the £77 million high-priority backlog maintenance costs previously identified in the SFC's 2017 estates survey.

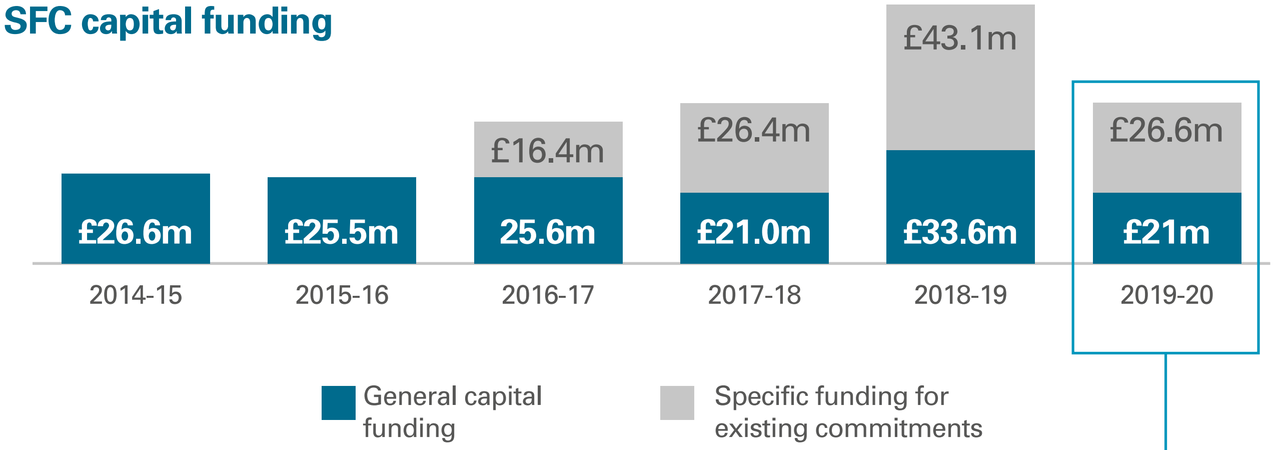
24. Reduced capital spending creates a risk that the cost of urgently needed backlog maintenance increases. This in turn poses a potential risk to some colleges' ability to continue to deliver their core services in a safe environment, and to invest in new digital infrastructure to generate efficiencies and enhance the student experience. The Scottish Government is working with the Scottish Futures Trust and the SFC to identify an appropriate revenue funding model for future investment in the college estate (Exhibit 8, page 16).

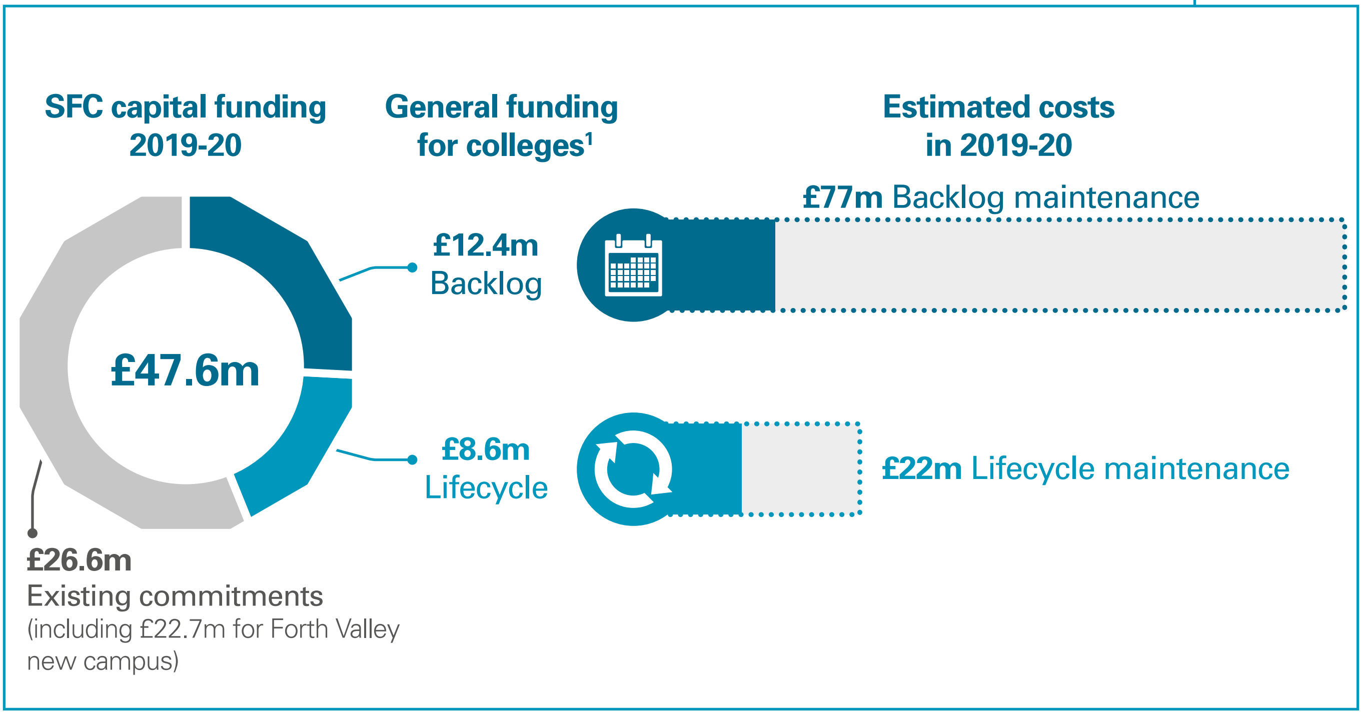
Exhibit 8
Capital funding

£47.6 million

Capital funding in 2019-20

Typically, capital funding is used for the maintenance and improvement of buildings but is becoming increasingly important for investing in and developing digital infrastructure.





Note: 1. Excluding Forth Valley

Source: Scottish Government/SFC

The potential implications of the UK's withdrawal from the EU remain unclear

25. The college sector is examining the potential implications surrounding the UK's planned withdrawal from the EU. The main areas that are likely to be affected are students, staff and funding. Data shows that:

- 7.3 per cent of credits are delivered to non-UK EU nationals (2016-17).

- Colleges' representative body, Colleges Scotland, estimates that non-UK EU nationals make up around three per cent of current staff in the sector. There will however be variation across colleges, with potentially the most significant impact being in Edinburgh and Glasgow.

- The SFC is allocating around £13 million to colleges to deliver European Social Fund (ESF) activity in 2019-20. This includes an assumed ESF contribution from the European Commission of around £5 million (around 0.7 per cent of current total sector income), subject to the submission of successful claims to the Scottish Government. College accounts for 2017-18 show that an additional £2.6 million of European income was received across the sector (0.4 per cent of total sector income). This was predominantly for ERASMUS+ placements.[6]

26. The wider potential implications of EU withdrawal remain unclear. While the direct impact on colleges is likely to be relatively small compared to some other parts of the public sector, colleges anticipate that the indirect effects could be much more significant. This includes potential reductions in EU funding that colleges receive through students funded by other organisations.

Part 2

Performance

Key messages

1 Student numbers increased, and the sector exceeded its learning activity targets. Over the past three years, colleges have been providing less learning to students aged 16-24 and more to students aged 25 and over.

2 Colleges are widening access to learning for disabled, ethnic minority and care-experienced students but the proportion of learning delivered provided to students from deprived areas fell slightly in 2017-18. Attainment rates for students in most of these categories continue to be below those of the student population overall.

3 Fewer students are completing their courses but a slightly higher proportion of students gaining a qualification are going on to positive destinations. Average attainment rates for students in full-time education have remained relatively static in recent years. The attainment rate for full-time further education, at 66 per cent, is some distance from the SFC target of 75 per cent by 2020-21.

4 There continues to be considerable variation across colleges in terms of student outcomes. The SFC has agreed aspirational and stretching targets with colleges in their latest outcome agreements. Based on recent performance trends, achieving some of these targets will be very challenging for colleges.

Student numbers increased, and the sector exceeded both the Scottish Government's learning target and the SFC's national activity target

27. In return for their funding from the SFC, college regions agree a range of outcomes they aim to deliver each year. Outcome Agreements contain ten measures to assess colleges' progress. Within these ten measures there are national priority measures based around learning credits delivered, the achievement of qualifications (attainment) and successful students going on to positive destinations.

Exhibit 9
Number of students and amount of learning delivered 2017-18

242,485
Students
(an increase of 6,748)

118,684
Full-time equivalent
(FTE) student places
(an increase of 1,182)
against the Scottish
Government's target of
116,269 FTE

1,778,466
Credits delivered
(an increase of 16,434)
against the SFC's national
target of 1,765,439

Source: SFC

28. Colleges delivered 16,434 more credits than in 2016-17 and exceeded the SFC's national activity target by 0.7 per cent. Five colleges missed their individual target (by a very small percentage in two instances):[7]

- Fife College (by 0.1 per cent)
- New College Lanarkshire College (by 0.2 per cent)
- North East Scotland College (by 1.4 per cent)
- Lews Castle College (by 4.7 per cent)
- Orkney College (by 4.5 per cent).

29. Where regions miss their credit target, the SFC – or the regional body, in a multi-college region – can decide to recover funding. Where the SFC or regional body is aware that a college may miss its target, it can look to redistribute both the activity and the funding to another college or region.

30. UHI is committed to providing access to learning across the region, and to avoid centralising delivery in urban areas. Where colleges in the Highlands and Islands region have not met their targets, UHI is working closely with the colleges to understand, support them and, where necessary, review targets to reflect circumstances. For example, Lews Castle College faces particular challenges due to a declining population in the Outer Hebrides, and UHI is working with the college to assess the effects of this change, and to support the college to adjust its focus to deliver a financially sustainable operating model.

31. Colleges also exceeded the Scottish Government's target of delivering 116,269 FTE places[8], delivering 118,684 FTE places, an increase of 1,182 (one per cent) on 2016-17 **(Exhibit 9)**. The Scottish Government's target has remained constant since 2012-13 though the context in which colleges operate has been changing:

- The young Scottish population has been reducing and is projected to reduce further over the next few years. This is resulting in fewer young students (16-24) at college, and more school-aged and older students.

- The Scottish Government continues to promote widening access to further and higher education. Its aim is for 20 per cent of students entering university to be from the 20 per cent most deprived areas by 2030. While colleges play an important role in supporting a learner's whole journey, this may reduce the number of students that will consider studying at college in future.

Over the past three years, colleges have been providing fewer credits to students aged 16-24 and more to students aged 25 and over

32. In October 2017, the Minister for Further Education, Higher Education and Science confirmed that colleges no longer needed to prioritise full-time education for 16-24 year olds.[9] It is clear that college provision was changing before this announcement. Between 2014-15 and 2017-18, the number of students aged 16-24 fell by 6,887 (or by six per cent). There was a corresponding increase in the number of students aged 25 and over by 6,664 (or by seven per cent). Over the same period, the proportion of learning credits delivered by colleges shifted from students aged 16-24 to students aged 25 and over by four percentage points (Exhibit 10, page 21).

33. Between 2014-15 and 2017-18, there was an increase of 86 per cent (15,815) in the number of school pupils under 16 years of age attending college. Students aged under 16 now make up an additional six per cent of the student population compared to 2014-15. Despite this, credits delivered to under 16 years old have remained very small at only around three per cent. Under the Scottish Government's Developing the Young Workforce programmes, colleges work closely with schools and councils, offering more vocational courses to school pupils. Most courses will not be graded but aim to expand pupils' curriculum choices and help them develop a career path. In 2017-18, all colleges except Newbattle Abbey College delivered credits to students under 16 years of age.[10]

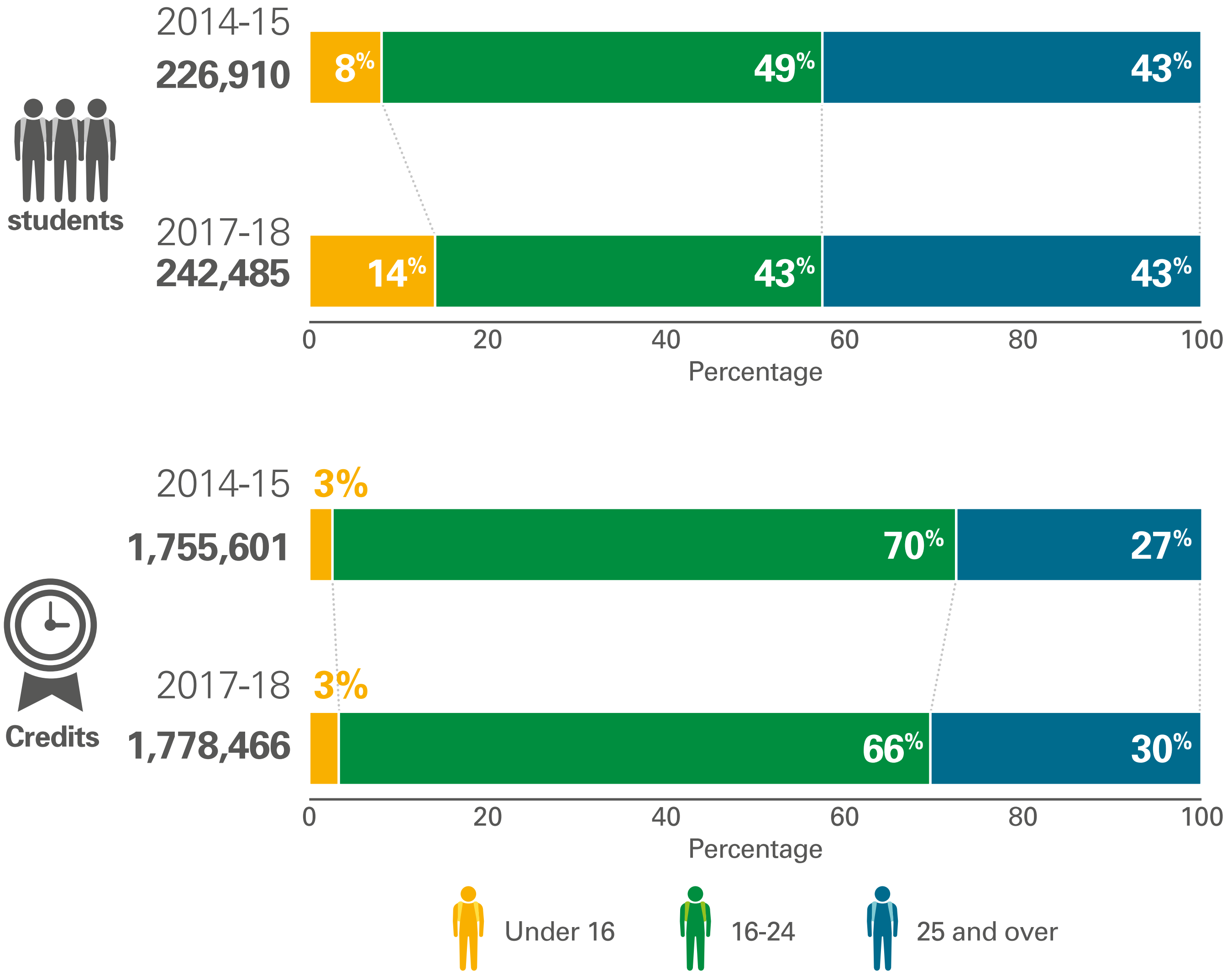
More change is needed to achieve gender balance across important subject areas

34. Female students represent 52 per cent of the student population (125,899) and males 48 per cent (115,945).[11] The number of female students increased by more than the number of male students in 2017-18 (increasing the proportion from 51 per cent last year).

35. In 2016, the SFC committed to increasing the minority gender share in the most imbalanced subjects.[12] Its aim is for the gender balance of students enrolling on important subject areas to be no greater than 75:25 per cent by 2030. Progress towards addressing the long-standing gender imbalances has been limited and will require a concerted effort from schools, colleges and wider society in making sustainable change (Exhibit 11, page 22).

Exhibit 10

Change in the number of students and learning credits delivered across the sector over the past three years



Note: The proportion of credits for 2017-18 doesn't add up to 100 per cent due to rounding.

Source: SFC

Eighteen college boards have more men than women

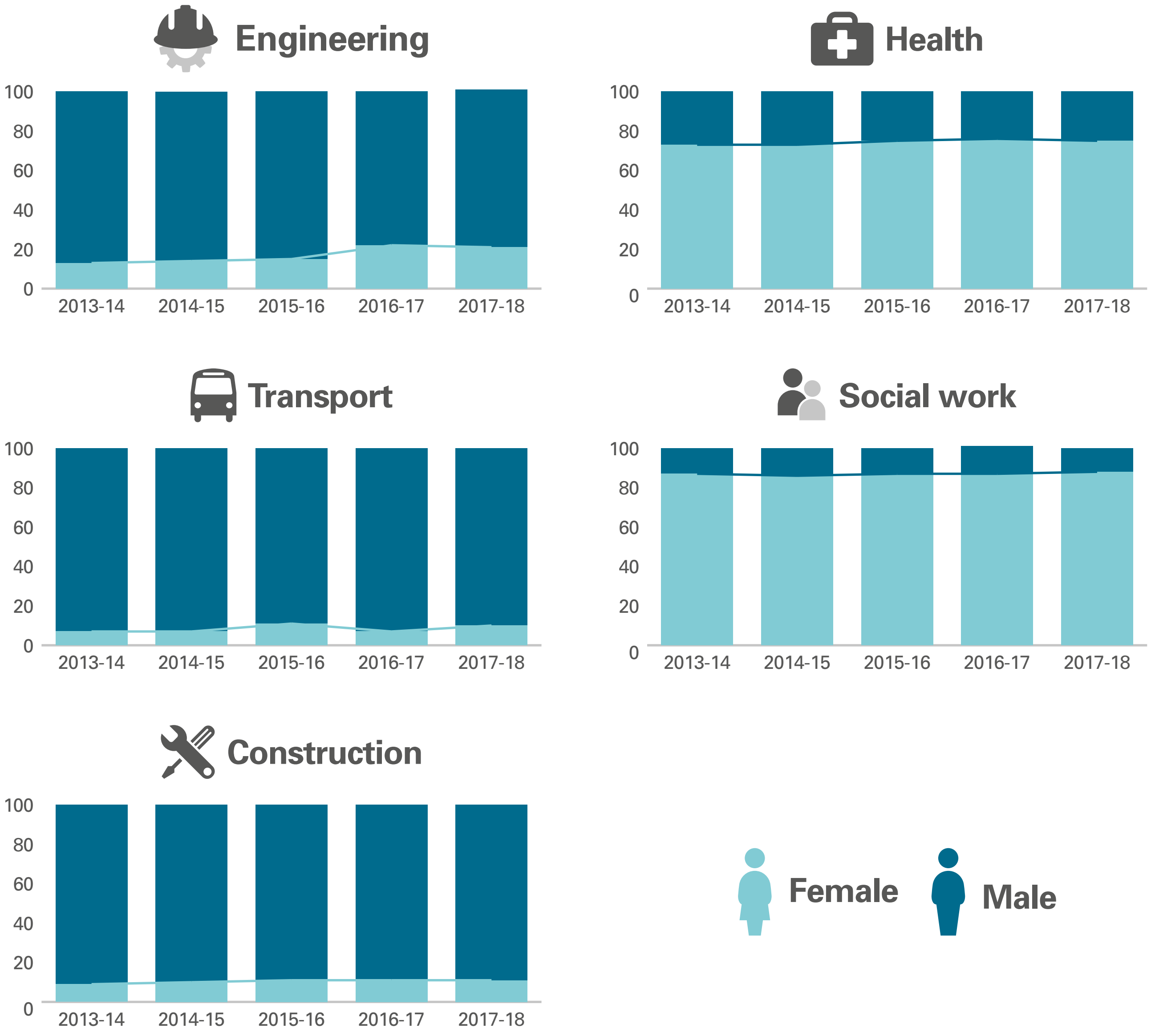
36. In February 2019, 246 board members across the sector were men (57 per cent of the total members) and 187 were women (43 per cent of the total members). The number of men increased by 12, while the number of women decreased by four.

