AUDIT & RISK ASSURANCE COMMITTEE

AGENDA

A meeting of the Audit & Risk Assurance Committee will be held at 15:00 hours on Wednesday 25 November 2020 via Microsoft Teams.

		Lead Speaker	**Paper**
1	WELCOME & APOLOGIES	Chair	
2	DECLARATIONS OF INTEREST	Chair	
3	MINUTES OF PREVIOUS MEETING ***for approval***	Chair	A
4	MATTERS ARISING REPORT		
	4.1 Matters Arising Update	Chair	B
	4.2 Business Committees of the Board Update		
	• Policy & Resources Committee	Chair	Verbal
	• Corporate Development Committee	L Drummond	Verbal
	• Academic Council	J Sischy	Verbal
5	INTERNAL AUDIT REPORTS		
	5.1 Internal Audit Report: EMA Audit	BDO	C
	5.2 Internal Audit Report: Student Support Funds	BDO	D
	5.3 Internal Audit Report: Job Retention Scheme	BDO	E

Item 5 is presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 30, Prejudice to the Effective Conduct of Public Affairs

6	RISK ASSURANCE		
	6.1 Risk Management Report	N Croft	F

Item 6.1 is presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 30, Prejudice to the Effective Conduct of Public Affairs

7	ANNUAL REPORT AND FINANCIAL STATEMENTS 2019/20		
	7.1 Draft Annual Report and Financial Statements for the Period Ended 31 July 2020	L Towns	G
	7.2 Draft Independent Auditor's Report and Letter of Representation	Audit Scotland	H
	7.3 2019/20 Draft Annual Audit Report	Audit Scotland	I

Item 7 is presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 27, Information Intended for Future Publication.

8	DRAFT AUDIT & RISK ASSURANCE COMMITTEE ANNUAL REPORT TO THE BOARD 2019/20	Chair	J

Item 9 is presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 27, Information Intended for Future Publication.

9	ANY OTHER COMPETENT BUSINESS		
	9.1 Evaluation of Internal Audit 2020/21	Chair	K

Item 9 is presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 30, Prejudice to the Effective Conduct of Public Affairs

10	FOR INFORMATION		
	10.1 Summary of Audit Recommendations Update		L
	10.2 Internal Audit Progress Report		M
	10.3 Annual Report on Data Breach Incidents and Cyber Attacks		N **Attached**
	10.4 Horizon Scanning Report		O **Attached**
	10.5 Audit & Risk Assurance Committee Business Planner 2020/21		P **Attached**

Items 10.1 and 10.2 are presently exempt from publication under the Freedom of Information (Scotland) Act 2002, Section 30, Prejudice to the Effective Conduct of Public Affairs

11 DATE OF NEXT MEETING: 24 February 2021

N.B: The minutes of the Audit & Risk Assurance Committee are reported directly to the Board of Management, with an accompany commentary from the Committee Chair.

AUDIT & RISK ASSURANCE COMMITTEE
25 NOVEMBER 2020
PAPER N

For the future you want

FOR INFORMATION			
Meeting:	Audit and Risk Assurance Committee 25.11.20		
Presented by	Nick Croft		
Author/Contact	Nick Murton	Department / Unit	Communications, Policy and Research
Date Created	27.10.20	Telephone	0131 297 8663
Appendices Attached	Appendix 1: ICO Data Breach Reporting Thresholds Appendix 2: Intrusions Blocked - January to October 2020		
Disclosable under FOISA		Yes	

ANNUAL REPORT ON CYBER-ATTACKS AND DATA BREACH INCIDENTS

1. PURPOSE

The Audit and Risk Assurance Committee indicated it would welcome an annual report on data breach incidents and cyber-attacks to help members understand the source, frequency and whether any specific trends existed. This report is intended to provide information in line with ARAC's request.