37. Four college boards have more women members than men and five have an equal gender split. Orkney College Board has the most uneven gender balance with 19 men and three women.

38. The Gender Representation on Public Boards (Scotland) Act 2018 requires 50 per cent of non-executive members on public boards to be women by 2022. The gender balance of college boards is not entirely under the control of colleges as some members are elected to their position.

Exhibit 11

Proportion of students on each course by gender (headcount)



Source: SFC

Colleges are widening access to students from a range of backgrounds, but are not meeting targets for students from the most deprived areas

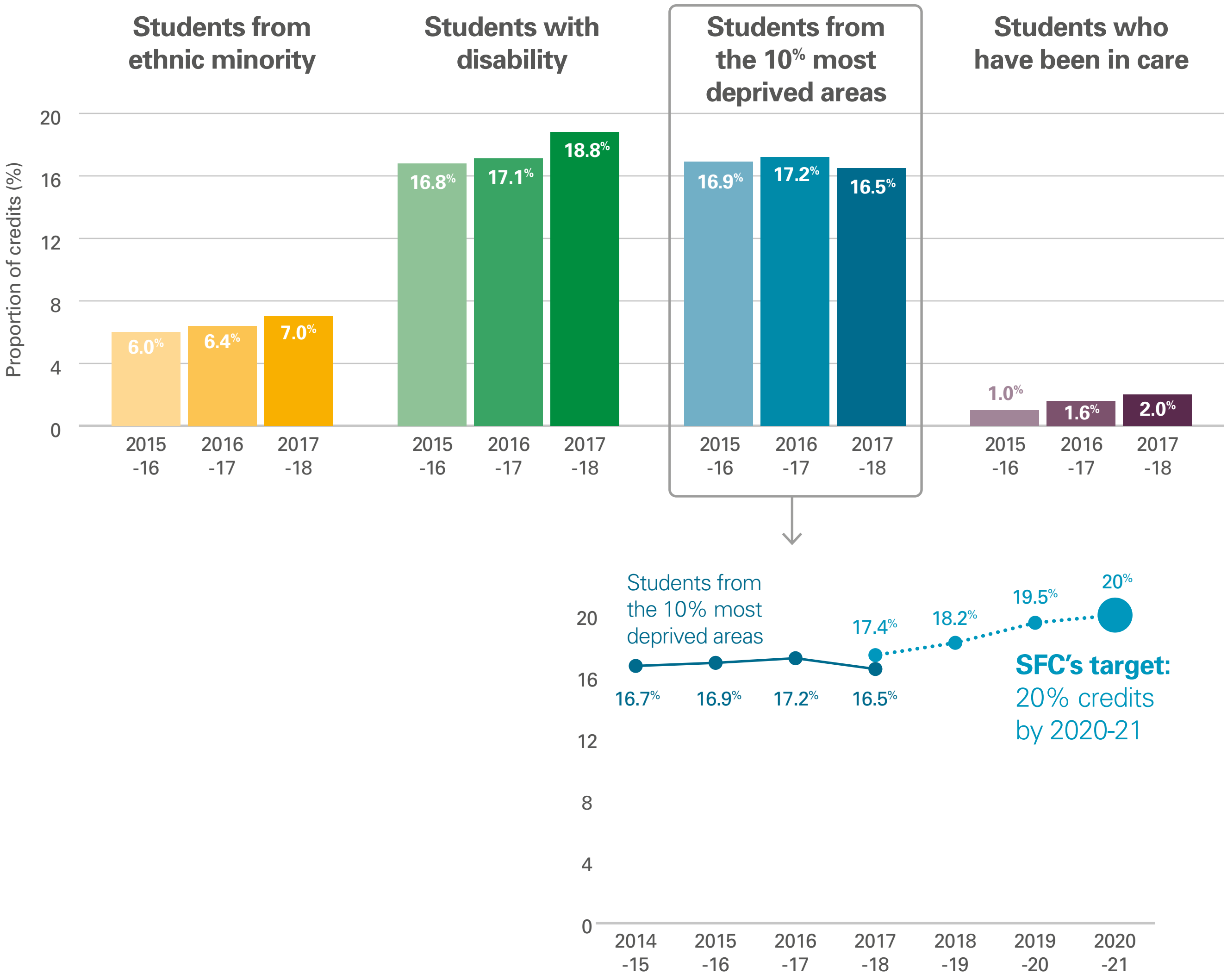
39. Colleges are committed to widening access to learning for all, particularly those who may have found it more difficult to enter further and/or higher education. Across the sector, the proportion of credits colleges deliver to students from an ethnic minority, who have been in care or who have disabilities has increased in recent years.[13]

40. The proportion of credits that colleges deliver to students from the ten per cent most deprived areas had also been increasing, but this trend reversed in 2017-18.[14] The proportion of credits delivered to these students, at 16.5 per cent, was below the SFC's national target of 17.4 per cent.[15] The reasons for this decrease are likely to be complex. For example, the trend is for school pupils to stay on longer at school. Also, in line with the Scottish Government's aim of widening access to higher education, there has been an increase in the proportion of students from deprived areas going to university. Increasing the proportion of credits to students from the most deprived areas will require a coordinated effort from schools, colleges, universities and other relevant stakeholders (Exhibit 12).

41. Based on recent trends, the SFC's target of delivering 20 per cent of credits to students from the ten per cent most deprived areas by 2020-21 looks difficult to achieve.

Exhibit 12

Proportions of credits delivered to students from selected groups



Source: SFC

Exhibit 13

National performance summary, 2017-18

The proportion of students completing their courses is falling, but the proportion of full-time students going on to positive destinations is improving.

	Attainment rates	Retention rates	Positive destinations	Satisfaction
Further education				
Full-time	66.1 ↑ (0.8%)	74.9 ⇄ (0.0%)	86.0 ↑ (1.9%)	93.1 ↑ (0.3%)
Part-time	78.2 ↑ (1.1%)	89.8 ↓ (0.2%)	–	–
Higher education				
Full-time	71.3 ↓ (0.3%)	81.6 ↓ (1.2%)	81.6 ↑ (1.4%)	83.2 ↓ (4.2%)
Part-time	80.4 ↑ (1.8%)	91.6 ↓ (0.3%)	–	–

(%) – Percentage change from the previous year

Note: The latest positive destinations data available is for 2016-17. Percentage change is from 2015-16.

Source: *College Performance Indicators 2017-18*, Scottish Funding Council, 2019; *College Leaver Destinations 2016-17*, Scottish Funding Council, 2018; and *Student Satisfaction and Engagement 2017-18*, Scottish Funding Council, 2018

Student attainment has remained relatively static in recent years and further work is required to address the attainment gap

42. The SFC aims to improve attainment rates (the proportion of students completing their course successfully) in full-time further education and higher education to 75 per cent by 2020-21. The average attainment rate for full-time further education improved in 2017-18. In contrast, the average attainment rate in full-time higher education fell slightly. Both remain below the SFC's long-term target, with a significant improvement needed in further education over the next three years. The SFC has set intermediate national attainment targets for full-time students, although it did not set a target for 2017-18. It does not set national targets for part-time students (Exhibit 14, page 25).

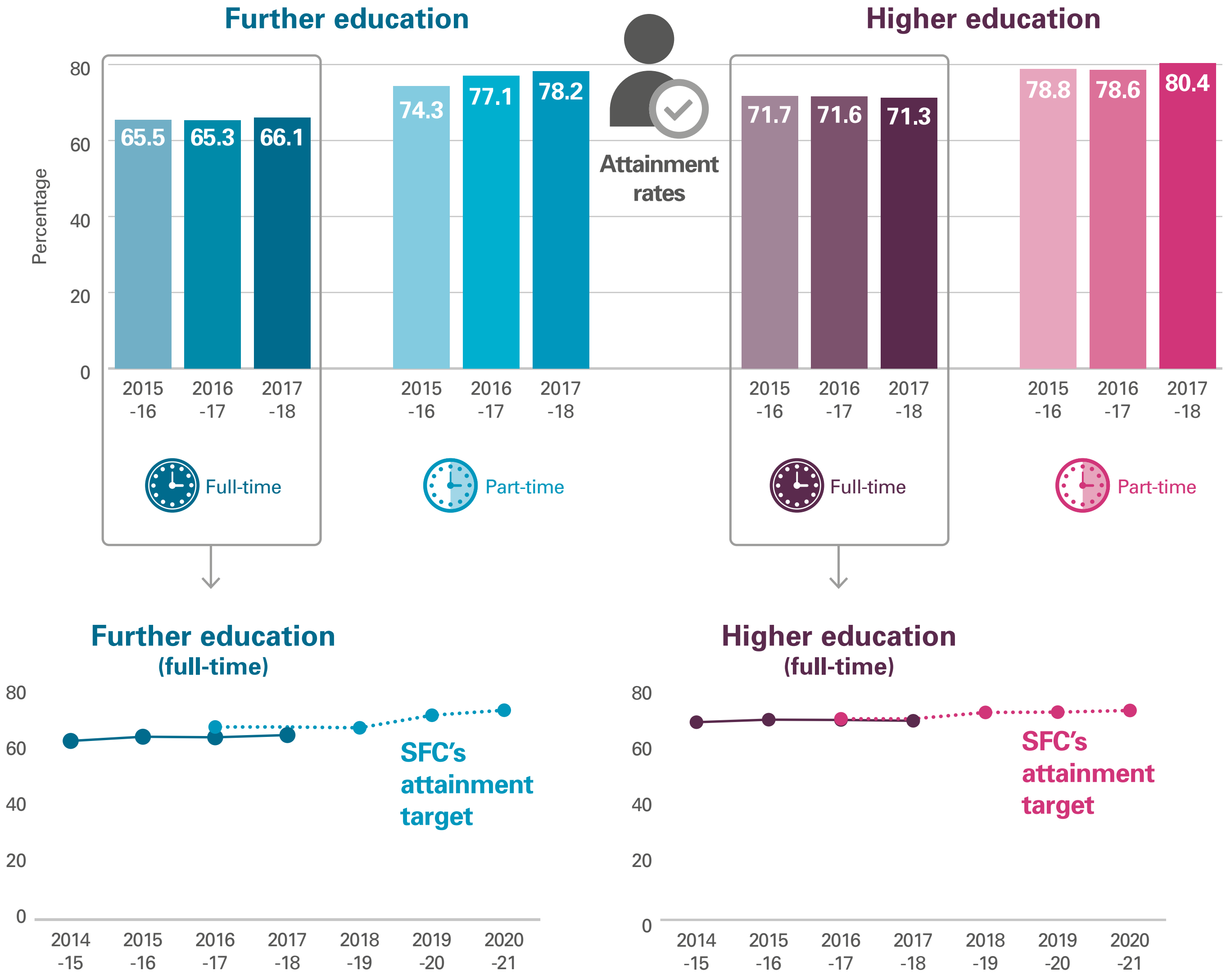
Only two regions met all of their agreed overall attainment targets

43. There is wide variation in regional performance against attainment targets (Exhibit 15, page 26):

- West College Scotland region met all four targets. Highlands and Islands region met both targets for further education.

- Two regions missed all four targets (Dumfries and Galloway and North East Scotland colleges).

Exhibit 14
Attainment rates



Source: SFC

44. The SFC does not report the performance of college regions against regionally agreed attainment targets in its Summary of Progress and Ambitions report.[16]

45. In 2018-19, the SFC plans to improve its use of Outcome Agreements to achieve its desired outcomes for learners, for skills development and ultimately for inclusive economic growth in Scotland. This includes agreeing more ambitious targets with college regions to deliver Scottish Government priorities. Based on performance to date, some existing targets will be very challenging for colleges. It is important for the SFC and colleges to be clear on what will be needed to deliver the more ambitious targets.

Exhibit 15

Attainment rates: progress towards outcome agreement targets

	Attainment target met in 2017-18		
Further education	No of college regions providing this type of study[1]	No of college regions	Percentage
Full-time	15	6	40%
Part-time	13	9	69%
Higher education			
Full-time	13	2	15%
Part-time	11	5	45%

Note: 1. Total numbers are based on 13 college regions plus SRUC and Newbattle Abbey College, with the exceptions being: Part-time further and higher education: Ayrshire and Newbattle Abbey colleges did not set 2017-18 targets for these measures in their Outcome Agreement; and Higher education: College outcome agreement measures are not applicable to Highlands and Islands region or SRUC at this level.

Source: SFC

More work is required to close the attainment gap for certain groups of students

46. Students from an ethnic minority, on average, achieve better results than the overall student population, but more work is required to close the attainment gap for the rest of the identified student groups.[17] Students who have been in care have the lowest attainment rates, and were the only group where attainment decreased in 2017-18 (Exhibit 16, page 27).

47. The SFC is committed to raising the attainment rates for students from the most deprived areas to achieve overall attainment rates of 75 per cent by 2027-28.[18] In *Scotland's colleges 2018*, we reported that the attainment gap between students from the least and most deprived areas had increased between 2011-12 and 2016-17.

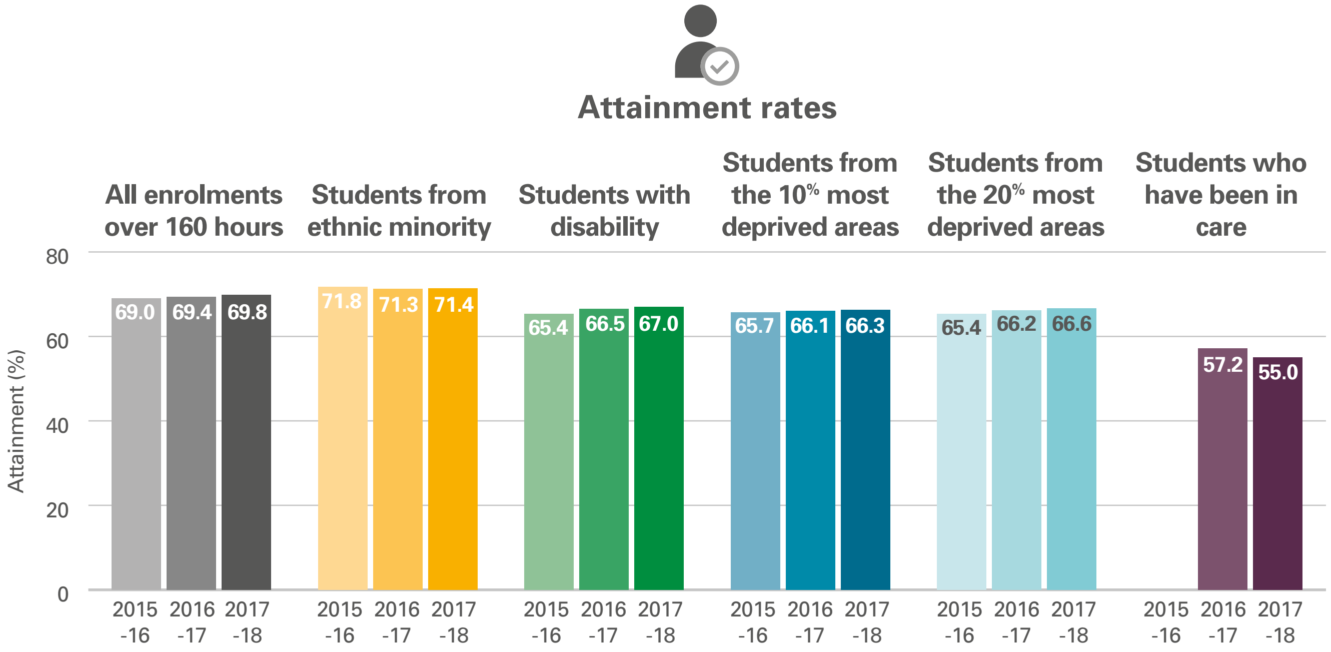
48. Last year, we reported that the attainment gap in 2016-17 increased between those students from the least and most deprived areas. In 2017-18, the attainment gap for those in further education closed slightly, from 7.4 to 6.5 percentage points (69.7 per cent compared to 63.2 per cent). The attainment gap for those in higher education was 7.7 percentage points, the same as in 2016-17 (74.4 per cent compared to 66.7 per cent).

Fewer students completed their course in 2017-18

49. Challenges still exist in improving student retention (the proportion of students completing their course, either successfully or partially). The proportion of full-time further education students that completed their course remained unchanged in 2017-18 but the proportions fell for all other types of study (Exhibit 17, page 27).

Exhibit 16

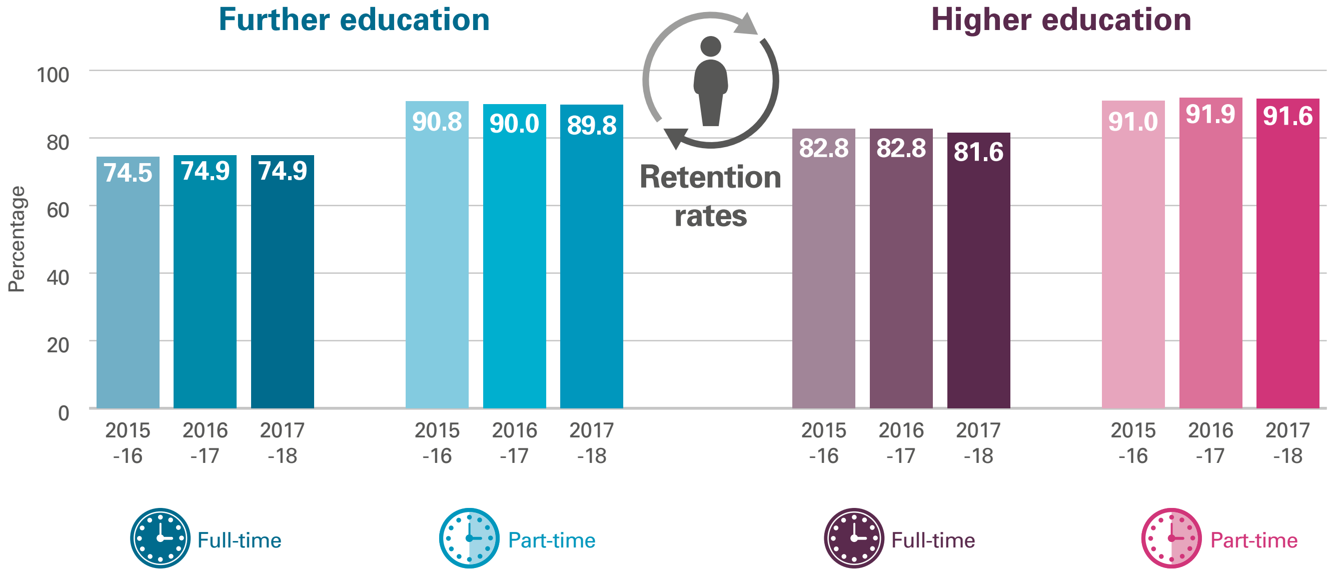
Attainment on courses over 160 hours for students from selected groups



Source: SFC

Exhibit 17

Proportion of students completing their course



Source: SFC

50. Since 2017, the Scottish Government has been running a College Improvement Project (CIP) to raise attainment and retention. It has worked with five colleges through the CIP, trying to identify what improvement can be shared across the sector.[19] The project is scheduled to finish in 2019. While it is too early to assess the impact of the project, more work is required to improve retention. The Scottish Government plans to monitor changes in retention as improvement actions are scaled up and spread to different courses within the colleges and across the sector.

A greater proportion of students who qualify are going on to positive destinations

51. Latest data (covering 2016-17) shows that 95 per cent of full-time student qualifiers with destinations confirmed entered a positive destination, such as employment or continued education (2015-16, 94.9 per cent).[20] Of all qualifiers, 84.5 per cent moved into a positive destination (2015-16, 82.7 per cent). Around two-thirds of all qualifiers went on to further study or training (up by one percentage point from 2015-16). 17.7 per cent of all qualifiers entered work (up by 0.7 percentage point).

The SFC does not publish college-level student satisfaction data

52. Student satisfaction is a performance measure in college Outcome Agreements. For 2017-18, the SFC reported student satisfaction for the sector, but only using data from those colleges that received at least a 50 per cent response rate to their survey (15 of 26 colleges for full-time further education and five of 15 colleges for full-time higher education). It does not publish student satisfaction data for individual colleges or results for part-time and distance or flexible learning students. Publishing good-quality information on student satisfaction for individual colleges would allow students, and potential students, to determine whether a college provides a good experience for students. It also means that colleges can be effectively held to account by other stakeholders.

53. The SFC has been working with the college sector to conduct the Student Satisfaction and Engagement Survey (SSES) since 2015-16. However, over the past three years, response rates to the SSES have varied noticeably across colleges and the SFC does not yet believe that all colleges are conducting the survey in a way that allows either it or individual colleges to place reliance on the survey results. The SFC held an event for colleges in February 2019 to explore ways to improve response rates.

College performance varies widely for student outcomes

54. Taken together indicators on student attainment, retention, destinations and satisfaction provide a broad indication of a college's performance. There was significant variation in performance across colleges; the proportion of students from deprived areas can influence performance, but it is clearly not the only factor (Exhibit 18, page 29).

Exhibit 18

Performance indicators for full-time further education in colleges

Colleges	% credits for FT	Attainment rates	Retention rates	Positive destinations	Satisfaction	College's self-evaluation for 'Outcome and Impact'
Glasgow Kelvin College	45.5	60.2 ↓	69.0 ↓	82.9 ↑	-	Good
West College Scotland	58.5	69.2 ↑	78.1 ↑	80.6 ↓	-	Good
Glasgow Clyde College	67.1	66.1 ↑	74.9 ↑	82.8 ↑	96.7 ↑	Good
Ayrshire College	74.4	66.9 ⇄	73.9 ↓	82.6 ↓	-	Good
City of Glasgow College	58.9	67.9 ↓	76.3 ↓	91.2 ↑	84.5 ↓	Very Good
New College Lanarkshire	75.4	61.4 ↑	68.3 ↑	89.9 ↑	89.0 ↑	Satisfactory
Dundee and Angus College	70.0	75.4 ↑	81.4 ↑	81.7 ↑	95.4 ↑	Very Good
Fife College	61.8	59.1 ↑	73.4 ↑	71.7 ↑	91.9 ↑	Satisfactory
South Lanarkshire College	74.5	69.7 ↓	76.2 ↑	89.1 ↓	98.5 ↑	Very Good
West Lothian College	67.9	65.5 ↑	75.3 ↑	89.7 ↑	-	Good
Forth Valley College	51.8	71.4 ↓	77.2 ↓	75.6 ↓	95.1 ↓	Very Good
Edinburgh College	62.9	60.7 ↓	70.6 ↓	85.9 ↑	-	Good
Newbattle Abbey College	100.0	52.1 ↓	69.9 ↓	81.3 ↑	100 ↑	Good
Dumfries and Galloway College	70.6	59.6 ↓	70.6 ↑	88.3 ↑	-	Satisfactory
Perth College	78.4	70.0 ↑	77.2 ↓	85.2 ↑	96.2 ↑	Good
Borders College	78.0	68.7 ↑	77.1 ↑	86.9 ↓	-	Very Good
SRUC Land based	63.9	68.3 ↓	82.3 ↓	87.8 ↓	-	-
North Highland College	55.7	71.8 ↑	83.2 ↑	90.0 ↑	-	Very Good
Argyll College	47.4	76.0 ↑	82.0 ↑	80.9 ↓	94.3 ↑	Very Good
West Highland College	48.1	69.8 ↓	77.8 ↓	87.4 ↑	100 ↑	Very Good
Inverness College	69.5	70.6 ↑	77.7 ↑	87.3 ↓	94.7 ↑	Very Good
North East Scotland College	72.6	66.6 ↑	77.0 ↑	87.2 ↓	94.0 ↑	Good
Lews Castle College	46.5	60.8 ↓	71.6 ↓	90.3 ↑	100 ↑	Satisfactory
Moray College	74.2	69.0 ↑	75.5 ↑	84.2 ↑	94.0 ↑	Good
Orkney College	33.1	75.0 ↓	80.3 ↓	84.3 ↓	-	Very Good
Shetland College of Further Education	32.0	77.8 ↓	85.6 ↑	97.2 ↑	-	Very Good
Number of colleges where performance increased in 2017-18 ↑		13	15	16	13	
Proportion of total number of colleges %		50%	58%	62%	87%	

Quartile:	Highest	1	2	3	4	Lowest

Notes:

1. Colleges are listed according to the proportion of students from the most deprived areas (Glasgow Kelvin College having the highest proportion).
2. Percentage point changes are from 2016-17 (For leaver's destination data, from 2015-16. See Note 3).
3. The latest leaver's destination data available is for 2016-17. The figures are across further and higher education study. College-level figures published are not broken down by the two.
4. The overall student satisfaction rates are included only for colleges with a response rate of 50 per cent or more, in line with the SFC publication.
5. For each indicator, we have shown colleges' performance broken down into quartiles, with the highest performance shown in Quartile 1 and the lowest performance in Quartile 4.

Source: *College Performance Indicators 2017-18*, Scottish Funding Council, 2019; *College Leaver Destinations 2016-17*, Scottish Funding Council, 2018; *Student Satisfaction and Engagement 2017-18*, Scottish Funding Council, 2018; Colleges' self-evaluation reports, 2019; and SFC's Infact database

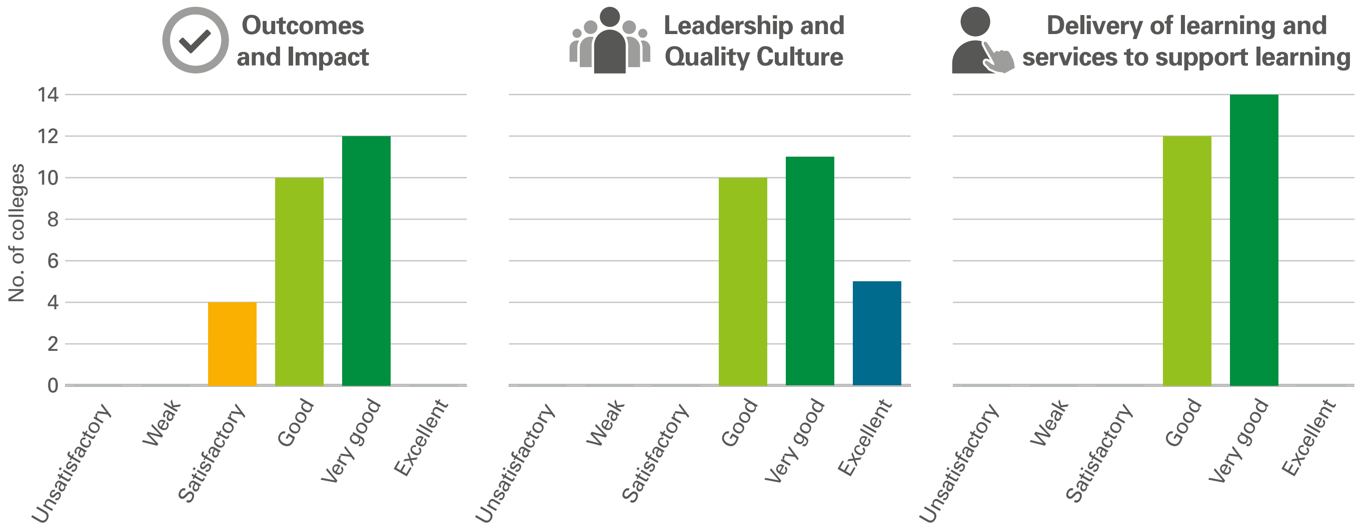
Colleges have published enhancement plans to improve their performance

55. The SFC and Education Scotland, the national body for supporting quality and improvement in learning and teaching, introduced a new quality assessment evaluation framework for colleges, *How good is our college?* in 2016.[21] The new quality framework is based on a validated self-evaluation and is intended to enable colleges to assess progress and develop an improvement plan.

56. In January 2019, individual college results were published for the first time with grades in three categories: Outcomes and impact; Leadership and quality culture; and Delivery of learning and services to support learning. All colleges graded themselves as 'Good' or above for two of the three categories. In general, colleges assessed their leadership most highly and the outcomes and impact for students least highly (Exhibit 19).

57. The factors considered in relation to 'Outcomes and impact' map closely to attainment and retention but not to positive destinations and student satisfaction. Some colleges which consider their performance to be 'Good' or better have relatively low levels of attainment (in the bottom half of the quartiles). It is not clear how colleges' own assessment of performance fits with the views of their students and staff.

Exhibit 19
College's self-evaluation grades



Source: Education Scotland

Endnotes

1 *College Staffing Data 2017-18*, Scottish Funding Council, 2019.

2 Financial forecast returns submitted by colleges to the SFC in September 2018 and covering the period to 2022-23.

3 College sector estates condition survey, Scottish Funding Council, December 2017.

4 This includes £1.5 million to support business cases for the highest priority campuses and £1.4 million for very high priority maintenance at Fife College.

5 *Outcome agreement funding for colleges*, Scottish Funding Council, 2019.

6 Erasmus+ is the European Union programme for education, training, youth and sport. It runs for seven years, from 2014 to 2020. Erasmus+ aims to modernise education, training and youth work across Europe. It is open to education, training, youth and sport organisations across all sectors of lifelong learning, including school education, further and higher education, adult education and the youth sector.

7 Lanarkshire region and the Highlands and Islands region both met their regional targets.

8 *College Statistics 2017-18*, Scottish Funding Council, 2019.

9 2018-19 Outcome Agreement Guidance, Letter from Minister for Further Education, Higher Education and Science to Chair of Scottish Funding Council, 2017.

10 SFC's Infact database.

11 According to the SFC's Infact database, 641 students did not give their gender or described it as 'Other'.

12 Gender Action Plan, Scottish Funding Council, 2016.

13 *College Statistics 2017-18*, Scottish Funding Council, 2019.

14 The level of deprivation is calculated using the Scottish Index of Multiple Deprivation (SIMD) 2016. In the previous two years, it is based on the SIMD 2012.

15 *College Region Outcome Agreements: Summary of Progress and Ambitions*, Scottish Funding Council, September 2017.

16 *College Region Outcome Agreements Summary of Progress and Ambitions report 2018*, Scottish Funding Council October 2018, summarises performance for the sector from colleges regions' Outcome Agreements.

17 *College Performance Indicators 2017-18, Scottish Funding Council*, 2019. Attainment on courses over 160 hours.

18 *Guidance for the development of College Outcome Agreements: 2017-18 to 2019-20*, Scottish Funding Council, 2016.

19 Dundee and Angus College, Edinburgh College, Inverness College UHI, New College Lanarkshire and West College Scotland.

20 *College Leaver Destinations 2016-17*, Scottish Funding Council, 2018. The data available is for full-time students only across further and higher education.

21 *How good is our college?*, Education Scotland, 2016.

Appendix

Audit methodology

What the report covers

This report looks at all colleges in the sector and Scotland's Rural College (SRUC), to present a comprehensive picture of the sector and its performance.

Until 1992, Scottish councils ran all publicly funded colleges in Scotland. Under the Further and Higher Education (Scotland) Act 1992, most of these colleges established their own corporate body and boards of management. The boards of management took over responsibility for the financial and strategic management of the colleges. These colleges are referred to as incorporated colleges and produce accounts which are subject to audit by the Auditor General for Scotland. The remaining six colleges are generally referred to as non-incorporated colleges. SRUC is classed as a higher education institution but counts towards the achievement of the national target for colleges. The report primarily focuses on incorporated colleges. However, we state clearly where we include data relating to non-incorporated colleges.

The college sector in Scotland comprises the 20 incorporated colleges and six non-incorporated colleges, organised into 13 college regions (as shown in Appendix 2 of *Scotland's colleges 2018*). Ten of these regions consist of one college. The three remaining regions (Glasgow, Highlands and Islands, and Lanarkshire) have more than one college. The individual colleges in Glasgow and in Highlands and Islands are assigned to the relevant regional strategic body, ie Glasgow Colleges' Regional Board (GCRB) or University of Highlands and Islands (UHI). In Lanarkshire, New College Lanarkshire is the regional body and South Lanarkshire College is assigned to the Lanarkshire Board.

Financial commentary

Incorporated colleges prepare their accounts based on the academic year, which runs from 1 August to 31 July. This differs from the Scottish Government's financial year, which runs from 1 April to 31 March. We use the following conventions in this report:

- 2017-18 when referring to figures from colleges' accounts, or figures relating to the academic year
- 2017/18 when referring to funding allocations made in the Scottish Government's financial year.

Financial figures in real terms are adjusted for inflation. The base year for this report is 2017-18. The GDP deflator provides a measure of general inflation in the domestic economy. We have used the GDP deflator from March 2019 to calculate the real-terms figures for other years.

Our audit involved

- Analysing relevant Scottish Government budget documentation, colleges' audited accounts and auditors' reports covering the financial periods ending July 2018.
- Analysing information held by the SFC, including financial, performance and activity data.
- Interviewing Colleges Scotland, student unions, trade unions, the SFC and the Scottish Government.
- Analysing data that we requested from colleges' external auditors.

Detailed methodology for specific sections in the report

Underlying financial position (page 7)

Incorporated colleges reported an overall deficit of £29.8 million in their 2017-18 audited accounts. In reporting the underlying financial position, we have used the SFC's data for each college based on the accounts direction it issued in 2018.

Calculating student numbers (page 19)

In this report we present student numbers by headcount, drawn from the SFC's Infact database. Where possible, this headcount excludes any multiple enrolments, meaning if a student had been enrolled at two colleges in 2017-18 they would only be counted once. Where we show full-time and part-time student numbers this will include multiple enrolments.

In line with last year's report, we have included non-incorporated colleges and SRUC to give a comprehensive picture of performance against the Scottish Government's national target for learning activity.

Scotland's colleges 2019

This report is available in PDF and RTF formats, along with a podcast summary at:
www.audit-scotland.gov.uk

If you require this publication in an alternative format and/or language, please contact us to discuss your needs: 0131 625 1500
or **info@audit-scotland.gov.uk**

For the latest news, reports and updates, follow us on:

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
T: 0131 625 1500 E: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

ISBN 978 1 911494 93 5 AGS/2019/2

Fraud and irregularity update

2018/19

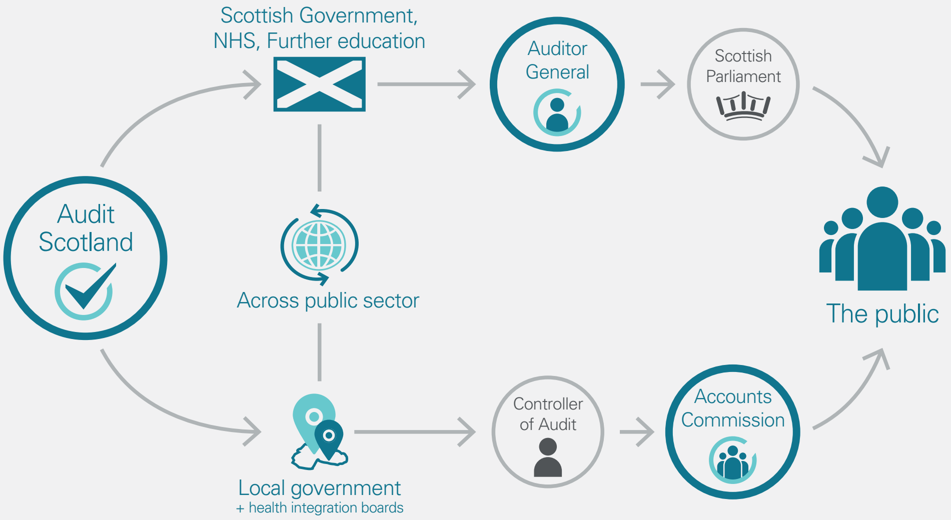
Prepared for public bodies and auditors
July 2019

AUDIT SCOTLAND

Who we are

The Auditor General, the Accounts Commission and Audit Scotland work together to deliver public audit in Scotland:

- **Audit Scotland** is governed by a board, consisting of the Auditor General, the chair of the Accounts Commission, a non-executive board chair, and two non-executive members appointed by the Scottish Commission for Public Audit, a commission of the Scottish Parliament.
- The **Auditor General** is an independent crown appointment, made on the recommendation of the Scottish Parliament, to audit the Scottish Government, NHS and other bodies and report to Parliament on their financial health and performance.
- The **Accounts Commission** is an independent public body appointed by Scottish ministers to hold local government to account. The Controller of Audit is an independent post established by statute, with powers to report directly to the Commission on the audit of local government.



About us

Our vision is to be a world-class audit organisation that improves the use of public money.

Through our work for the Auditor General and the Accounts Commission, we provide independent assurance to the people of Scotland that public money is spent properly and provides value. We aim to achieve this by:

- carrying out relevant and timely audits of the way the public sector manages and spends money
- reporting our findings and conclusions in public
- identifying risks, making clear and relevant recommendations.

Contents

Summary

Key messages

- **External auditors have reported a variety of fraud and irregular activities across a range of Scottish public bodies during 2018/19.**

- **During 2018/19, external auditors reported 17 cases of frauds and irregularities valued at almost £674,000. The value of reported fraud and irregularity is small compared to Scottish public sector expenditure.**

- **Common control weaknesses have contributed to the fraudulent and irregular activity reported during 2018/19.**

Recommendations

- Public bodies should consider whether the weaknesses in internal control that facilitated the cases identified in this report may also exist in their own organisations and take the required corrective action.

- Auditors should confirm whether internal controls at their audit clients are sufficiently strong to prevent the types of frauds and errors highlighted in this report.

Background

1. This report aims to share information about cases where internal control weaknesses in public bodies have led to fraud and irregularities, to help prevent similar circumstances happening again. It is based on information reported to Audit Scotland about significant frauds and other irregularities in public bodies during 2018/19. The level of fraud and irregularity reported is small compared to Scottish public sector expenditure of £44 billion.

2. A key objective of public audit is to deter fraud. The CIPFA Code of Practice on Managing the Risk of Fraud and Corruption explains that fraud can be prevented through the implementation of appropriate and robust internal control measures that safeguard assets. It follows that weaknesses in internal control increase the risk of fraud.

3. International Standards of Auditing (ISAs) include certain requirements relating to the auditor's consideration of fraud. Audit Scotland's Code of Audit Practice sets out additional responsibilities of public sector external auditors in respect to fraud, error and irregularities.

4. Appointed auditors in Scottish public sector bodies are required to consider the risks and the arrangements put in place by audited bodies to ensure that all material revenue is identified and collected, and that material payments are made correctly.

5. Historically, auditors of local government bodies and non-departmental public bodies (NDPBs) have provided Audit Scotland with details of cases of fraud and other irregularities discovered in those bodies. During 2018/19, we extended this to the college sector.[1] The focus in reporting cases is on highlighting fraud and irregularities caused by weaknesses in internal control and then sharing the learning from these reported cases in order to prevent similar circumstances from occurring.

6. Public bodies are encouraged to consider whether the weaknesses in internal control that facilitated cases in this report may also exist in their own arrangements and take the required corrective action.

7. Auditors should confirm whether internal controls at their audit clients are sufficiently strong to prevent the types of frauds highlighted in this report.