2. BACKGROUND

In the wake of the Wannacry ransomware attacks in May 2017, the Scottish Government published its Public Sector Action Plan on Cyber Resilience, outlining a common, effective, risk-based approach to cyber-security across the public sector. In line with the requirements of the Scottish Government's action plan, Edinburgh College attained Cyber Essentials Plus accreditation in August 2018, assuring that the college has in place five critical controls to reduce vulnerability to the most common internet-based threats (including hacking and phishing).

Separately, under the General Data Protection Regulation (GDPR), Edinburgh College has a legal duty to investigate any security incident which may affect the confidentiality, integrity or availability of **personal data**; evaluate whether a data breach has occurred; and (if of sufficient seriousness) report it to the ICO and the individual(s) affected with 72 hours of discovery. Failure to report a breach when required to do so can result in a fine of up to €10m or 2% of turnover. A significant personal data breach can result in an additional fine of up to €20m or 4% of turnover.

3. DETAIL

The sections below provide an annual overview of cyber-attacks, and data breaches, at Edinburgh College over the past 12 months.

3.1 Cyber-Attacks

<u>Source, frequency and trends</u>

Edinburgh College does not formally record *attempted* cyber-attacks, unless these are extraordinary or significant in some way, due to the volume of attacks on a daily basis.

Attempted cyber-attacks are treated as Business as Usual, as each day the college's firewall (similar to other large public bodies) blocks a high volume of attempted phishing and spoofing emails (the attempt to procure or alter staff personal data through fraud and social engineering); and other unsuccessful external attempts to penetrate the college's firewall (for the purposes of hacking; or transmission of malware, viruses, trojan horses, and ransomware).

The college's Infrastructure and Network team 'patch' identified security vulnerabilities on a rolling basis to minimise risk. The College has in place the following five key security controls, and has received externally-validated Cyber Essentials Plus accreditation accordingly:

- Firewalls
- Secure configuration
- User access control
- Malware protection
- Patch management

An indicative report showing intrusions 'blocked' over the period January 2020 to October 2020 is provided by Appendix 2 of this document.

Cyber incidents

The college has recorded no significant impactful external 'cyber-attack' in session 2019/2020. It is important to remember that the college can only measure the breaches or attacks that have been identified. There are likely to be hidden attacks, and others that go unidentified, so the finding reported here may underestimate the full extent of the problem.

3.2 Personal Data Incidents & Data Breaches

Data Breach Definition

The Information Commissioner's Office (ICO) defines a data breach as: "a security incident that has affected the confidentiality, integrity or availability of personal data.

"In short, there will be a personal data breach whenever any personal data is:

- *lost, destroyed, corrupted or disclosed*;
- if someone *accesses the data or passes it on without proper authorisation*; *or*
- *if the data is made unavailable*, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed".

Under the General Data Protection Regulation (GDPR) Edinburgh College has a legal duty to investigate any security incident which may affect the confidentiality, integrity or availability of personal data; evaluate whether a data breach has occurred; and (if of sufficient seriousness) report it to the ICO and the individual(s) affected within 72 hours of discovery.

Edinburgh College's Data Protection Policy; Data Breach Reporting Procedure; mandatory GDPR training module, and employee induction direct staff to the DataProtection@Edinburghcollege.ac.uk inbox and data incident reporting form, for the purposes of reporting data incidents/suspected data breaches.

Incidents and Breaches

Over the period October 2019 to September 2020 the college's Information Management Team (IMT) was notified of, and investigated, 31 data incidents to evaluate whether personal data breaches had occurred (in line with the breach definition provided by the ICO).

The IMT determined that:

- 28 of these incidents technically comprised a data breach; and
- 3 manifestly did not qualify as a data breach.

The college's Data Breach Reporting Procedure sets out a scoring matrix which the IMT uses to consistently evaluate whether or not a confirmed breach is reportable to a). the Information Commissioner's Office b). the individuals affected ("data subjects").