8. The cases in this report include instances where fraud is merely suspected. Such cases are likely to have been investigated internally, but it is not necessary for the police to have been involved or for it to have been proven as fraud in a court of law.

About this report

9. This report has two parts:

- Part 1 (page 6) sets out some key factors that can lead to fraud.
- Part 2 (pages 8 to 15) sets out examples of the various different categories of fraud and irregularity reported during 2018/19 and the control weaknesses which have contributed to these cases.

10. The cases included in this report are based on reviewing documents and returns from external auditors. Our audit methodology is in the Appendix (page 16).

[1] NHS bodies report fraud and irregularities to NHS Scotland's Counter Fraud Service and central government bodies report cases to the Scottish Government.

Part 1

Background

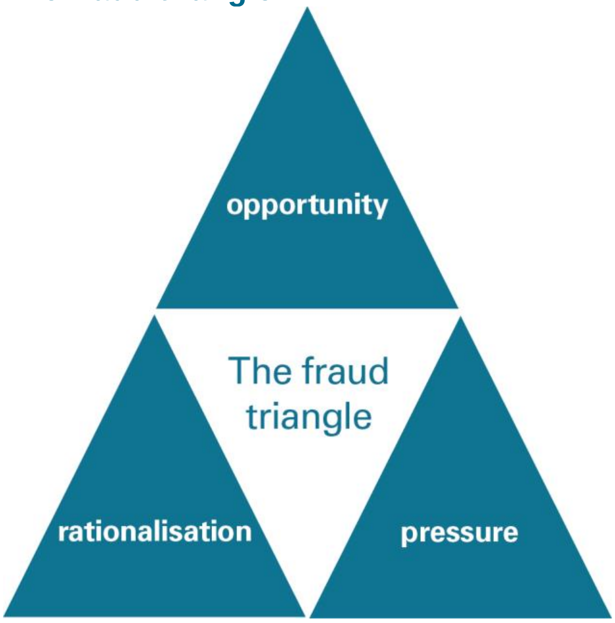
The fraud triangle

11. The fraud triangle is a well-used model to help explain why individuals may commit fraud (Exhibit 1). It suggests that the following are key factors:

- the individual has the opportunity – this may be through weak internal controls such as a lack of segregation of duties
- the individual is under some pressure – this may be personal financial pressures, or through addictions
- the individual can rationalise and justify the fraudulent behaviours in their mind – this may be the belief that they will pay the funds back or that they have been working hard and are due to be compensated.

> Fraud is the misappropriation of assets involving deception to obtain an unjust and illegal financial advantage

Exhibit 1
The fraud triangle



Source: Donald R. Cressey, Other People's Money (Montclair: Patterson Smith, 1973) p. 30.

12. Auditors and management should be aware of key signs in financial records that may indicate fraud. These include:

- an increase in stock or equipment going missing or being written off
- missing documentation to support transactions or contracts
- multiple payments and duplicate payments
- frequent customer complaints about an employee or service, eg the good or service received is less than was requested, or payments are required in cash
- excessive adjustments or 'corrections' through the ledger.

13. There are also behavioural 'reg flags' that are often witnessed when an employee is committing fraudulent activities. Organisations should have systems in place to identify and report any of these behaviours if they appear. These include employees:

- living beyond their means
- getting into financial difficulties or having addictions
- not taking leave
- rewriting records
- being unwilling to share their duties
- developing inappropriate close relationships with customers and suppliers.

14. Auditors continue to engage with audited bodies in order to identify and report fraud and irregularities. The aim is to identify and share events leading to control weaknesses and losses in order to aid learning and hopefully prevent similar events occurring in other audited bodies.

15. Audit Scotland's counter-fraud hub is available on our website and includes details of all of our counter-fraud work, for example, on the National Fraud Initiative, as well as details of the partners we work with.

Management should consider whether the weaknesses in internal control that facilitated cases in this report exist in their own arrangements

Part 2

Examples of fraud and irregularities reported in 2018/19

Key messages

- **Fraud and irregularities reported during 2018/19 fall into the following key categories:**
  - **Six cases of fraud and irregularity involving expenditure have been reported. All six cases, amounting to £82,000, were the result of weaknesses around changing bank details of suppliers.**
  - **Auditors reported four cases of fraud involving income totalling £36,500.**
  - **Two cases of fraud involving payroll have been reported totalling £10,000.**
  - **Three cases of fraud involving theft and totalling £45,000 have been reported.**
  - **Two cases of misuse of assets fraud totalling up to £500,000 have been reported.**
- **Common control weaknesses were identified across organisations where fraudulent or irregular activity was identified.**

Various types of fraud and irregularities were identified during 2018/19

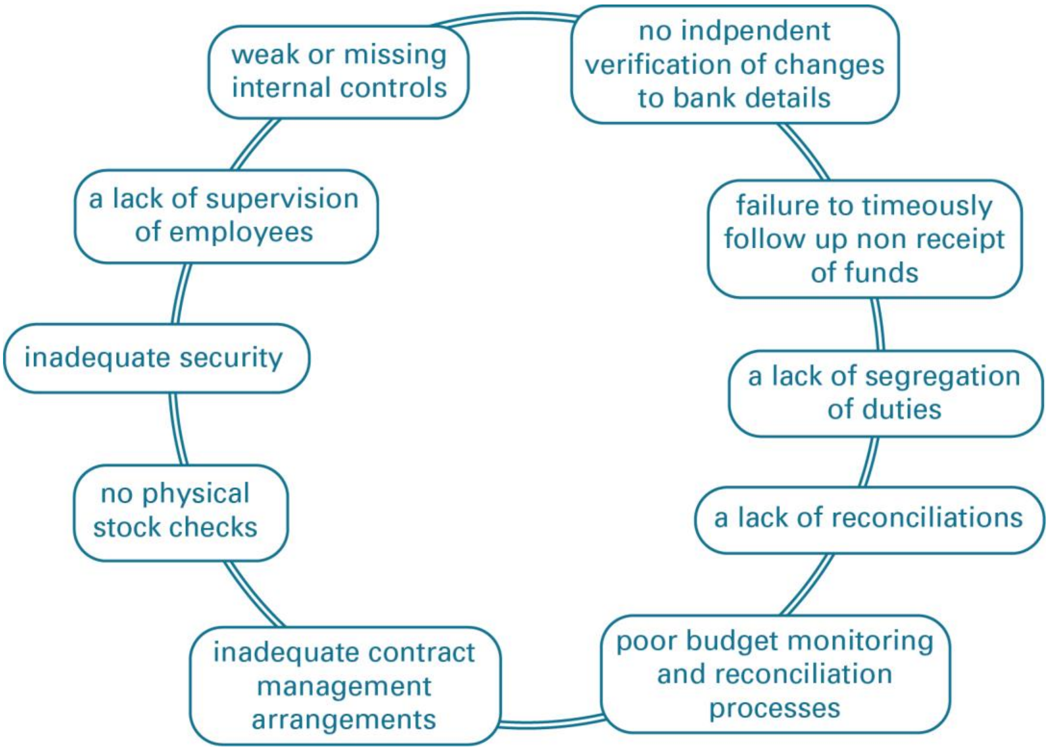
16. The types of reported fraud and irregularities communicated by audit teams to Audit Scotland in 2018/19 include:

- expenditure frauds, where an organisation has incurred additional expenditure because of fraud
- income frauds, including the misappropriation of cash
- payroll overpayments or misappropriations
- theft of assets
- the misuse of assets for personal gain.

17. Common control weaknesses have contributed to the fraudulent and irregular activity reported by external auditors (Exhibit 2, page 9).

This report focusses on fraud caused by weaknesses in internal control

Exhibit 2
Common control weaknesses


weak or missing internal controls
no indpendent verification of changes to bank details
failure to timeously follow up non receipt of funds
a lack of segregation of duties
a lack of reconciliations
poor budget monitoring and reconciliation processes
inadequate contract management arrangements
no physical stock checks
inadequate security
a lack of supervision of employees

Source: Audit Scotland

Expenditure

18. Expenditure frauds relate to cases where a body has incurred additional expenditure because of fraud, eg due to invalid suppliers, fictitious invoicing, or the redirection of payments intended for legitimate suppliers.

Change of bank details

19. Third parties defrauded £82,000 from six public sector bodies by re-directing payments intended for legitimate suppliers.

Key features

The organisations received emails which appeared to be from valid suppliers. The legitimate email addresses had either been hacked or the emails originated from an address very similar to the legitimate email address.

Emails from the fraudulent email addresses requested that bank details were amended. Subsequently a payment was made to the amended bank account.

It was later identified, often when the genuine supplier queried non-receipt of funds, that the new bank details were false.

One organisation was able to recoup £12,000 by promptly contacting Police Scotland and the bank as soon as the fraud was uncovered.

Weakness in internal control

The frauds were possible as:

Weakness: no independent verification of changes to bank details

- no independent verification of the change was undertaken to confirm the change of bank account, eg a phone call to the supplier
- subtle differences from the usual email address were not spotted.

Source: Audit Scotland auditor returns

Income

20. Income frauds relate to cases where a body's income has been misappropriated, eg cash takings being re-directed, or invalid refunds processed.

School fundraising

21. Over £6,000 of cash collected at a school fundraising event was misappropriated by a third party.

Key features

A council organised a fundraising event with one of its suppliers. One of the supplier's employees collected the money but failed to pay the funds to the school.

The head teacher identified that the cash had not been received six months after the event and notified the council's counter-fraud team.

The perpetrator was reported to their employer and the police. £1,200 of the funds have so far been recovered.

Weakness in internal control

The fraud was facilitated by a failure to timeously follow up non-receipt of funds.

Source: Audit Scotland auditor returns

Weakness: failure to timeously follow up non-receipt of funds

Admission ticket sales

22. Perpetrators defrauded £12,000 from an NDPB through fraudulent ticket sales.

Key features

The perpetrators purchased several tickets for overseas events using stolen credit card details, and then re-sold the tickets. The fraud was not identified until the genuine card holders queried the transactions and requested refunds. A subsequent review identified an unusual increase in refunds for disputed card transactions.

The NDPB has now moved to an enhanced card payment system. The IP addresses used for the fraudulent ticket sales have also been blocked.

Weakness in internal control

The fraud was facilitated by a card payment system which did not include secondary authentication for payments.

Source: Audit Scotland auditor returns

Weakness: the card payment system did not include secondary authentication for payments

Fraudulent refunds

23. An employee in a council's environmental services department defrauded £12,500 from the council by failing to bank income and by processing false refunds.

Key features

The employee legitimately sold refuse sacks to residents, but subsequently processed a refund and retained the cash. The individual also identified council tax and housing rent accounts that were in credit, processed a refund for the overpayment, and again retained the cash.

No issues were initially detected as the cash recorded in the ledger agreed to the cash in the till.

The fraud was identified following a review of transactions by the sales ledger team, who identified that it was unusual to expect refunds for refuse sacks. Further investigation identified that refunds were being processed by the same officer for council tax and housing rents payments.

The council has now introduced a daily review of all refunds processed. Council tax and housing rent account credit balances are now being identified and highlighted to customers.

Weakness in internal control

The fraud was facilitated by the absence of regular reviews to highlight unusual items as well as inadequate segregation of duties.

Source: Audit Scotland auditor returns

Weakness: an absence of regular reviews of ledger entries and a lack of segregation of duties

Failure to bank income

24. A housing officer defrauded £6,000 from a council by failing to bank income.

Key features

The officer did not record cash income on income records. The main control was to reconcile the income records to the bank statement, and therefore the missing income was not timeously detected.

The fraud was identified when a finance officer discovered that expected income was not in the relevant bank account. Following investigation, it was established that this income had not been banked and that the issue went back several years.

The council has reviewed its system controls to enable weaknesses to be identified and addressed.

Weakness in internal control

The fraud was possible due to a failure in budget monitoring processes and the income reconciliation process relying upon income details being recorded in the income records.

Source: Audit Scotland auditor returns

Weakness: poor budget monitoring and reconciliation processes

Payroll

25. Payroll frauds relate to cases where an organisation's payroll has been misappropriated, eg employees working elsewhere while claiming to be unfit.

Working while claiming to be unfit for work

26. An occupational therapist defrauded £8,000 from a council by falsely claiming to be unfit for work.

Key features

The occupational therapist was on sick leave for ten months. The fraud was identified when colleagues advised the manager that the size of the employee's private business had expanded significantly during the period of absence. Covert surveillance by the council's counter-fraud team confirmed that the employee was working on a self-employed basis during their period of sickness absence from the council.

Recovery action is in progress. The employee has been dismissed and the case has been reported to the perpetrator's professional institute.

The council had controls in place to prevent this type of fraud, which included requiring employees to seek written permission if they wish to carry out other work whilst on sick leave and regular reviews for employees on long-term sickness absence.

However, despite having these controls in place, the employee was still able to commit the fraud because the employee withheld the fact that they were carrying out outside work and falsely exaggerated the symptoms of their illness at sickness absence reviews.

Source: Audit Scotland auditor returns

Diversion of salary payments

27. A college received a fraudulent request to change employee details for two employees from hacked email accounts. This led to a loss of £2,000.

Key features

The college's payroll team paid the salary of the two employees into the fraudsters' bank accounts instead of the employees' bank accounts. The fraud was uncovered when one of the employees alerted the payroll accounting officer about the non-payment of their salary. In one case, emailed payslips appear also to have been misdirected, revealing personal details.

Weakness in internal control

Payroll did not seek a confirmation from the staff, either in person or on the phone, prior to making a change to bank account details.

Source: Audit Scotland auditor returns

Weakness: failure to obtain confirmation of bank detail changes from employees

Theft

28. Thefts of assets by third parties can be considered fraud if they are facilitated by poor security arrangements, eg theft of equipment or stores.

Embezzlement of care home residents' funds

29. The owner of a council-funded care home defrauded £38,000 from residents.

Key features

The owner of a council-funded care home was not managing residents' funds through individual bank accounts, as required by the contract with the council, so that they could hide the fraudulent transactions.

A council employee responsible for managing the contract initially identified that residents were having financial difficulty and cash flow problems. A subsequent investigation of residents' funds identified unusual bank transfers with a lack of supporting information.

The business owner was reported to the Procurator Fiscal and is awaiting trial but has repaid the funds.

Weakness in internal control

The alleged fraud was facilitated by inadequate contract management arrangements.

Source: Audit Scotland auditor returns

Weakness: inadequate contract management arrangements

Theft of school laptops

30. An unknown third party allegedly stole laptops valued at £7,000 from a school.

Key features

The equipment was allegedly stolen from a secure storage area within the school. The theft was discovered when an employee went to retrieve the equipment prior to use. The matter has been reported to the police.

Weakness in internal control

An internal audit investigation identified physical control weaknesses including:

- key boxes not being locked
- annual asset returns not being completed
- computer equipment not being security marked.

Source: Audit Scotland auditor returns

Weakness: no physical checks of stock and poor security

Theft of prescription drugs

31. An employee stole prescribed drugs from a locked medicine cabinet in a council-run care home and replaced them with paracetamol.

Key features

Internal controls identified that the drugs had gone missing on a particular shift.

Following investigation, a member of staff admitted the theft and resigned. The individual was charged by Police Scotland and received a six-month suspended sentence.

Weakness in internal control

The theft was possible as the keys to the cabinet were used by a number of staff on the shift.

Source: Audit Scotland auditor returns

Weakness: inadequate security of prescription drugs

Misuse of assets

32. Misuse of assets relates to fraud where fraudsters use the assets of a public body for personal gain, eg the use of social housing by people who have no rights to occupy the accommodation

Misuse of vehicles

33. Up to £500,000 was lost to a public body when employees used the body's assets for their own personal gain.

Key features

Employees used the body's vehicles to conduct unauthorised activities for cash payments that required inappropriate use of the vehicles and employee time. The misuse of the vehicles for the drivers' personal gain was discovered when a member of the public called the body's call centre to express his concerns regarding the employees' activities. These concerns were also substantiated by a whistle-blower. Four employees have left their employment as result of these activities. The body is currently assessing opportunities for recovery of the lost revenue.

Weakness in internal control

An internal investigation identified the following weaknesses:

- too much flexibility given to the drivers in scheduling their work
- a lack of monitoring of the driver's activities and the vehicles movements.

Source: Audit Scotland auditor returns

Weakness: a lack of supervision of employees and employees having inappropriate flexibility in respect to work schedules

Tenancy fraud

34. A council tenant was sub-letting their home.

Key features

The fraud was identified following receipt of an allegation of illegal sub-letting. An investigation identified that the tenant was sub-letting the property without proper authority. The property was recovered by the council.

Source: Audit Scotland auditor returns

Appendix

Audit methodology

Audit Scotland's Code of Audit Practice sets out the responsibilities of audit bodies and external auditors in respect to fraud, error and irregularities. The Code states that:

> "Audited bodies are responsible for establishing arrangements for the prevention and detection of fraud, error and irregularities, bribery and corruption and also to ensure that their affairs are managed in accordance with proper standards of conduct by putting proper arrangements in place.
>
> International Standards on Auditing (ISAs) include certain requirements relating to the auditor's consideration of fraud. The nature of public sector organisations means that there are specific fraud risks that are relevant to a public sector audit which should be considered when applying ISA 240. These include taxation receipts, welfare benefits, grants and other claims made by individuals and organisations on the public purse.
>
> Appointed auditors should consider the risks and the arrangements put in place by audited bodies to ensure that all material revenue is identified and collected and that material payments are made correctly.
>
> Audit work would include reviewing, concluding and reporting on areas such as: whether the body has established appropriate and effective arrangements for the prevention and detection of fraud and corruption.
>
> Appointed auditors are required to report information on cases of fraud and irregularities in accordance with guidance from Audit Scotland. Appointed auditors should also review information about frauds disseminated by Audit Scotland and consider whether any action is required in relation to their own audit appointments."

This report is informed by information provided by external auditors during 2018/19 in their fraud and irregularity returns to Audit Scotland.

External auditors are required to report frauds (or suspected frauds) where they are caused or facilitated by weaknesses in internal controls at local authorities or non-departmental public bodies. We extended this to the college sector in 2018/19.

Frauds and irregularities are considered significant where the value of the loss is over £5,000 or where it is of significant due to the nature of the activity.

Auditors of local authorities are not required to report cases of fraud perpetrated by claimants, for example, housing benefit claimants, unless the fraud was facilitated by the collusion of local authority staff or otherwise by weaknesses in internal control.

The cases included in this report are likely to have been investigated internally, but it is not necessary for the police to have been involved or for it to have been proven as fraud in a court of law.

NHS Scotland Counter Fraud Services (CFS) collates and investigates all cases of reported fraud and irregularity in NHS Scotland. CFS deals with the prevention, detection and investigation of fraud, embezzlement, theft, corruption and other irregularities against NHS Scotland.

The Scottish Government collates and ensures appropriate action is taken for all cases of reported fraud and irregularity in the Scottish Government and other central government bodies.

Fraud and irregularity update

2018/19

This report is available in PDF and RTF formats, along with a podcast summary at:
www.audit-scotland.gov.uk

If you require this publication in an alternative format and/or language, please contact us to discuss your needs: 0131 625 1500
or **info@audit-scotland.gov.uk**

For the latest news, reports and updates, follow us on:

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
T: 0131 625 1500 E: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

ISBN 978 1 913287 04 7

Technical bulletin 2019/2

Technical developments and emerging risks from April to June 2019

AUDIT SCOTLAND

Prepared for appointed auditors and audited bodies in all sectors

12 June 2019

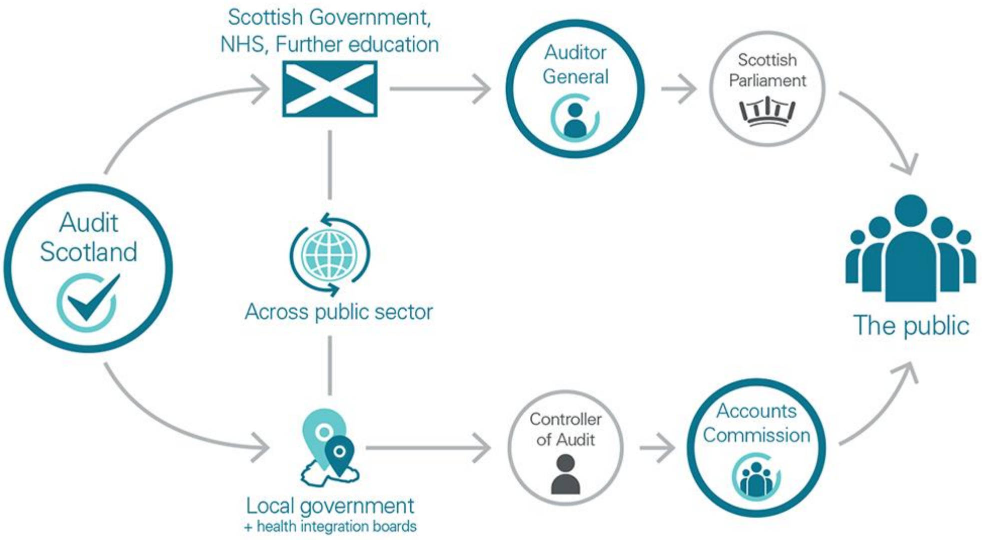
Who we are

The Auditor General, the Accounts Commission and Audit Scotland work together to deliver public audit in Scotland:

- The Auditor General is an independent crown appointment, made on the recommendation of the Scottish Parliament, to audit the Scottish Government, NHS and other bodies and report to Parliament on their financial health and performance.

- The Accounts Commission is an independent public body appointed by Scottish ministers to hold local government to account. The Controller of Audit is an independent post established by statute, with powers to report directly to the Commission on the audit of local government.

- Audit Scotland is governed by a board, consisting of the Auditor General, the chair of the Accounts Commission, a non-executive board chair, and two non-executive members appointed by the Scottish Commission for Public Audit, a commission of the Scottish Parliament.



About us

Our vision is to be a world-class audit organisation that improves the use of public money.

Through our work for the Auditor General and the Accounts Commission, we provide independent assurance to the people of Scotland that public money is spent properly and provides value. We aim to achieve this by:

- carrying out relevant and timely audits of the way the public sector manages and spends money

- reporting our findings and conclusions in public

- identifying risks, making clear and relevant recommendations.

Contents

Introduction

Purpose

1. The purpose of technical bulletins from Audit Scotland's Professional Support is to provide auditors appointed by the Auditor General and Accounts Commission with:

- information on the main technical developments in each sector and on professional matters during the quarter
- guidance on any emerging risks identified in the quarter.

Technical bulletins provide information on developments and guidance on emerging risks

2. The information on technical developments is aimed at highlighting the key points that Professional Support considers appointed auditors require to be aware of. It may still be necessary for auditors to read the source material if greater detail is required. These can be accessed by using the hyperlinks, where provided. They are also available to appointed auditors from the Technical Reference Library maintained by Professional Support on ishare and the Extranet.

3. The actions by auditors recommended by Professional Support in respect of each item are highlighted in red and summarised at the end of each section.

4. Technical bulletins are also published on the Audit Scotland website and therefore are available to audited bodies and other stakeholders.

Highlights summary

5. Particular attention is drawn to nine of the items in this technical bulletin summarised in the following table:

Professional Support has published an update to technical guidance note 2018/10(LG) [see paragraph 7]	The Scottish Government has issued statutory guidance on using capital receipts to fund transformation projects [see paragraph 18]	Professional Support has provided revised guidance on loans fund repayments [see paragraph 30]
Professional Support has provided an update on Guaranteed Minimum Pension [see paragraph 58]	Professional Support has provided guidance on the McCloud judgement [see paragraph 62]	Treasury has issued application guidance on IFRS 16 [see paragraph 98]
Professional Support has published a good practice note on governance statements [see paragraph 130]	The Competition and Markets Authority has issued their final report on the audit market [see paragraph 141]	The Brydon Review has called for views [see paragraph 144]

Contact point

6. The main contact point for this technical bulletin is Paul O'Brien, Senior Manager (Professional Support) – pobrien@audit-scotland.gov.uk.

Feedback on this technical bulletin is welcome

Section 1
Local government sector

Auditing developments

Update to technical guidance note 2018/10(LG)

7. Professional Support has published an update to technical guidance note 2018/10(LG) to summarise the events since the technical guidance note's publication on 19 November 2018 which impact directly on its contents.

8. Auditors have been advised of these events in technical bulletins. The purpose of this update is to pull the events together in one document and set out the auditor actions arising.

Auditor action
Auditors should refer to this update when auditing the 2018/19 annual accounts of local government bodies

2018/19 model independent auditor's reports

9. Professional Support has published 2018/19 independent auditor's report (local government) -Technical guidance note 2019/5(LG) to provide auditors with the model independent auditor's reports which should be used for the 2018/19 annual accounts. The technical guidance note also provides application guidance on their use.

10. In order to comply with section 101(4) of the Local Government (Scotland) Act 1973 which requires the independent auditor’s report to be in the form directed by the Accounts Commission, the Code of Audit Practice requires auditors to use the relevant model report in the appendices of the technical guidance note as a condition of their audit appointment. The only exception to using the wording in each model is to tailor the terminology to reflect local circumstances.

11. The changes to the model independent auditor's reports for 2018/19 are summarised in the following table:

 2018/19 independent auditor's reports (local government) - Technical guidance note 2019/5(LG) AUDIT SCOTLAND Prepared for appointed auditors in the local government sector 11 April 2019	• Additional wording has been added to reflect the requirements in ISA (UK) 700 for public interest entities • A reference has been added to highlight that risks of material misstatement are reported in the annual audit report • A similar reference has been added to highlight that conclusions on wider scope responsibilities are reported in the annual audit report • The ‘Bannerman’ paragraph has been moved from the beginning of the model reports to the end

12. Any proposed modifications to any audit opinion or conclusion, or the inclusion of 'emphasis of matter' or 'other matter' paragraphs, should be discussed with Professional Support in advance of finalising the report.

13. Auditors should use this technical guidance note when reporting on 2018/19 audits. They should complete for each report the checklist at Appendix 6 which provides a list of the key auditor actions.

Auditor action
Auditors should use this technical guidance note when reporting the audit of the 2018/19 annual accounts and complete the relevant checklist

Financial statements developments

Guidance on internal transactions

14. The Local Authority (Scotland) Accounts Advisory Committee (LASAAC) has issued an advisory note to assist local government bodies in implementing changes to the Code of Practice on Local Authority Accounting (the accounting code) for 2018/19 which no longer permit transactions between segments to be reported in the Comprehensive Income and Expenditure Statement (CIES), i.e. they should not be included in income and expenditure in service segments.

15. The note emphasises that:

- the change does not preclude bodies from recording inter-segment transactions for internal management purposes. Adjustments which reconcile a body's management arrangements for segments to the required presentation in the CIES should be included in the Expenditure and Funding Analysis
- the re-allocation of underlying expenditure from one segment to another in the CIES continues to be allowed. This should be accounted for as an increase in the expenditure of the segment that consumed the resources and the reduction in the expenditure (rather than increase in income) of the segment which initially procured the resources.

Reconciling adjustments should be in the Expenditure and Funding Analysis

16. Auditors should confirm that:

- any inter-segment transactions for management purposes during 2018/19 have been removed from both segments in the Expenditure and Funding Analysis
- any underlying expenditure re-allocated between segments in 2018/19 resulted in an increase in the expenditure of the segment that consumed the resources and a reduction in the expenditure of the segment which initially procured the resources.

Auditor action
Auditors should carry out the actions set out at paragraph 16

17. As a consequence of the change to the accounting code, previous LASAAC guidance on accounting for insurance, which recommended internal premiums, is withdrawn.

Use of capital receipts to fund transformation projects

18. The Scottish Government has issued statutory guidance with finance circular 4/2019 which permits councils to use capital receipts to fund projects designed to transform service delivery to reduce costs and/or reduce demand.

Capital receipts can be used to fund eligible expenditure on transformation projects

19. In addition to capital receipts received during the period 2018/19 to 2021/22, any balance on the Severance Provision Statutory Adjustment Account at 31 March 2018 is also eligible to be used under the scheme. Capital receipts in the Capital Fund are not eligible.

20. The eligibility of the expenditure that may be funded from capital receipts is summarised in the following table:

Qualifying	Non-qualifying
Non-recurring, set up and implementation costs including statutory, lump sum severance payments to non-teachers Incurred on a qualifying transformation/service redesign project Incurred during the period from 1 April 2018 to 31 March 2022	Ongoing revenue costs Severance costs related to teachers Severance costs for non-teachers that are simply applying to service cuts or discretionary payments to enhance severance packages

21. Qualifying projects are those which transform service delivery in a way that reduces either the cost of, or demand for, that service in the future. The key criterion is whether the project will generate ongoing savings. It is for each council to demonstrate that a project qualifies. Examples of transformation projects are provided at paragraph 7 of the statutory guidance and include:

- setting up a shared back-office or administrative services with other public bodies
- expanding the use of digital approaches to the delivery of services.

22. The full council must approve the use of capital receipts to fund qualifying expenditure. A report requires to be presented to full council that sets out the:

- total estimated cost of each project
- expected saving/service demand reduction
- types and amounts of qualifying expenditure
- amount of capital receipts planned to be used.

23. Capital receipts to be applied to fund qualifying expenditure cannot be transferred directly to the General Fund. They should first be credited to the Capital Grants and Receipts Unapplied Account as a statutory adjustment. The decision to do so must be taken on receipt. The amount credited in any financial year to the General Fund can exceed the amount of qualifying expenditure for that year. However, over the four-year period, the total capital receipts cannot exceed total expenditure. Any unused capital receipts at 31 March 2022 are to be transferred to the Capital Fund.

The decision on whether to apply capital receipts must be taken on receipt

24. An analysis of the reason for each transfer from the Capital Grants and Receipts Unapplied account to the General Fund requires to be disclosed. Paragraph 29 of the statutory guidance provides suggested descriptors for the analysis.

25. There is a requirement to disclose separately the amount held in the Capital Grants and Receipts Unapplied Account for:

- funding service transformation projects
- capital grants (under finance circular 3/2018)
- equal pay (under finance circular 1/2019).

26. Where a body intends to fund a project from capital receipts in 2018/19, auditors should confirm that the:

- project is a qualifying one

Auditor action
Auditors should carry out the actions set out at paragraph 26

- expenditure meets the eligibility criteria
- capital receipts to be applied have first been credited to the Capital Grants and Receipts Unapplied Account as a statutory adjustment.

Accounting for teachers 2018/19 pay award

27. The Scottish Government has sent an email to local government bodies on accounting for the teachers' pay award for 2018/19. The email explains that the share of the increase funded by the Scottish Government was not included in the redetermination of the 2018/19 general revenue grant (it will instead be included in the 2019/20 grant). The allocation of the £10 million funding is set out in a table.

Funding for the 2018/19 teachers' pay award will be paid as part of 2019/20 grant

28. The email advised that the Scottish Government will accrue their share in their 2018/19 financial statements, and Local Financial Returns for 2018/19 will assume a local government body will accrue the income in that year.

29. In Professional Support's view, it is appropriate for a local government body to recognise its share of the funding as income in 2018/19 as the Scottish Government email provides reasonable assurance that it will be received.

The funding can be recognised in 2018/19

Loans fund repayments – update

30. Auditors will be aware, from technical bulletin 2019/1 (paragraph 26) and from other communications, of discussions that have taken place between Audit Scotland, the CIPFA Directors of Finance Section, CoSLA, the Scottish Government and other stakeholders on the repayment of loans fund advances made prior to 1 April 2016 (pre-April 2016 advances).

31. Professional Support's previous guidance was that pre-April 2016 advances should continue to be repaid as if paragraph 15 of Schedule 3 of the Local Government (Scotland) Act 1975 had not been repealed. That position reflected the treatment set out in statutory guidance contained in finance circular 7/2016, and was on the basis that The Local Authority (Capital Finance and Accounting (Scotland) Regulations 2016 (the 2016 Regulations), which permit other repayment options, did not apply to pre-April 2016 advances.

32. Having carefully considered all the available evidence, including obtaining independent legal opinion, Professional Support is now satisfied that the 2016 Regulations can be applied to pre-April 2016 advances. Specifically, this includes Regulation 14(2) which permits a local government body to vary the period and amount of the repayment if it considers it prudent to do so.

Professional Support is satisfied that the 2016 Regulations can be applied to pre-April 2016 advances

33. While the ultimate judgement rests with each appointed auditor, in Professional Support's view, any local government body wishing to vary the amount and/or period of loans fund repayment of pre-April 2016 advances in 2018/19 has the statutory power to do so subject to the repayment being considered prudent. Similarly, the councils which varied repayment in 2017/18 had the power to so and therefore no restatement in 2018/19 is necessary, again subject to the repayment being considered prudent.

34. The 2016 Regulations do not define prudent repayment, but the statutory guidance explains that it is a repayment which is reasonably commensurate with the period and pattern of benefits provided to the community from the capital expenditure. The statutory guidance also sets out a number of options that are considered to be prudent.

35. In making decisions about prudent repayment, it is important that local government bodies follow appropriate governance processes. The statutory guidance refers to the requirement for the policy on prudent repayment, and any proposed variation of repayments, to be approved by the full council (or equivalent for other bodies).

36. Auditors should:

- confirm that the body's policy on prudent repayment, and any proposed variations of repayments in 2018/19, have been approved by the full council (or equivalent)
- assess whether the policy meets the requirements for prudence set out in the statutory guidance
- assess whether the repayments for 2018/19 comply with the approved policy.

Auditor action
Auditors should carry out the actions set out at paragraph 36

Financial instruments – modified loans

37. The CIPFA/LASAAC Local Authority Code Board has issued an update to the 2018/19 accounting code. The need for the update arises from clarification contained in IFRS 9 Financial Instruments: Prepayment Features with Negative Compensation in respect of loan exchanges which result in the modification (rather than derecognition) of the original loan.

38. The update provides transitional provisions for changes in accounting treatment as a result of the IFRS 9 clarification. The Chartered Institute of Public Finance and Accountancy (CIPFA) has issued Bulletin 3 to explain the accounting treatment. Paragraphs 1 to 18 explain that it involves the new amortised cost of a modified loan being measured using the original (rather than the new) effective interest rate.

The update provides transitional provisions where the accounting treatment for modified loans changes in 2018/19

39. The difference in accounting treatment is therefore summarised in the following table:

IFRS 9	IAS 39
Calculate a new carrying amount by discounting the revised contractual cash flows with the original effective interest rate (resulting in a gain or loss on modification Take the difference between the new carrying amount and the old carrying amount to the Comprehensive Income and Expenditure Statement as a gain/loss on modification Adjust the new carrying amount and recalculate the effective interest rate to amortise any other costs and fees incurred in the modification	Retain the old carrying amount Recalculate the effective interest rate using the revised cash flows

40. The clarification applies on the adoption of IFRS 9 and therefore to the 2018/19 financial statements. Any change in accounting treatment is to be applied retrospectively, but the transitional provisions set out in the code update allow recognition as an opening adjustment to reserves.

41. The update includes tracked changes to appropriate extracts of the 2018/19 accounting code with both new and amended paragraphs forming the revised 2018/19 code.

42. It should be noted that CIPFA's IFRS 9 Financial Instruments - An Early Guide for Local Authority Practitioners does not reflect the amended treatment. Paragraph 14 of bulletin 3 replaces the affected guidance in that early guide.

Financial instruments – negative compensation

43. CIPFA bulletin 3 also provides guidance on IFRS 9 Financial Instruments: Prepayment Features with Negative Compensation more generally. Paragraphs 19 and 20 of the bulletin explain that negative compensation arises in a financial instrument where:

- the contractual terms permit the borrower to prepay the financial instrument before its contractual maturity; and
- the prepayment amount could be less than unpaid amounts of principal and interest.

44. Under the previous IFRS 9 requirements, a lender having to make a settlement payment in the event of termination by the borrower led to the financial asset being classified as fair value through profit or loss (FVPL). The amendment to IFRS 9 allows bodies to classify such assets at amortised cost or at fair value through other comprehensive income (FVOCI) if the relevant criteria are met.

Financial assets with negative compensation can be classified as amortised cost or FVOCI

45. Some local government bodies lend to other entities with prepayment terms at a discount. Where that is the case, bodies will be permitted to apply this amendment in 2018/19 on transition to IFRS 9.

Financial instruments – earmarking unrealised gains

46. LASAAC has issued mandatory guidance on earmarking an element of the General Fund balance arising from the increase in the fair value of financial assets.

47. Under IFRS 9, increases in the fair value of financial assets classified as FVPL are recognised in the General Fund. The guidance requires that an element of the resulting unrealised gains in the General Fund balance should be earmarked as not being available to fund the delivery of services. The element relates to the net cumulative gains arising from increases in fair value to the extent they are not readily convertible to cash.

Gains on FVPL financial instruments in the General Fund should be earmarked if not available to fund service delivery

48. Gains in the fair value of a financial asset are considered to be ‘readily convertible to cash’ if all of the criteria set out in the following table apply:

Criteria	Explanation
Value determination	A value can be determined at which a transaction could occur to convert the change in fair value into cash
Observable information	In determining the value, information that market participants would consider in setting a price is observable (closely aligned with levels 1 and 2 in the IFRS 13 fair value hierarchy)
Immediate conversion	There are no circumstances that prevent the immediate conversion to cash of the change in fair value

49. Even where an increase in fair value meets the above criteria, bodies are required to judge whether it is prudent to use the increase to fund services where the fair value of the asset is considered to be volatile.

50. Where earmarking of the General Fund is required, it should be disclosed in a note along with an explanation.

51. Where there is a net cumulative gain in respect of financial assets included in the General Fund balance at 31 March 2019, auditors should confirm that an element of the balance has been earmarked to the extent the gains are:

Auditor action

Auditors should carry out the actions set out at paragraph 51

- not readily convertible to cash; or
- considered to be volatile.

52. The guidance also applies to any unrealised gains arising from recalculating the carrying amount of modified loans (explained at paragraph 39).

Retirement benefits – 2018/19 report on actuarial information

53. PWC has prepared a report to provide support to auditors when assessing the actuaries who produce retirement benefits figures under IAS 19 Employee Benefits as at 31 March 2019.

54. The work carried out for the report involved assessing the competence and objectivity of, and assumptions and approach adopted by, the relevant actuaries. It found that actuaries signing-off the calculation of the figures are appropriately qualified, and the actuarial firms are experienced and well-reputed. There are no known circumstances which would impair their objectivity to produce the figures.

The report considers the proposed actuarial assumptions to be reasonable in typical cases

55. PWC also consider that the assumptions proposed, when taken together, will produce liability figures in line with their expectations. However, the report advises auditors to consider whether:

- local issues have been adequately covered in instructions issued by employers to actuaries
- to subject the source data provided to the actuaries by employers to further audit procedures as discussed in section 4 of the report
- material significant events have been communicated to the actuary and undertake additional audit procedures as appropriate.

Auditor action
Auditors should evaluate PWC as an auditor's expert before using the report

56. Where intending to make use of the report, auditors are reminded of the need to first evaluate PWC as an auditor's expert under ISA (UK) 620.

Retirement benefits - guaranteed minimum pension update

57. Technical bulletin 2019/1 (paragraph 12) drew auditors' attention to issues related to the indexation of Guaranteed Minimum Pension (GMP). In summary, a pension scheme that was 'contracted-out' of additional state pension arrangements before contracting-out ended on 6 April 2016 is required to provide a GMP to members for contracted-out service between 6 April 1978 and 5 April 1997. If the contracted-out pension benefits are less than the pensioner would otherwise have received, the pension scheme would be required to increase the pension paid to reach the GMP.