This breach evaluation matrix has been adopted by a number of colleges across Scotland who are members of the Data Protection Officer Shared Service provided by HEFESTIS.

To date, zero breaches have been determined as reaching the threshold for reporting to the Information Commissioner's Office; each decision is recorded on a case-by-case basis on the college's data incident recording tracker.

It should be noted that in five instances, the affected data subjects were already aware of the breach. In four further instances, the college notified the individuals concerned of the breach to enable them to take steps to minimise any potential harm, prior it to the harm occurring. In this situation, reducing the 'likely harm' brought it below the threshold to report to ICO

Table 1: Recorded data breaches at Edinburgh College (by ICO Classification)

Data Breach (ICO Classification)	EC total June 18 to Sep 2019	Oct 19 to Sep 2020	Change +/-
Data emailed to incorrect recipient	13	12	-1
Failure to use bcc	4	6	+2
Unauthorised access	3	1	-2
Data of wrong data subject shown in client portal	3	2	-1
Other cyber incident	2	0	-2
Data posted or faxed to incorrect recipient	2	0	-2
Alteration of personal data	2	0	-2
Loss/theft of paperwork or data left in insecure location	1	3	+2
Failure to redact	1	4	+3
Verbal disclosure of personal data	1	0	-1
TOTAL:	**32**	**31**	**-1**

Source of breaches & trends

As outlined below, over the period October 2019 to September 2020 the principle source of data breaches at Edinburgh College has been human error. A limited narrative for the main data breaches is provided below.

Human error – incorrect email recipients; failure to use BCC

As outlined in Table 1, 18 (**58%**) of 31 recorded data breaches at Edinburgh College have been the result of personal data being emailed to the incorrect recipient; or the failure to use the "BCC" function appropriately when sending emails.

The above are categorised as '**human error**' data breaches by the ICO. The sending of data to incorrect recipients via email, and the failure to use BCC when necessary (due to human error) accounted for the second and third greatest number of data breaches reported to the ICO in Q1 of 2019-2020.

In 2018 the college initialised warning messages on all outgoing emails (to external email addresses), reminding senders that they their email was being directed outside the organisation. The college's Data Protection 'top 10 tips' business cards circulated to all college staff reminds them to double-check email addresses prior to distribution; and this message is reinforced in the college's mandatory GDPR training and directly with staff who have committed a data breach of this nature.

Failure to redact (4 data breaches)

- Four data breaches resulted from the re-use of existing college documents as 'templates' where existing personal data had not been comprehensively deleted prior to their re-use.

Loss/theft of paperwork or data left in insecure location (3 data breaches)

- One data breach resulted from the theft of an unencrypted college laptop from a member of staff travelling on public transport.

- One data breach was caused by the loss of a physical folder of student data on campus.

Data of wrong data subject shown in client portal (2 data breaches)

- Both data breaches were caused by human error:
    - Assessment feedback was provided to a candidate via Moodle, but also contained another student's original assessment submission; and
    - A student's audio recording/assessment was stored and discovered in another candidate's portfolio by an internal assessor.

4. BENEFITS AND OPPORTUNITIES

Annual reporting of trends in cyber-attacks and personal data breaches will enable the college's Senior Management Team, and Audit and Risk Assurance Committee, to identify areas of significant risk and respond and resource accordingly. Identification of these trends will enable operational teams, including the IT Digital Infrastructure team and Information Management Team to prioritise activities to mitigate risk, including appropriate staff training.

5. STRATEGIC IMPLICATIONS

The monitoring and analysis of cyber-attacks and personal data breaches supports the college's compliance with, the General Data Protection Regulation. A robust approach to cyber and information security provides assurance to the Scottish Government in line with the Public Sector Action Plan on Cyber Resilience. Being seen as a trustworthy organisation, where individuals' personal data are concerned, supports a number of strategic aims: valued in partnership and by

communities (“EC is a trusted partner”); effective and efficient college (“strong corporate controls; high standards of governance; assured Board of Management, staff, students, and stakeholders,

6. RISK

The occurrence of successful, significant cyber-attack, and/or significant data breach - could potentially lead to sanctions (and reputational damage). Ppotential sanctions under the GDPR include:

- A warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater;
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

7. FINANCIAL IMPLICATIONS

Financial resource to improve and increase detection of cyber-attacks has not been available.