The report considers the approaches by actuaries to be reasonable subject to materiality considerations

58. Page 22 of the PWC report (referred to in the previous item) provides a summary of the approach each actuary is taking to GMP indexation. The report considers the approaches to be reasonable on the basis that the likely impact on liabilities is estimated to be low (0.1% of liabilities for those reaching pension age before April 2021 and 0.2% after that date).

59. Paragraphs 71 to 74 of CIPFA bulletin 3 provide guidance on GMP requirements and advise that bodies should liaise with their relevant pension schemes' administrators and consider what evidence is available regarding the potential impact to inform a relevant accounting treatment for 2018/19, e.g. disclosure of a contingent liability.

Auditor action
Auditors should carry out the actions set out at paragraph 60

60. Auditors should:

- consider the likely impacts against materiality levels

- assess whether the accounting treatment in 2018/19 is appropriate.

Retirement benefits – McCloud judgement

61. Auditors will be aware of recent court rulings (generally referred to as the McCloud judgement) regarding transitional provisions in public sector pension schemes being unlawfully age discriminatory which may have implications for the Local Government Pension Scheme (LGPS).

Actuaries are not making allowances for the McCloud judgement

62. The PWC report advises that actuaries are not proposing to make any allowance for the rulings because of uncertainty around an appeal by the UK Government.

63. The CIPFA Pension Network has issued a briefing note to advise that the Government Actuary's Department (GAD) is currently undertaking a scheme level review of the LGPS for England and Wales to:

- assess the scale of the overall impact
- estimate the change in pension liabilities and service cost
- carry out a sensitivity analysis to identify the impact that changes in key factors may have.

GAD is reviewing LGPS in England and Wales

64. The review may assist local government bodies in evaluating the impact on their 2018/19 annual accounts and inform any disclosure within the accounts. It is currently unclear what arrangements will be made to provide similar information for the LGPS in Scotland. Bodies will need to consider:

- whether they have sufficient information, having taken appropriate advice, to amend the pension liabilities
- appropriate disclosures on risks and cash flow uncertainties.

The briefing suggests appropriate disclosures

65. The briefing suggests that disclosure should set out:

- the background and reason for the uncertainty concerning the pension liability (i.e. the court case and implications)
- an indication of the scale of the uncertainty and, if quantification is not currently possible, an explanation of why that is the case
- an indication of 'scheme level' estimates where appropriate and available
- an indication of any uncertainties affecting the cash flows (e.g. appeal by government)
- an explanation of the impact that this may have on funding arrangements, specifically the employer contributions in future years and any deficit recovery plan arrangements.

Auditor action
Auditors should assess whether the accounting treatment/disclosure (e.g. contingent liability) in 2018/19 is appropriate

Pension funds – illustrative accounts for 2018/19

66. CIPFA has issued Preparing the annual report - guidance for LGPS funds (2019) on preparing LGPS annual reports from 2018/19.

67. This guidance represents a general framework for reference purposes only. It identifies the topics that need to be covered and provides illustrations of how these requirements could be addressed in practice, but does not prescribe the format or level of detail required.

This guidance provides illustrations but does not prescribe the format or level of detail

68. There is no requirement for annual reports to follow the ordering or structure of this guidance, and there is no recommended length or layout.

2019/20 accounting code

69. CIPFA/LASAAC has issued the accounting code for 2019/20. It has been prepared on the basis of accounting standards and other pronouncements in effect for accounting periods commencing on or before 1 January 2019 (except for IFRS 16 Leases which will not apply until 2020/21).

IFRS 16 has not been adopted in 2019/20

70. The main changes in the 2019/20 accounting code are as follows:

- Updates to reflect the issue of the IFRS Conceptual Framework 2018.
- Augmented description of adaptations and interpretations.
- Amendment to the Movement in Reserves Statement (MiRS).
- The ability to transfer an element of the revaluation gain to the General Fund.
- Amendments to section 7.1 on financial instruments.

Auditor action
Auditors should assess whether bodies are making the necessary preparations to comply

Updates to reflect the issue of the IFRS Conceptual Framework 2018

71. Section 2.1 of the accounting code has been extensively re-written to reflect the IFRS Conceptual Framework 2018. The main changes are briefly outlined in the following paragraphs.

72. Changes to the qualitative characteristics of useful financial information at paragraph 2.1.2.15 include those set out in the following table:

Subject	Change
Prudence	A reference to prudence has been re-introduced. The paragraph states that neutrality is supported by the exercise of prudence, which it defines as the exercise of caution when making judgements under conditions of uncertainty. It also explains that prudence does not mean requiring more persuasive evidence to support the recognition of assets than the recognition of liabilities
Substance over form	There is an explicit reference to substance over form. The paragraph states that in many circumstances, the substance of an economic phenomenon and its legal form are the same, but when they are not, providing information only about the legal form will not faithfully represent the economic phenomenon.
Measurement uncertainty	The paragraph advises that even a high level of measurement uncertainty does not necessarily prevent an estimate from providing useful information.

73. Paragraphs 2.1.2.28 and 29 contain revised definitions for assets and liabilities which are expressed in terms of economic resources. An economic resource is a right that has the potential to produce economic benefits or service potential. Paragraph 2.1.2.27 also refers to substance over form by stating that, when assessing whether an item meets the definition of an asset or liability, attention needs to be given to its underlying substance and economic reality and not merely its legal form. The new definitions are set out in the following table:

Assets and liabilities are defined in terms of economic resources

Item	Definition
Asset	Present economic resource controlled by the body as a result of past events
Liability	Present obligation of the body to transfer an economic resource as a result of past events

74. Paragraphs 2.1.2.36 and 37 cover the recognition process and criteria by explaining that:

- recognition captures items in the Balance Sheet and CIES that meet the definition of one of the elements of financial statements
- only items meeting the definition of an asset, a liability or reserves are recognised in the Balance Sheet
- only items meeting the definition of income or expenses are recognised in the CIES.

75. Paragraph 2.1.2.38 explains that derecognition is the removal of all or part of an asset or liability from the Balance Sheet, and normally occurs when the item no longer meets the definition of an asset or liability. Derecognition normally occurs when the body:

- loses control of all or part of an asset; or
- no longer has a present obligation for all or part of a liability.

76. Paragraph 2.1.2.54 clarifies that the term measurement basis means either historical cost, fair value or current value.

Measurement bases are historical cost, fair value or current value

Augmented description of adaptations and interpretations

77. Paragraphs 1.2.5 to 1.2.13 explain the application of the code in respect of proper accounting practices. It explains that IFRS may be subject to adaptations or interpretations for the local government context and defines these as follows:

Item	Definition
Adaptation	Amendment to the requirements of a standard
Interpretation	Specifies more precisely how a body is required to apply the requirements in a standard

78. The paragraphs also confirm that that when accounting requirements conflict with statutory requirements, the latter determines what is chargeable to the general fund.

79. Paragraph 1.2.13 explains that IFRS increasingly uses application guidance to support the provisions in standards. Where particularly relevant to local government, such application guidance may be included directly in the accounting code. However, even where that is not the case, if a standard is clear that the application guidance is an integral part of it, bodies are required to refer to that application guidance when relevant transactions, events or circumstances arise.

Application guidance in a standard may have to be referred to

Amendment to the movement in reserves statement

80. An additional line has been added to the MiRS at paragraph 3.4.2.55 for transfers between statutory reserves. This brings the code into line with existing normal practice.

Transferring an element of revaluation gain to general fund

An element of revaluation gain may be transferred to the General Fund rather than Capital Adjustment Account

81. Paragraph 4.1.2.48 allows Scottish local government bodies to transfer the difference between annual depreciation based on the revalued carrying amount of an asset and the depreciation based on the asset's historical cost from the Revaluation Reserve to the General Fund. This is instead of being treated as part of the statutory adjustment and being routed through the Capital Adjustment Account.

82. A line has been added to the MiRS to reflect that option.

Amendment to section 7.1 on financial instruments

83. Paragraph 7.1.1.3 has been amended to clarify the accounting code's interpretation of a loan contract with Lender Option Borrower Option (LOBO) clauses. The interpretation previously stated that LOBO options should not be separately accounted for. The amendment clarifies that the options referred to are only those that allow the lender to increase the interest charge by any amount chosen at specified option exercise dates embedded in a LOBO.

84. Paragraph 7.1.5.6 has been added as a result of IFRS 9 Prepayment Features with Negative Compensation (explained at paragraph 43). It advises bodies to refer to IFRS 9 in the unlikely event that they have previously designated a financial instrument at FVPL.

Grant claims developments

Technical guidance notes for 2018/19

85. Professional Support has published Certification of 2018/19 approved local government grant claims and returns - Technical guidance note TGN/GEN/19 to provide general guidance to auditors on the certification of 2018/19 local government grant claims and returns and to explain the approach and procedures to be adopted. The technical guidance note:

- explains the arrangements for the certification of grant claims and other returns
- provides a list of grant claims and other returns which external auditors are required to certify in 2018/19 under their audit appointment
- considers the roles and responsibilities of Professional Support, grant-paying bodies, local government bodies, and appointed auditors
- sets out the overall approach to be adopted by auditors
- provides guidance on auditor reporting.

86. Professional Support also separately publishes a technical guidance note on each significant approved claim to provide auditors with specific guidance on certifying that claim. The following have been published to date for 2018/19:

- Auditor certification of the 2018/19 housing benefit subsidy claim - technical guidance note TGN/HBS/19
- Auditor certification of the 2018/19 Bellwin scheme claims - technical guidance note TGN/BEL/19
- Auditor certification of 2018/19 education maintenance allowances grant claim - technical guidance note TGN/EMA/19.

Auditor action
Auditors should follow these technical guidance notes when reviewing and reporting on 2018/19 grant claims

Housing benefits

2018/19 HBAP modules

87. The Department for Work and Pensions (DWP) has issued the following modules of the Housing Benefit Assurance Process (Housing Benefits Assurance Process(HBAP) approach to the certification of housing benefit (HB) subsidy claims for 2018/19:

- Module 3 comprises workbooks to be completed for detailed testing, incorporating a test result summary. A Helpfile has been provided separately providing guidance for each cell tested.
- Module 5 contains a control matrix that requires to be completed by auditors. The aim of this module is to ensure that subsidy claims have been completed using the correct software and that the HB system has been internally balanced in terms of benefit 'granted' and benefit 'paid'.

Auditor action
Auditors should use these modules when reviewing 2018/19 subsidy claims

Other circulars

88. The DWP has issued the following adjudication circulars:

- HB Circular A4/2019 provides details on the treatment of disguised remuneration schemes for HB purposes.
- HB Circular A7/2019 provides details of a new 'basis of stay' rules being created for European Economic Area and Swiss nationals under the EU Settlement Scheme (EUSS), and the associated treatment for HB administration purposes.
- HB Circular A8/2019 provides details of how the Windrush Compensation Scheme should be treated for HB administration purposes.
- HB Circular A9/2019 provides clarification on changes to HB policy for mixed age couples which came into force from 15 May 2019. HB Circular S5/2019 (Revised) set out information on funding.

89. The DWP has also issued circulars S4/2019, S6/2019, S7/2019, S8/2019, S9/2019 and S10/2019 to announce funding for various new burdens in 2018/19 and 2019/20.

Non-domestic rates

2018/19 return

90. The Scottish Government has issued the 2018/19 return and accompanying guidance notes for non-domestic rates. The most significant changes from 2017/18 are summarised in the following table:

Line	Relief	Change
8	Fresh Start	Expanded from 50% to 100%, extended to all properties (except payday lending) and is now available to properties unoccupied for six months or more
10a and 11a	Charities and Sports Clubs	Separate analysis required for reliefs to Arm's-Length External Organisations
15	Hydro schemes	Removed from Transitional Relief and replaced under the Renewable Energy Relief scheme

Line	Relief	Change
20	Day Nurseries	New
21	Business Growth Accelerator	New relief for new and improved properties that have been added to the valuation roll on or after 1 April 2018 and re occupied (separately identifying the relief paid in respect of occupied properties, from relief paid as unoccupied new build relief)
22	Unoccupied New Buildings	New relief for new and improved properties that have been added to the valuation roll on or after 1 April 2018 and are not yet occupied
23	Mobile Mast	Separate reporting now required

Whole of government accounts developments

2018/19 guidance

91. Treasury has issued guidance on preparing whole of government accounts returns for 2018/19. There are no significant changes from 2017/18.

92. Professional Support will shortly provide a technical guidance note for auditors.

Wider audit scope developments

Financial management

93. CIPFA has issued a consultation draft of a new Financial Management Code. The draft code is designed to support good practice in financial management and to assist local government bodies in demonstrating their financial sustainability. It is proposed that bodies be required to apply the requirements of the code with effect from 1 April 2020.

94. The draft code is based on a series of principles supported by specific standards and statements of practice which are considered necessary to provide the strong foundation to:

- financially manage the short, medium and long term finances of a local government body
- manage financial resilience to meet foreseen demands on services
- financially manage unexpected shocks in their financial circumstances.

The draft code is based on principles supported by standards and statements of practice

95. Rather than prescribing the financial management processes that local government bodies should adopt, the draft code requires that a body demonstrate that its processes satisfy the principles of good financial management for a body of its size, responsibilities and circumstances. The proposed underlying principles are set out in the following table:

Area	Principle
Organisational leadership	Demonstrating a clear strategic direction based on a vision in which financial management is embedded into organisational culture
Accountability	Based on medium term financial planning which drives the annual budget process supported by effective risk management, quality supporting data and whole life costs

Area	Principle
Transparency	Financial management is undertaken with transparency at its core using consistent, meaningful and understandable data, reported frequently with evidence of periodic officer action and elected member decision-making
Professional standards	Adherence to professional standards is promoted by the leadership team and is evidenced
Assurance	Sources of assurance are recognised as an effective tool mainstreamed into financial management and includes political scrutiny and the results of external audit, internal audit and inspection
Sustainability	The long-term sustainability of local services is at the heart of all financial management process and is evidenced by prudent use of public resources

Guide to capital finance

96. CIPFA has issued an updated Guide to Local Government Finance which includes analysis of capital finance arrangements under the Prudential Code and explanations and definitions of:

- capital expenditure
- credit arrangements
- capital financing, including loans fund repayment arrangements and local authority borrowing.

97. It includes worked examples throughout to illustrate the practical application of theoretical concepts and extracts from the relevant legislation and the Prudential Code.

The guide includes analysis of capital finance arrangements under the Prudential Code

Summary of auditor actions in this section

Paragraphs	Auditor actions
7 - 8	Refer to the update to technical guidance note 2018/10(LG) when auditing the 2018/19 annual accounts of local government bodies
9 - 13	Use technical guidance note 2019/5(LG) when reporting the audit of the 2018/19 annual accounts and complete the relevant checklist
14 - 17	Carry out the actions set out at paragraph 16 in respect of inter-segment transactions and allocations
18 - 26	Carry out the actions set out at paragraph 26 in respect of capital receipts being used to fund transformation projects
30 - 36	Carry out the actions set out at paragraph 36 in respect of loans fund repayments
47 - 53	Carry out the actions set out at paragraph 52 in respect of earmarking unrealised gains in financial instruments
58 - 61	Carry out the actions set out at paragraph 61 in respect of GMP
62 - 66	Assess whether the accounting treatment/disclosure (e.g. contingent liability) in 2018/19 to reflect the McCloud judgement is appropriate

Paragraphs	Auditor actions
70 - 85	Assess whether bodies are making the necessary preparations to comply with the 2019/20 accounting code
86 - 87	Use the applicable technical guidance notes when reviewing and reporting on 2018/19 grant claims
88	Use the HBAP modules when reviewing 2018/19 subsidy claims

Contact points for this section

98. The contact points for this section of the technical bulletin are:

- Paul O'Brien, Senior Manager (Professional Support) - pobrien@audit-scotland.gov.uk
- Anne Cairns, Manager (Professional Support) – acairns@audit-scotland.gov.uk (grant claims items only).

Section 2

Central government sector

Financial statements developments

Leases - IFRS 16 application guidance

IFRS 16 applies from 2020/21

99. HM Treasury has published guidance on applying IFRS 16 Leases to public bodies covered by the Government Financial Reporting Manual (FReM) from 2020/21. IFRS 16 sets out the principles for the recognition, measurement, presentation and disclosure of leases and will replace IAS 17 Leases and related interpretations.

IFRS 16 introduces a single lessee accounting model

100. IFRS 16 introduces a single lessee accounting model that requires a lessee to recognise assets and liabilities for all leases (apart from specified exemptions). This will replace the dual lessee accounting model in IAS 17. At a high level, the IFRS 16 lessee accounting model treats leases in a similar way to finance leases under IAS 17.

101. IFRS 16 retains the definition of a lease in IAS 17 (i.e. a contract that conveys the right to control the use of an identified asset for a period of time in exchange for consideration) but changes the application guidance around how to apply that definition. The most substantive change is around the concept of control used within the definition of a lease.

102. In addition, the definition of a contract (and therefore, of a lease) is expanded to include:

- intra-UK government agreements that are not legally enforceable
- agreements that have nil consideration.

IAS 17 and IFRIC 1 assessments are carried forward on transition

103. The guidance in IFRS 16 on the definition of a lease is only relevant for contracts that are entered into, or amended, after 1 April 2020. However, on transition, bodies are required to carry forward the assessments that were made in accordance with the requirements in IAS 17 and IFRIC 4.

104. IFRS 16 provides two recognition and measurement exemptions that are to be applied in central government as follows:

- All bodies are required to apply the exemption for short-term leases (i.e. with a lease term of 12 months or less).
- The exemption for leases where the underlying asset is of low value is optional for leases entered into from 1 April 2020 and undertaken on a lease-by-lease basis. However, the FReM mandates that there should be no adjustments made for leases of low-value asset leases on transition to IFRS 16.

105. A lessee is required to recognise a right-of-use asset representing its right to use the underlying leased asset and a lease liability representing its obligation to make lease payments.

IFRS 16 cost model to be used as a proxy for current value

106. An interpretation has been introduced in the FReM for the subsequent measurement of right-of-use assets. In most cases, the cost measurement model in IFRS 16 will be an appropriate proxy for current value in existing use

or fair value. However, it will not be appropriate when both of the following conditions are met:

- A longer-term lease has no provisions to update lease payments for market conditions (such as rent reviews), or there is a significant period of time between those updates; and
- The fair value or current value in existing use of the underlying asset is likely to fluctuate significantly due to changes in market prices. This is more likely to be the case with property assets.

107. IFRS 16 includes an overarching disclosure objective that requires lessees to disclose information that enables a user to understand the effect that leases have on the financial position, financial performance and cash flows.

Retrospective restatement as adjustment to opening taxpayers' equity

108. IFRS 16 has been interpreted so that bodies are required to recognise the cumulative effect of initially applying the standard at 1 April 2020 as an adjustment to taxpayers' equity. This should include the elimination of any revaluation reserves associated with existing finance leases.

Employees in LGPS

109. Auditors of any bodies with employees who are members of the LGPS (or other affected schemes) should refer to paragraphs 55 to 67 of the local government section which cover:

- a report on actuaries from PWC
- an update on GMP
- guidance on the McCloud judgement.

Government financial reporting review

110. Treasury has published a document called Government financial reporting review to:

- share the results of its review of progress in government financial reporting since the Simplifying and Streamlining review in 2014
- respond to recommendations from a UK parliamentary committee to make the annual report and accounts more usable and understandable.

111. The parliamentary committee proposed that the four purposes of government financial reporting should be to:

Four proposed purposes of financial reporting

- maintain and ensure the parliamentary control of government spending, enabling the Government to be accountable for its spending
- enable the public and researchers to understand and consider the value for money offered by public spending, so that they can make decisions about the effectiveness, efficiency and economy of particular policies or programmes
- provide a credible and accurate record which can be relied upon
- provide managers with the information they require to run the bodies efficiently and effectively.

112. In order to respond to the recommendations, the Treasury will:

- carry out a zero-based review of the FReM

- establish a bank of best practice examples
- engage with departments to share the findings of the review and support continuous improvement
- publish a map of the financial reporting landscape online and look for other ways to help users navigate financial reports
- carry out regular thematic reviews on specific issues in financial and performance reporting

Treasury to carry out a zero-based review of the FReM

113. Chapters 6 and 7 provide a detailed review of best practice and areas for improvement in government financial reporting. Chapter 8 highlights recommendations and actions to drive continuous improvement in government financial reporting.

Whole of government accounts developments

2018/19 guidance

114. Treasury has issued guidance on preparing whole of government accounts returns for 2018/19. There are no significant changes from 2017/18.

115. Professional Support will shortly provide a technical guidance note for auditors.

Contact point

116. The main contact point for this section of the technical bulletin is Neil Cameron, Manager (Professional Support) – ncameron@audit-scotland.gov.uk.

Section 3
Health sector

Auditing developments

Going concern conclusion

117. Auditors have raised with Professional Support the issue of whether the receipt of brokerage by a health board calls into question the going concern basis of accounting and whether this has implications for the independent auditor's report.

118. ISA (UK) 700 requires auditors to report in accordance with ISA (UK) 570 in respect of going concern. ISA (UK) 570 requires auditors to conclude on:

- the appropriateness of the board's use of the going concern basis of accounting
- whether a material uncertainty exists about the board's ability to continue to adopt the going concern basis of accounting.

Auditors are required to conclude on the appropriateness of the going concern basis of accounting

119. Technical guidance note 2019/3(H) (paragraph 33) advises auditors that, while a health board may face financial sustainability issues, it is highly unlikely that there will be a material uncertainty regarding the use of the going concern basis of accounting or that it would not be considered appropriate. In assessing whether this may be the case, it also advises auditors to refer to the guidance on applying ISA (UK) 570 in practice note 10.

120. Practice note 10 (paragraphs 144 to 159) advises that the operational existence of a public sector body will not always cease as a result of an inability to finance its operations or of net liabilities. Cessation is most likely to result from a legislative change or a decision made by Parliament. The auditor should ascertain whether there is a known intention to abolish, transfer or privatise the activities of the audited body. If there is not, then the going concern basis of accounting is likely to remain appropriate.

121. The FReM interprets the IAS 1 going concern basis of accounting for the public sector. Key extracts are as follows:

- "the anticipated continuation of the provision of a service in the future, as evidenced by inclusion of financial provision for that service in published documents, is normally sufficient evidence of going concern"
- "entities whose statements of financial position show total net liabilities should prepare their financial statements on the going concern basis unless, after discussion with their sponsors, the going concern basis is deemed inappropriate"

122. A health board in receipt of brokerage prepares financial plans demonstrating how it will return to financial balance. Health boards are required to prepare financial plans for three years, as a minimum, which are submitted to the Scottish Government.

123. In accordance with the FReM interpretation, even where a particular health board ceased to exist, the functions that the health board delivered would still require to be provided under the National Health Scotland Act 1978.

124. In Professional Support's view, these expectations are sufficient for a health board in receipt of brokerage to satisfy the criteria set out in the FReM to continue to adopt the going concern basis of accounting. Brokerage therefore does not have any implications on the going concern conclusion in the independent auditor's report.

125. However, auditors should consider the impact of brokerage on their wider scope conclusions on financial management and financial sustainability reported in the annual audit report.

Brokerage does not have implications for the going concern basis of accounting

Review of clinical negligence claims

126. Professional Support has undertaken a review of the work carried out by the NHS Central Legal Office (CLO) relating to the Clinical Negligence and Other Risks Indemnity Scheme (CNORIS). The objective of the review was to establish the extent to which the information prepared using the work of the CLO, as a management expert under *ISA (UK) 500 Audit evidence*, can be used as audit evidence.

127. Professional Support has also evaluated the appropriateness of the methodology adopted by the Scottish Government to establish the total national liability for CNORIS. The review focused on the estimation of the liability as at 31 March 2018 and identified an understatement of £6.321 million in relation to the national liability figures notified by Scottish Government. Following discussions with Scottish Government, they have confirmed that where adjustments are required to the amounts recognised in the financial statements, they would be in a position to amend boards' Annual Managed Expenditure (AME) allocations to provide budget cover, if required.

£6.3 million understatement in national clinical negligence liability

128. Professional Support has provided auditors with the results of the above reviews.

Financial statements developments

Deferral of research and development income

129. Auditors have asked Professional Support for a view on whether it is appropriate for research and development income received from pharmaceutical companies to be deferred. Under the accounts manual, deferred income represents an obligation where a future service is required to be performed before the income can be recognised.

130. IFRS 15 Revenue from Contracts with Customers applies to this income from 2018/19, and requires bodies to follow five steps when recognising income. These steps include identifying the performance obligations in the contract and the transaction price. The transaction price is allocated to the performance obligations in the contract and income is recognised when (or as) the body satisfies a performance obligation.

Research and development income should be recognised as performance obligations are satisfied

131. Professional Support has carried out a review of the contracts in place and confirmed that the board in question has performance obligations that it satisfies on a quarterly basis. It should recognise the income as these quarterly obligations are met. In Professional Support's view, the structure of the reviewed contracts make it unlikely that income would require to be deferred.

Contact point

132. The main contact point for this section of the technical bulletin is Neil Cameron, Manager (Professional Support) – ncameron@audit-scotland.gov.uk.

Section 4

College sector

Non-financial statements developments

New good practice note on governance statements

133. Professional Support has published a good practice note to share the findings from a review of the governance statements in the 2017/18 annual report and accounts of colleges. Some issues for colleges to consider highlighted in the good practice note are set out in the following table:

Auditor action
Auditors should confirm that bodies have considered this good practice note

 Good practice note on improving the quality of college annual report and accounts Governance statements AUDIT SCOTLAND Prepared for colleges and appointed auditors 14 May 2019	Structure the statement in a way that allows a cohesive and clear narrative Include an action plan and progress on implementing previous year action plans Include a clear assessment of whether governance arrangements are fit for purpose Be sufficiently specific so that users can understand why risks are important, and describe the actions to mitigate the key risks Avoid using jargon, or explain it where it cannot be avoided

134. Colleges are encouraged to use the findings in this good practice note to assess and enhance their own 2018/19 governance statements.

Auditor General reports

2017/18 overview

135. The Auditor General has issued Scotland's colleges 2019 to provide an overview of the further education sector in Scotland.

136. The report states that the sector remains financially stable and reported a small, but improved, underlying financial surplus in 2017/18. However, this sector-wide increase masks significant variations between colleges.

137. The report notes that, in calculating and reporting their underlying operating positions, colleges continue to interpret the accounts direction inconsistently. While the differences are small overall, they can be significant at an individual college level.

Inconsistent reporting of underlying operating position

138. Fifteen colleges received funding from arm's-length foundations (ALFs) in 2017/18. Colleges have typically used income from ALFs to fund voluntary severance, capital works and investment in equipment and digital infrastructure. ALF balances vary significantly, with some colleges having little or no scope to access any ALF income. For the remainder of colleges, the ability to apply for income from ALFs is becoming increasingly limited as balances reduce.

Summary of auditor actions in this section

Paragraphs	Auditor action
130 - 131	Auditors should confirm that bodies have considered the good practice note on governance statements

Contact point

139. The main contact point for this section of the technical bulletin is Helen Cobb, Senior Adviser (Professional Support) – Hcobb@audit-scotland.gov.uk.

Section 5

Professional matters

Auditing developments

Consultation paper on Kingman proposals

140. The Department for Business, Energy and Industrial Strategy has issued a consultation paper to takes forward the recommendations from the Kingman Review (explained at paragraph 125 of technical bulletin 2019/1).

141. The UK Government welcomed the Kingman Review's recommendations to establish a new regulator called the Audit, Reporting and Governance Authority (ARGA). Taking some of the recommendations forward will require primary legislation, which the Government intends to introduce as soon as Parliamentary time allows.

142. The consultation splits the various Kingman recommendations into three categories as set out in the following table:

Category	Examples of recommendations
1 Reforms to be taken forward immediately	The publication of audit quality review reports on an anonymised basis Revisiting and strengthening audit quality review resourcing ARGA to promote brevity and comprehensibility in accounts and annual reports, engage meaningfully with users and asset owners about their information needs, and ensure the proportionality and value of reports ARGA to be more sparing and disciplined in promulgating guidance and discussion documents ARGA to develop a robust market intelligence function to identify emerging risks at an early stage
2 Reforms to be delivered in advance of legislation but implementation choices to be considered	ARGA to have a strategic objective to protect the interests of users of financial information The proposed new core functions for ARGA ARGA to be funded by a statutory levy rather than on a voluntary basis
3 Reforms that require primary legislation and require deeper consideration and wider consultation	To work towards a position where individual audit quality inspection reports, including gradings, are published in full upon completion of audit quality reviews The arrangements for local audit in England to be fundamentally rethought, with the role undertaken by a separate body Individual audit quality reviews in relation to the NAO to be shared with the relevant audit committee and Parliament, and published, and apply to all of the NAO's financial audits.

143. This consultation focuses on category 2 recommendations. For example, respondents are asked for comments on ARGA's proposed strategic objective:

Proposed strategic objective
"To protect the interests of users of financial information and the wider public interest by setting high standards of statutory audit, corporate reporting and corporate governance, and by holding to account the companies and professional advisers responsible for meeting those standards."

144. The consultation asks for views on the category 3 recommendations but consultation on detailed proposals will follow.

Statutory audit services market study - final report

145. The Competition and Markets Authority has issued the final report on their market study into statutory audit in the private sector. The report follows discussion with stakeholders on the previous update (covered at paragraph 144 of technical bulletin 2019/1).

146. The report concludes that the market exhibits the following deep-seated problems:

- Audit committees are only a partial solution to the problem that companies select their own auditors.
- High concentration among four big audit firms, resulting in limited choice and a market that is not resilient.
- Audits being carried out by firms whose main business is not in audit.

147. The market, supported by the right regulation, should consistently reward high quality audits above all else, and penalise poor quality. The CMA's recommendations to address the issues identified are summarised in the following table:

The market should reward high quality audits and penalise low quality

Recommendation	Features
Audit committee scrutiny: Audit Committees should come under greater scrutiny by ARGA. This should include selection and oversight of auditors based on audit quality, while also mitigating any bias against non-Big Four firms.	ARGA should: • mandate minimum standards for the appointment and oversight of auditors • monitor compliance with these standards, including placing an observer on a committee if necessary • take remedial action where necessary, for example, by issuing public reprimands or making direct statements to shareholders.
Mandatory joint audit: FTSE 350 companies (unless exempt) to be jointly audited by at least two audit firms.	• At least one joint auditor should be a non-Big Four firm. • ARGA should establish criteria on which companies should be exempted, covering the largest and most complex companies, and those with very simple single-entity accounts. • Any company should also be exempt if it appoints a non-Big Four firm as its sole auditor.
Peer reviews: Companies exempt from mandatory joint audit should instead be subject to periodic peer reviews commissioned by ARGA.	• The peer reviewer should not generally be one of the Big Four. • These should be 'hot' reviews and should report to, and be accountable only to, ARGA. • ARGA should consider how to select peer review targets, either on rotation or incorporating an element of risk assessment, as is the case with its current quality reviews.

Recommendation	Features
An operational split between the audit and non-audit practices of the Big Four: The Big Four to put in place a strong strategic and operational split between their audit and non-audit services practices, including separate governance and strategy, and separate accounts and remuneration policies.	• No profit-sharing between the audit practice and the non-audit practice, with audit partner remuneration linked to the profits of the audit practice only. • Transparent transfer pricing, checked by ARGA, particularly for the use of non-audit specialists on audits. • ARGA should be able to add other firms in later years.
Review of progress: The regulator to set a specific point at which progress can be reviewed (e.g. five years from full implementation) and to assess the effectiveness of the overall package of remedies.	The review should consider in particular: • the merits of moving to independent appointment of auditors • the possible need for a structural split between audit and non-audit services • how to fine tune joint audit to adapt to market developments.

Brydon Review call for views

Review calls for views on quality and effectiveness of audit

148. The Brydon Review (explained at paragraph 148 of technical bulletin 2019/1) has issued a paper calling for views on the quality and effectiveness of audit. The review is examining the existing purpose, scope and quality of statutory audit in the UK, in order to determine:

- the needs and expectations of users of financial and non-financial corporate reporting
- how far the audit process and product may need to improve and evolve to meet the needs of users and to serve the wider public interest
- what specific changes to the statutory audit model and wider regulatory framework for audit may be needed
- whether other forms of business assurance should be developed or enhanced to enable stakeholders to assess better the future financial prospects and sustainability of companies.

149. The paper is requesting views on the extent of assurance that audit currently provides to the users of financial statements, and how it might develop to meet better those users' needs and to serve the interests of other stakeholders and the wider public interest. Many of the proposed changes are already features of public audit in Scotland. Some of the specific points are summarised in the following paragraphs.

Users

150. The paper asks:

- for whose benefit should audit be conducted
- whether the audit should be designed to enhance the degree of confidence of intended users in the company or just in the financial statements
- whether UK law should be amended to provide greater clarity regarding the purpose of an audit, and for whom it is conducted.

Should legislation set out the purpose of an audit?

Wider assurance

151. The paper raises the need for independent assurance concerning the statements made by directors of companies. It discusses whether such assurance should all be delivered through:

- a statutory audit or one commissioned by shareholders; or
- the statutory audit might have two parts, with different liabilities attaching to the providers of the parts and possibly different requirements for independence.

Internal audit

152. The paper explores the interaction between internal and external audit. It notes that, while the international auditing standard allows internal audit to provide direct assistance to the external auditor, the UK standard specifically prohibits this.

Risk management and internal controls

153. The review asks whether:

- directors should make an explicit statement in respect of risk management and internal controls and, if so, should such a statement be subject to audit
- auditors' responsibilities regarding assessing the effectiveness of a company's system of internal control should be extended or clarified.

Should directors make an explicit statement on internal control that is subject to audit?

Unaudited information

154. The paper highlights that information published alongside the audited financial statements in annual reports is not generally subject to audit. Rather, the auditor is required to read it and identify whether the information is materially inconsistent with the financial statements or the auditor's knowledge obtained in the audit, or otherwise appears to be materially misstated.

155. The paper requests views on whether audit or assurance over information outside the annual financial statements (e.g. key performance indicators or non-financial metrics, payment practices or half-yearly reports) enhance its reliability and therefore be of benefit to users.

Should other information be audited?

Audit reporting

156. The paper notes that audit at the moment is largely a 'pass or fail test', and in practice a modified opinion is rare. The review is interested in views on possible models for published auditor reporting that may provide more meaningful insight and narrative, across the whole of the audit or perhaps on particular elements. It asks:

- what additional benefit might a switch from a binary audit opinion to a more graduated disclosure of auditor conclusions provide
- whether further narrative could be disclosed alongside the opinion to provide more informative insights.

Should there be a switch from a binary audit opinion to graduated reporting

Fraud

157. Auditors' responsibilities relating to fraud have been the subject of considerable debate over the years. Recent potentially fraudulent financial reporting practices have again attracted considerable attention which have given rise to renewed debate regarding the nature of auditors' responsibilities for detecting fraud and whether auditors are fulfilling these responsibilities in practice.

158. The paper requests views on whether:

- users' expectations of the role of auditors in fraud detection are consistent with the requirements in UK law and auditing standards
- auditors should be given greater responsibility to detect material fraud
- existing auditing standards help to engender an appropriate fraud detection mindset on the part of auditors
- it would be possible to devise a 'reasonable person' test in assessing the auditor's work in relation to fraud detection
- auditors should be required to evaluate and report on a company's systems to prevent and detect fraud.

Should auditors be given greater responsibility for detecting fraud?

Report on future of audit enquiry

159. The UK Parliament's Business Energy and Industrial Strategy (BEIS) Committee has issued a report on the future of audit. The report sets out the findings from the BEIS's recent inquiry into audit in the private sector which is intended to feed into the Brydon Review and the CMA market study.

The report feeds into the Brydon Review and CMA market study

160. The report includes a number of recommendations including the following:

- Auditors should state how they have investigated potential fraud.
- Audits of companies should be more forward-looking.
- Reporting graduated findings should be mandatory.
- The scope of audit should be extended to cover the entire annual report with different levels of assurance and reporting.
- There should be full legal separation of audit and non-audit services.
- There should be greater reporting on audit fees, potentially including the disclosure of audit hours, staff mix, and rate per hour. Auditors should also report instances where they have performed additional procedures but have been unsuccessful at increasing their fee.
- The potential independent appointment of auditors of companies should be considered with a view to developing it as a viable option if other remedies and reforms fail.
- Joint audits should be piloted in the upper reaches of the FTSE 100 in conjunction with a market cap for the rest of the FTSE 350
- Audit quality reports should be published in full, but not anonymised even in the first instance.
- Audit quality reviews should move beyond process-driven box ticking and offer a robust appraisal of the opinions offered and on the quality of the analysis and evidence used to drive those opinions. This should include reviewing what steps an audit had taken to identify fraud.
- The ARGA should inspect firms' audit software to ensure that it is sound and that the audit trail cannot be tampered with.

Mandatory graduated findings recommended

Scope of audit recommended to be extended to entire annual report

Full publication of audit quality reports recommended

Contact point

161. The contact point for this section of the technical bulletin is Paul O'Brien, Senior Manager (Professional Support) - pobrien@audit-scotland.gov.uk.

Section 6
Fraud and irregularities

162. This chapter contains a summary of fraud cases and other irregularities facilitated by weaknesses in internal control at audited bodies that have recently been reported by auditors to Professional Support.

Auditor action

Auditors should consider whether weaknesses in internal control which facilitated each fraud may exist in their bodies and take the appropriate action

Expenditure

Social work direct payments

163. A council was defrauded of over £55,000 by recipients of social work direct payments over a six-year period.

Key features

Following an assessment of care needs for a social work client, relatives received direct payments to pay for the assessed care.

Subsequent checks on the use of the bank account were not undertaken in accordance with scheduled timescales. When a check was eventually carried out, it identified spending that was outwith the care identified in the care plan. The bank account was also being used for other purposes including funds being transferred to and from a personal bank account and cash withdrawals. The multiple uses of the account was in breach of the service agreement, which states that a bank account must be opened for the sole purpose of managing direct payment income and expenditure.

A direct payment option has been removed for this particular case and the frequency of checks of direct payment spending in all cases has been increased. A recent internal audit review has confirmed improved controls within direct payments, whilst highlighting further areas where improvements can be made. To date £50,000 has been repaid.

Change of bank details

164. A third party defrauded £5,000 from a public sector body by hacking into a staff email account and re-directing payments intended for legitimate suppliers.

Key features

A member of staff received an email, purporting to be from another staff member, containing an invoice where the bank details had been amended. This email was then passed through to finance and paid.

The fraud was identified when the genuine supplier sent a reminder invoice. Investigations then revealed that the staff email account had been hacked.

The fraud was possible as the established procedure to independently verify a change of bank details was not followed.

Income

Non-domestic rates income

165. A third party purporting to be a business owner made a non-domestic rates payment of £6,000 to a council using a stolen credit card and then subsequently requested a refund.

Key features

The perpetrator contacted the council and stated that they had leased commercial premises. The council amended their business rates records and created a liability for business rates. The perpetrator made a £6,000 payment but then reported that they had terminated the tenancy and requested that it be refunded.