8. LEGAL IMPLICATIONS

The college must comply with the General Data Protection Regulation (GDPR).

9. WORKFORCE IMPLICATIONS

The Information Manager, IT Digital Infrastructure Lead (and team), and Data Protection Officer must be available out-of-hours, including weekends, to respond to successful or significant cyber-attacks and/or data breaches.

10. REPUTATIONAL IMPLICATIONS

GDPR compliance, and the prevention of a significant, successful, cyber-attack is essential to maintaining the college’s reputation with legislators, staff, students and partners.

11. EQUALITIES IMPLICATIONS

No specific equalities implications.

CONCLUSIONS/RECOMMENDATIONS

Audit and Risk Assurance Committee are asked to NOTE the update provided.

ICO Definition of ICO/Data Subject reporting thresholds

Threshold for reporting data breach to ICO	Higher threshold for reporting data breach to Data Subject
Likely to result in risk to people's rights and freedoms: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."	**Likely to result in high risk to people's rights and freedoms:** Must inform those concerned directly and without undue delay (as soon as possible) A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher

Intrusions Blocked

Report Date: October 6, 2020
Data Range: 2020-01-01 - 2020-10-06

#	Attack Name	Attack Description	Counts
1	HTTP.URI.SQL.Injection	Indicates an attempt to exploit a SQL-injection vulnerability through HTTP requests	11,319
2	Web.Server.Password.Files.Access	Attempts to access a sensitive file through HTTP requests.	8,186
3	PHP.Diescan	Malicious usage of PHP code	5,717
4	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Attack attempts against a Remote Code Execution vulnerability in PHPUnit, a PHP testing framework	4,887
5	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Attempts against a Remote Code Execution vulnerability in ZeroShell	4,507
6	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Attack attempts to exploit a Remote Code Execution Vulnerability in ThinkPHP, a web application framework	3,916
7	Mirai.Botnet	Indicates Mirai botnet-controlled device attempt blocked on gateway firewall	2,436
8	PHP.CGI.Argument.Injection	Attempts against an argument Injection vulnerability in PHP CGI	2,180
9	Joomla!.Core.Session.Remote.Code.Execution	Attempt to execute a Remote Code Execution vulnerability in Joomla CMS	2,091
10	Novell.NetBasic.Scripting.Server.Directory.Traversal	Attempts to exploit a Directory Traversal vulnerability in Novell NetBasic Scripting Server	1,872

AUDIT & RISK ASSURANCE COMMITTEE
25 NOVEMBER 2020
PAPER O

FOR INFORMATION			
Meeting	Audit & Risk Assurance Committee 25.11.20		
Presented by	Nick Croft		
Author/Contact	Nick Croft	Department / Unit	Communications, Policy & Research
Date Created	28.10.20	Telephone	-
Appendices Attached			
Disclosable under FOISA		Yes.	

EDINBURGH COLLEGE HORIZON SCANNING REPORT – DECEMBER 2020 BOARD OF MANAGEMENT CYCLE – EDITION 10

1. PURPOSE

This report seeks Committee consideration and discussion, about developments identified in the College's tenth edition of the Horizon Scanning Report.

2. MAIN REPORT

Background

As with the previous edition, this report indicates organisational, sector-wide, economic and social impacts arising from the Covid 19 Pandemic, in addition to other strategic developments impacting on college business.

Responses to any impacts on college business are agreed at the Board and its committees, Senior Management and Executive Teams, linked to key college strategies and plans, and referenced in the College's Risk Registers and Operational Plans. Many of these matters are also considered at Board Development Days.

Scottish Funding Council (SFC) – Review of Coherent Provision and Sustainability

The SFC has published the first phase findings and recommendations of the above review, which can be found at: http://www.sfc.ac.uk/review/review.aspx. Ten key themes have been identified during Phase 1 which will shape future review activity: 1: Keeping the interests of current and future students, and equalities, at the heart of everything we do. 2: Supporting the digital revolution for learners. 3: Towards an integrated, connected tertiary education and skills system for learners and employers. 4: Recognising colleges and universities as national assets and civic anchors. 5: Building long-term relationships with employers and industry. 6: Protecting and leveraging the excellence of our research and science base. 7: Driving the innovation agenda. 8: Enhancing collaboration. 9: Making the most of the sector's global connections. 10: Focusing on the financial sustainability of colleges and universities, and current funding models.

UK Government – Economic Forecasts Research 2020

The UK Government has published a comparative analysis of various independent economic forecasts for the remainder of 2020, and 2021. In summary, based on the average of GDP growth forecasts, the UK economy is projected to decrease by 10.1% in 2020, and increase by 6.5% in 2021. The equivalent projections for (i) unemployment rate are 8.3% in 2020 and 6.6% in 2020, and (ii) Retail Price Index 1% 2020 and 2.9% in 2021. https://www.gov.uk/government/statistics/forecasts-for-the-uk-economy-august-2020

Scottish Government

Further to the Programme for Government 2020 https://www.gov.scot/programme-for-government/ announcement in September 2020, relevant new legislation passing through the Parliament includes (i) Domestic Abuse Bill, (ii) incorporating the UNCRC into Scots law, (iii) UK Withdrawal from the EU (continuity) Bill, and (iv) Hate Crime and Public Order Bill.
The Government has also launched a consultation on a new national digital strategy (https://www.gov.scot/publications/renewing-scotlands-full-potential-digital-world/). The OECD led review of Curriculum for Excellence - Senior Phase S4-S6 and the Rapid Review of National Qualifications Experience also continue.

In addition, a new consultation on *Rebuilding a Fairer Scotland after COVID-19* has been launched https://www.gov.scot/news/rebuilding-a-fairer-scotland-after-covid-19/. Colleges Scotland are pulling together a sector wide response.

Scottish Government Covid 19 Guidance

A new plan to help tackle mental health issues arising from the pandemic has also been published (https://www.gov.scot/news/supporting-scotlands-mental-health-recovery/).

The Scottish Government has updated its COVID-19 – Framework for Decision Making: Scotland's route map through and out of the crisis. Guidance on the safe re-opening of colleges, universities and purpose-built student accommodation has also been published.

The SFC's webpage on coronavirus preparedness continues to be updated. The College's 5R Plan Steering Group and five Sub Groups continue to respond to such guidance.

UK Independent Commission on the College of the Future

The Commission produced a new report, prior to the publication of its final report in Autumn 2020, entitled '*People, Productivity and Place: A New Vision for Colleges' https://www.collegecommission.co.uk/vision*. The report indicated that college of the future will be central to driving a fairer, more sustainable and more prosperous society, delivering for people (colleges will be a touchpoint for everyone throughout their lives as the world changes. Flexible and blended learning and guidance will empower each person to get a job, progress in their career and be an active citizen); for productivity (colleges will provide strategic advice and support for employers to drive business change, innovation and future workforce planning); and for place (colleges will have the resources and funding to play an even greater role in fostering healthy and connected communities).

Edinburgh Poverty Commission

The Edinburgh Poverty Commission's final report can now be viewed via this **link**. The report indicates a number of recommendations for public sector institutions, businesses and communities, to address rising poverty rates in the Capital City. A new community of interest

has been established to help progress work: Further details can be found at: https://edinburghpovertycommission.org.uk

New Student Visa Regulations

From 5 October 2020, all prospective international students coming to study in the UK on, or after, 1 January 2021, including those from the EU, EEA and Switzerland (excluding Ireland), will need to apply for a Student Visa, and receive a decision, before they arrive. More information about the Student Visa can be found at: https://www.gov.uk/student-visa

CDN New Strategic Framework

CDN have published a new and ambitious Strategic Framework, setting out the organisation's aims and objectives for the coming three years. Priority objectives for the 2020/21 academic session are: (i) supporting the learning workforce to develop excellent digital skills; (ii) promoting systems leadership development opportunities across the sector; (iii) developing collaborative research and enquiry programmes focused on recovery and practical innovation in education and skills; and (iv) ensuring that tackling the climate emergency and building a sustainable economy is at the heart of the post-Covid strategy.

Logan Review – Scottish Technology Ecosystem

This extensive report into the 'Scottish Tech Sector' can be found at: https://www.gov.scot/publications/scottish-technology-ecosystem-review/. It identifies a series of recommendations to ensure Scotland has a world-class tech sector, by focussing on education and talent, infrastructure and funding. A particular focus is placed on the importance of enabling more 'tech start ups', to 'generate a tipping point' in the pace of ecosystem development.

DDI Creative Industries 'White Paper' Briefing

A 'white paper' on 'Developing Data Driven Innovation in Creative Industries' has been produced by the Data-Driven Innovation Programme at the University of Edinburgh, as part of the Edinburgh and South East Scotland City Region Deal, which will be published on 16 September 2020 at https://ddi.ac.uk/data-driven-vision-for-city-regions-creative-sector.
This research was undertaken in advance of the publication of the Scottish Technology Ecosystem Review.

JISC Report – Shaping the Digital Future of FE and Skills

JISC collaborated with the Association of Colleges and college principals on a research programme: Shaping the Digital Future of FE and Skills, The report that concludes this project is linked here.

The SFC has published the following documents since the last briefing note:

- Flexible Workforce Development Fund 2020-21 - http://www.sfc.ac.uk/sectorcommunications
- Analysis of the 2018-19 Annual Accounts of Scotland's Colleges and Universities - http://www.sfc.ac.uk/sectorcommunications
- Funding for counsellors 2020-21
- Additional AY 2020-21 student number collection (college sector)

3. BENEFITS AND OPPORTUNITIES

This report will enable the Board of Management and its committees to improve awareness of, and better respond to, impacts arising from the Covid 19 Pandemic, and other legislative and policy developments.

4. STRATEGIC IMPLICATIONS

All identified horizon scanning impacts, and local economic recovery actions, are well aligned to the five strategic aims of the Edinburgh College Strategic Plan 2017/22, and transformational themes of a 'Future Proofed College'.

5. RISK

This report will enable the College to better identify the risks arising from the Covid 19 Pandemic, and risks emanating from other national developments. Agreed risks are managed via a specific Covid 19 Risk Register, Departmental Operational Risk Registers, and the College's Top-Level Risk Register.

6. FINANCIAL IMPLICATIONS

Any financial implications for the College identified in this report will be managed by the Senior Management Team, and Executive Team.

7. LEGAL IMPLICATIONS

Any legal implications arising as a result of this report will be managed by the Senior Management Team, and Executive Team.

8. WORKFORCE IMPLICATIONS

Any workforce implications arising as a result of this report will be managed by the Senior Management Team, and Executive Team.

9. REPUTATIONAL IMPLICATIONS

Any reputational implications arising as a result of this report will be managed by the Senior Management Team, and Executive Team.

10. EQUALITIES IMPLICATIONS

Any equalities implications arising as a result of this report will be managed by the Senior Management Team, and Executive Team.

RECOMMENDATIONS

The Committee is recommended to CONSIDER and DISCUSS the implications for the College arising from the Horizon Scanning Report.

AUDIT & RISK ASSURANCE COMMITTEE
25 NOVEMBER 2020
PAPER P

For the future you want

FOR INFORMATION			
Meeting	Audit & Risk Assurance Committee 25.11.20		
Presented by	Chair		
Author/Contact	Marcus Walker	Department / Unit	Governance
Date Created	19.10.20	Telephone	-
Appendices			
Disclosable under FOISA		Yes.	

AUDIT & RISK ASSURANCE COMMITTEE - AGENDA PLANNER 2020/21

1. PURPOSE

To provide Committee members with an opportunity to review upcoming items of business.

2. BACKGROUND

It is important that the Board and its committees follow an appropriate plan of work in order to ensure they effectively cover all areas of their remit throughout the year and make the most efficient use of their time.

3. DETAIL

Below are proposed agenda items (and lead speaker) for the next three meetings of the Audit & Risk Assurance Committee, excluding Minutes of the Previous Meeting, Matters Arising, Any Other Competent Business and For Information papers (e.g. Data Breach Report):

3.1 Wednesday 24 February 2021

- INTERNAL AUDIT
  - Summary of Audit Recommendations (A Williamson)
  - Internal Audit Report: Curriculum Planning (BDO)
  - Internal Audit Report: Project Management / Progress Against the Future Proofed College Programme (BDO)
  - Internal Audit Report: Student Support (BDO)
  - Internal Audit Progress Report (BDO)
- RISK ASSURANCE
  - Risk Management Report (N Croft)
  - Deep Dive: EU Withdrawal (M Jeffrey)
- HORIZON SCANNING REPORT (N Croft)
- AUDIT SCOTLAND STATUTORY FEES 2021/222 (A Williamson)

3.2 Wednesday 26 May 2021

- INTERNAL AUDIT
  - Summary of Audit Recommendations (A Williamson)
  - Internal Audit Report: International Contracts (BDO)
  - Internal Audit Report: Workforce Planning (BDO)
  - Internal Audit Report: Communications (BDO)
  - Internal Audit Report: Progress Report 2020/21 (BDO)
  - Internal Audit Plan 2021/22 (BDO)

- RISK ASSURANCE
  - Risk Management Report (N Croft)
  - Deep Dive: Safeguarding (M Hoenigmann)

- AUDIT SCOTLAND: 2020/21 ANNUAL AUDIT PLAN (Audit Scotland)

- HORIZON SCANNING REPORT (N Croft)

- REVIEW OF COMMITTEE OPERATION 2020/21 (Chair)

3.3 October 2020 (Date to be confirmed)

- REVIEW OF COMMITTEE OPERATION 2020/21 (Chair)

- TERMS OF REFERENCE (Chair)

- AUDIT SCOTLAND: SCOTLAND'S COLLEGE 2021 (Audit Scotland)

- INTERNAL AUDIT
  - Summary of Audit Recommendations (A Williamson)
  - Internal Audit Report: Follow-up Report 2020/21 (BDO)
  - Internal Audit Annual Report 2020/21 (BDO)

- RISK ASSURANCE
  - Risk Assurance Report (N Croft)
  - Annual Report on Data Breach Incident and Cyber Attacks (N Croft)
  - Deep Dive: Commercial Development (M Jeffrey / J Grant)

- EXTERNAL AUDIT
  - Compliance with the Code of Good Governance (N Croft)
  - Internal Control Assurance Statements (A Cumberford)
  - Draft Annual Report and Financial Statement (L Towns)

- ANNUAL COMPLAINTS REPORT (K Heathcote)

- HORIZON SCANNING REPORT (N Croft)

4. BENEFITS AND OPPORTUNITIES

Effective agenda planning will allow the Committee to monitor all aspects of business within its remit in a timely manner.

CONCLUSIONS/RECOMMENDATIONS

The Audit & Risk Assurance Committee are asked to NOTE upcoming items of business, and CONSIDER any additional items for discussion at upcoming meetings.