A business rates employee reported the case as being suspicious. Inquiries established that the business was fictitious and that the payment had been made using a stolen credit card. It was also established that the perpetrator had undertaken similar scams with several councils in England.

The bank account to which the refund would have been, and other bank accounts related to the perpetrator, were ‘red flagged’ to the banks. A £6,000 refund was made to the bank associated with the stolen card. Guidance on the fraud vulnerabilities in the rates system has been produced and disseminated to all relevant employees.

Misappropriation of income and misuse of assets

166. Up to £500,000 of potential income was lost to a public body when employees used the body’s assets for their own personal gain.

Key features

Employees used the body’s vehicles to conduct unauthorised activities for cash payments during work hours.

The fraud was discovered when a member of the public and a whistle-blower both contacted the body to report their concerns regarding the employees’ activities. An internal investigation identified the fraud was possible due to:

- too much flexibility given to the drivers in scheduling their work
- a lack of monitoring of the driver’s activities and the vehicles’ movements.

Four employees have left the body’s employment as result of these activities. The body is currently assessing opportunities for recovery of the lost revenue. An action plan has been put in place to strengthen controls.

Payroll

Diversion of salary payments

167. A third party defrauded £2,000 from a public body by hacking staff email accounts to request changes to employee details.

Key features

The payroll team received instructions to change bank account details for two employees by email. The emails appeared genuine and, in both cases, a reply was given, and a further response received.

Payroll then paid the salary of the two employees into the new bank accounts. The fraud was uncovered when one of the employees alerted payroll about the non-payment of their salary. In one case, emailed payslips appear also to have been misdirected, revealing personal details.

The fraud was possible as payroll did not seek independent confirmation from the employee, either in person or on the phone, prior to making a change to their bank account details.

Contact point

168. The contact point for this section of the technical bulletin is Anne Cairns, Manager (Professional Support) – acairns@audit-scotland.gov.uk.

Technical bulletin 2019/2

If you require this publication in an alternative
format and/or language, please contact us to
discuss your needs: 0131 625 1500
or **info@audit-scotland.gov.uk**

For the latest news, reports
and updates, follow us on:

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh, EH3 9DN
T: 0131 625 1500

Dumfries & Galloway College

Agenda Item No 9
Audit 01.10.19

Audit Committee

DRAFT – ANNUAL REPORT OF THE AUDIT COMMITTEE 2018-19

1 PURPOSE OF REPORT

1.1 To advise the Board of Management of the activities and decisions of the Audit Committee during Financial Period 2018-19 and to provide opinions on matters specified by the Code of Audit Practice.

2 BACKGROUND TO REPORT

2.1 It is a requirement of the Code of Audit Practice and the College's Standing Orders and Financial Regulations that the Audit Committee provides the Board with an Annual Report so that all members of the Board can be fully informed of, amongst other things, aspects of the system of Internal Control.

3 ADMINISTRATIVE MATTERS

3.1 The period covered by this report is the twelve-month period 1 August 2018 to 31 July 2019.

3.2 The membership of the Committee during the period was:

Hugh Carr, Chair
Naomi Johnson
Pat Kirby
Stuart Martin (retired 2 March 2019)
Robbie Thomas (from 1 September 2018)

3.3 Other attendees at Audit Committee meetings include:

Carol Turnbull (Principal)
Andy Glen (Vice Principal)
Andy Wright (Vice Principal)
Brian Johnstone (Regional College Chair)
Ann Walsh (Board Secretary)
Karen Hunter (Head of Finance)
Heather Tinning (Minute Taker)
Rob Barnett (RSM)
David Eardley (Scott-Moncrieff)
Claire Gardiner (Scott-Moncrieff)
Philip Church (RSM)
Katy Matkin (RSM

3.4 During the relevant period, the Committee's formal meetings were as follows:

Date of Meeting:	Board members present:
19.09.18	Hugh Carr Naomi Johnson Robbie Thomas
13.11.2019	Hugh Carr Naomi Johnson Robbie Thomas
19.02.2019	Hugh Carr Pat Kirby Robbie Thomas
21.05.2019	Hugh Carr Pat Kirby Robbie Thomas

There was an average attendance of 3 members (60%).

4 INTERNAL AUDIT

4.1 RSM acted as internal auditors throughout the year.

4.2 RSM have provided their Annual Audit Report for 2018-19. The opinion for the 12 months ended 31 July 2019 was as follows:

'***Head of internal audit opinion 2018-19***

Our student funding reviews, Student Activity Data and Student Support Funds, concluded that substantial assurance could be taken that the controls were both adequately designed and applied consistently. We raised two medium and two low management actions across both areas to improve the application of the College's control framework.
Financial Forecasting and Planning continues to be a key focus for the Scottish Funding Council (SFC), and we confirmed the College has an appropriate control framework in place that resulted in a substantial assurance opinion. We did raise two medium management actions to improve the financial forecasting framework in place at the College.'

A copy of the full report is detailed in RSM's Annual Internal Audit Report - Year ended 31st July 2019.

4.3 A summary of the internal audit undertaken, and the resulting opinions, is provided below:

Assignment	Assurance level	Uncategorised	Actions agreed		
			L	M	H
Student Activity Data	Substantial assurance		0	2	0
Student Support Fund	Substantial assurance		2	0	0
Health & Safety	Reasonable assurance		2	2	0
Creditor Payments	Reasonable assurance		2	4	0
Follow Up			1	2	0
Equality & Diversity	Substantial assurance		3	1	0
Financial Planning & Forecast	Substantial assurance		0	2	0
Total (2018-19)			**10**	**13**	**0**
Total (2017-18)			12	6	0

4.4 The recommendations are categorised by the auditors according to the level of priority – High, Medium and Low, and are prioritised to reflect the auditors' assessment of risk associated with the control weaknesses.

In addition, Suggestions may be included as part of the Action Plan reported. These are not formal recommendations that impact the overall audit opinion but used to highlight a suggestion or idea that management may want to consider.

13 of the recommendations made during the year were categorised as Medium Priority, with 10 categorised as Low Priority.

No High Priority management actions were made during the year.

4.5 Where a recommendation is not accepted this is documented in the individual audit reports considered by the Audit Committee. In general, recommendations may not be accepted where it is considered that the benefits of implementation are outweighed by the costs.

4.6 RSM undertook six audits of the control environment that resulted in formal assurance opinions. These six reviews concluded that two reasonable (positive) assurance and four substantial (positive) assurance opinions could be taken. The reviews identified the College had established control frameworks in place for a number of the audits undertaken.

Furthermore, the implementation of agreed management actions raised during the course of the year are an important contributing factor when assessing the overall opinion on control. RSM have performed a follow up and during the year which concluded in reasonable progress being made towards the implementation of those actions.

4.7 A procurement exercise was carried out to re-tender the Internal Audit contract. A mini-competition was carried out using the APUC Framework Agreement for Internal Audit Services, and four submissions were evaluated for Price and Quality. RSM were re-appointed following the evaluation.

5 EXTERNAL AUDITORS

5.1 The external auditors throughout the period were Scott Moncrieff Chartered Accountants, Exchange Place 3, Semple Street, Edinburgh.

5.2 The external auditors were appointed by Audit Scotland for the five-year period 2016-17 to 2020-21.

5.3 The fundamental objective of the planning, approach and execution of the audit is to enable the auditors to express an opinion on whether or not the financial statements, as a whole, give a true and fair view of the activities of the College since the last audit and of its state of affairs as at the Balance Sheet date.

5.4 We confirm that the external auditors have been approved by the Auditor General in accordance with the Code of Audit Practice and the letter from the Auditor General dated 20 April 2000 for provision of external audit services for the financial period 2018-19.

5.5 The external audit of the financial statements for the period ended 31st July 2019 commenced in September 2019, and Scott Moncrieff are expected to issue their report 'Dumfries and Galloway College 2018-19 Annual Audit Report to the Board of Management and the Auditor General for Scotland' in November.

6 THE FINANCIAL STATEMENTS

6.1 The External Auditors will provide their Annual Report to the Board of Management following completion of their work as noted above

7 VALUE FOR MONEY PROGRAMME (VFM)

7.1 The Scottish Funding Council requires internal audit to provide an appraisal each year on the College's arrangements for value for money. We have considered the College's creditor payments process and undertook substantive testing to confirm its application, this resulted in a reasonable assurance opinion. A summary of internal audit work undertaken, and the resulting conclusions, is provided at Appendix B.

7.2 Both reviews resulted in reasonable assurance opinions and management actions were raised to improve the control framework.

8 OTHER MATTERS

8.1 There are no matters arising from trusts, joint ventures, subsidiary or associated companies.

8.2 There were no issues of alleged fraud/irregularity investigated during the audit period.

8.3 There are no foreseeable events that will affect the work of the Audit Committee.

9 GOOD GOVERNANCE

9.1 In line with the 'Code of Good Governance for Scotland's Colleges' the College Internal and External Auditors have access to the Audit Committee members to discuss any issues without College staff being present.

9.2 At the Audit Committee meeting on 13 November 2018, the Chair invited Philip Church to feedback to the committee on any issues or concerns that RSM wished to draw to the committee's attention. Philip spoke positively of the relationship between Internal Audit and Management and stated there were no issues or concerns to report to the committee. He spoke positively of the standard of controls tested and reviewed by Internal Audit, and of the approach taken to implementing recommendations made, noting that this gave an encouraging view of the overall standard of control and governance in the college.

10 OPINION

10.1 The Audit Committee's opinion will be reported for the final report following completion of the Financial Statements audit, when the External Auditors' reports are available.

11 RECOMMENDATION

11.1 It is recommended that the Board take note of the work of the Committee for the period August 2018 to July 2019.

Cyber Security Update

1 Purpose of the Report

The purpose of this report is to provide the Audit Committee with an update on Cyber Security.

2 Cyber Security Update

The College is currently working towards the renewal of the Cyber Essentials certification. This renewal has been held back whilst the team carry out essential upgrading of the network backup infrastructure which forms part of our cyber security defenses. With this work now fully complete the renewal will be sent through and completed by the end of October 2019.

The ICT Manager has been continuing to work with the Chief Information Security Officer (CISO) from Higher Education Further Education Shared Technology and Information Services (HEFESTIS) and the ICT team to plan the way forward to achieve Cyber Essentials Plus
The current forecast is that the College would aim to achieve this by October 2020 and will begin to work with the wider College in implementing the requirements for Cyber Essentials Plus before the end of 2019.

As part of the SoSEP project the College are upgrading the wireless network across the Estate and also the network switch at Stranraer. These upgrades will feature enhanced identity and access management to further protect network assets

Within the ICT budget this year the request has been made for a new next generation anti virus software as well as new webmail filtering software. Both of these packages will increase the Colleges security defenses significantly and assist in the achievement of Cyber Essentials Plus.

Darren Morton - Infrastructure Officer, will be undertaking training to become a Systems Security Certified Practitioner. This will mean the College has a fully trained member of staff specialising in cyber security. This is a major step forward and shows that the College is fully committed to investing in our team and ensuring cyber security is our foremost thought at all times.

3. Recommendations

Members are asked to note the report and continue to monitor Cyber Security activities.

Calum Rogers
ICT/IS Manager
September 2019

Agenda Item No 11
Audit 1.10.19

Audit Committee

Strategic Risk Register

1 Purpose of the Report

1.1 The purpose of this paper is to provide the Committee with the opportunity to review the College’s Strategic Risk Register.

2 The Report

2.1 The Principal and Executive Leadership Team routinely review the Strategic Risk Register to reflect the risks the College is facing and the mitigation that will be applied to each risk. There are currently 21 strategic risks, 4 of which are rated 9 (Amber = Significant risk) or above.

There are 5 risks identified that have specific oversight from the Audit committee. Risk 3.6 has been changed as follows:

Risk 3.6 – Failure to achieve ambitions of ICT strategy; strategy and development is ineffective, programme of change not achieved. This risk score has been changed to reflect a failure to replenish the ICT Estate, post mitigation score remains.

3 Recommendation

3.1 It is recommended that the Committee consider and, if so minded, approve the Strategic Risk Register.

Joanna Campbell
Principal
October 2019

Dumfries and Galloway College

Strategic Risk Register 2019-20

Post Holders						
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
1	**Strategic and Structural**									
1.1	Failure of College strategy to meet the needs of Dumfries and Galloway Region and/or national priorities (eg Employability, DYW, attainment, articulation)	4	4	16	• Robust strategic planning • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice • Concerted demands for increased activity levels	4	1	4	• Robust monitoring via ROA • Clear performance metrics • Amendment of strategic direction/plans • Rolling curriculum review	Board, ELT BoM
1.2	College may be disadvantaged by changes to either UK or Scottish Government policies	4	3	12	• Effective environmental scanning • Negotiation/influence at national level	4	2	8	• Review of changes and amendment of strategic direction/plans • Financial strategy sensitivities	ELT BoM
1.3	College disadvantaged by changes arising from UK leaving European Union	3	4	12	• Negotiation/influence at national level • Review of activities/ projects • Responsiveness to new opportunities	2	2	4	• Review of changes and amendment of strategic direction/plans/ curriculum • Financial strategy not ESF dependent	ELT BoM

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Dumfries and Galloway College **Strategic Risk Register 2019-20**

Post Holders						
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility/ Committee Oversight
2	Financial									
2.1	Change in SFC Funding Methodology and Allocation – Reduction in Funding	3	3	9	• Negotiation/influence at national level • Contingency plans for reduced funding	2	3	6	• Advance modelling of new funding methodologies and allocations • Monitoring impact of changes • Amendment of strategic or operational direction/plans • Financial strategy sensitivities	ELT F&GP
2.2	Failure to achieve institutional sustainability	5	4	20	• Protection of funding through dialogue with SFC • Robust annual budget-setting and multi-year financial strategic planning (from 2018-19) • Effective budgetary control • Where required, swift action to implement savings	4	4	16	• Regular monitoring of budgets • Regular review of financial strategy and non-core income sensitivity • Financial forecast requires a clear programme of transformation to achieve financial sustainability.	ELT BOM HoF F&GP
2.3	Salary and conditions of service pressures outstrip ability to pay	4	4	16	• Influence within Employers Association • Management of staffing expenditures	4	3	12	• Expenditure modelling • On-going discussions with staff • Financial strategy sensitivities	ELT HoHR F&GP

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Dumfries and Galloway College **Strategic Risk Register 2019-20**

Post Holders	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility/ Committee Oversight
2	**Financial (cont.)**									
2.4	Financial Fraud	4	3	12	• Strong financial controls: segregation of duties and review of transactions • Review of impact of any changes in structure or duties • Whistleblowing arrangements	3	2	6	• Continuous review of financial controls • Internal Audit programme	HoF Audit
2.5	Failure to achieve credit (activity) target	5	3	15	• Real time monitoring system • Identify & implement additional/alternative provision where required	4	1	4	• Continuous review of progress v targets.	ELT F&GP
2.6	Insufficient Student Support Funding to meet demand.	4	5	20	• Strong financial monitoring • Possible opportunity to request additional in year funding	4	2	8	• Continuous monitoring of demand v funding allocation • Ongoing dialogue with Scottish Funding Council. Confirmation received from SFC that full amount of additional funding requested would be allocated	PRIN HoF F&GP

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Dumfries and Galloway College

Strategic Risk Register 2019-20

Post Holders	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3	Organisational									
3.1	Legal actions; serious accident; incident or civil/criminal breach	4	5	20	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes	3	2	6	• Monitoring and reporting in key areas – eg H&S, equalities, employee engagement • Continuous professional development • Internal audit programme • Staff surveys	ELT BoM
3.2	Reputational Risk – Loss of reputation with key stakeholders	4	3	12	• Marketing strategy • Positive marketing approaches	4	2	8	• Stakeholder engagement • Social media monitoring arrangements	PRIN VPBD&CS HoP&Q BoM
3.3	Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures	5	4	20	• Sound systems of administration • Clear fire and disaster recovery arrangements • Staff CPD	5	1	5	• Business Continuity Plan including scenario testing	ELT HoCS BoM
3.4	Failure to meet Prevent and related obligations	5	3	15	• Prevent training • Staff awareness and contingency planning • Engagement/practice sharing with local agencies	5	1	5	• Business Continuity Plan including scenario testing • Information sharing with local agencies	VPBD&CS HoCS **BoM**

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Post Holders						
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	**Impact**	**Likelihood**
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	**POTENTIAL CONTRIBUTING FACTORS**				**TREATMENT**	**POST MITIGATION EVALUATION**				
	Risks	**Impact**	**Likelihood**	**Score**	**Mitigation Actions**	**Impact**	**Likelihood**	**Score**	**Monitoring**	**Responsibility /Committee Oversight**
3	**Organisational (cont.)**									
3.5	Industrial Relations Problems (including industrial action)	4	1	4	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes • Industrial action continuity planning	4	1	4	• Regular union/management dialogue • Regular employee engagement monitoring • Open communication with staff • JNCC now in place	ELT HoHR HR L&T
3.6	Failure to achieve ambitions of ICT strategy; strategy and development is ineffective, programme of change not achieved	4	4	16	• Planning, careful phasing of changes to processes, systems and equipment • Effective management of ICT arrangements Replenish of ICT Estate	4	2	8	• Regular review/reporting on milestones, systems effectiveness etc • Regular CPD • Rolling programme of updates to systems and equipment	VPBD&CS HoCS VP L T & SE Audit
3.7	Breach of ICT/Cyber security	4	3	12	• Effective management of ICT arrangements • Active ICT/data security monitoring and cyber security policy	4	2	8	• Staff CPD on cyber security issues • Regular security monitoring/testing • Cyber resilience plan	VPBD&CS HoCS Audit

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3	Organisational (cont.)									
3.8	Breach of data security/data protection	5	4	🟥 20	• Effective management of ICT arrangements and GDPR compliance • Mandatory staff CPD and awareness raising on data protection (relative to role)	4	2	🟩 8	• Active data protection monitoring and auditing • Effective information and data security policies in operation • Regular data security monitoring/testing • GDPR Action Plan	VPBD&CS, HoCS Data users Audit
3.9	Failure to reach aspirational standards in learning, teaching and service delivery	4	4	🟥 16	• Clear quality arrangements and priority actions • Continuous self-evaluation and action planning • Introduction of Academic Board, and new random checks of core packs • Rigorous CPD arrangements in place • Regular classroom observation and learner feedback arrangements	4	3	🟧 12	• Comprehensive monitoring of key PIs and student/staff feedback • Regular Stop and Review events • External review and validation findings • Current PI report indicates no significant improvement in retention at this moment	VPL&S, VPBD&CS HoP&Q HoC L&T
3.10	Failure to achieve/maintain compliance arrangements, eg contracts; awarding bodies; audit	4	3	🟧 12	• Robust strategic planning and monitoring • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice	2	2	🟩 4	• Effective internal monitoring/review/verification arrangements • External review findings	PRIN CLT Audit

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3	Organisational (cont.)									
3.11	Failure to meet the deadlines in our successful bid to SoSEP regarding the provision of Hub and Spoke model for Engineering, Construction and Care	3	4	12	• Robust project planning in place and feedback via EMT to Board of Management • Clear and consistent approach to the project with Borders College • Independent scrutiny through clerk of works (for building works) • SFC involvement at all stages of the project	3	3	9	• Curriculum development planning through L&T Committee • Overall project through regular Board of Management updates • Further scrutiny through SoSEP Board	PRIN VP BD&CS VP L&S BoM
3.12	Failure to reach contractual agreement with CITB regarding delivery of Construction related Apprenticeships	4	4	16	• National issue, discussions with CITB, SQA now escalated to include SDS and Scottish Government • Request to defer new qualification until 2019/20 being considered by SQA regulatory body	4	1	4	• Agreement has been reached on settlement for 18/19 and 19/20 • Colleges to review assessor/verifier arrangements going forward	PRIN VP L&S CM BoM

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk