

Board of Management

Date of Meeting	Wednesday 11 March 2020
Paper No.	BoM5-C
Agenda Item	3.3
Subject of Paper	Strategic Risk Review
FOISA Status	Disclosable
Primary Contact	Paul Clark, College Secretary/Planning
Date of production	4 March 2020
Action	For Approval

1. Recommendations

1. To review and approve the College Risk Register.

2. Purpose of report

2.1 The purpose of this report is to enable a review of the College Risk Register, and provide the Board with an update on significant changes, and an opportunity to discuss and evaluate present risks.

3. Context

3.1 Risk Management is a key component of the College's internal control and governance arrangements, and as such is an important responsibility of the Senior Management Team, Board Committees, and the Board of Management. The risks listed on the Risk Register have been identified by SMT and Board Committees, as the current strategic risks faced by the College. The risks are aligned within the same framework of four strategic themes as the College Strategic Plan, and those included in the Risk Register and Matrix have potential impacts on one or more of the College's strategic priorities.

3.2 A full review of strategic risks is currently underway involving senior Risk "owners", senior managers as appropriate, and Board Committees. All Risk MAPs are being updated accordingly and reported to the respective Board Committees.

3.3 A trend analysis of overall risk scores, illustrated on the Risk Register (the table below the Register itself) indicates a reduction of average risk score from June 2019 (9.43) to December 2019 (8.95) which has not significantly changed since.

3.4 The Risk Register is attached, together with the Risk MAPs for the highest scoring risks, RAG-rated RED. SMT/ELT has discussed the potential impacts of coronavirus Covid-19, and to date has followed the advice from HPS/NHS Scotland. There is significant potential risk to business continuity, and the Board is invited to consider this risk in that context.

- Risk 6 - ■ Negative impact upon College reputation. Reason – Potential outcomes from fraud investigations and associated media coverage (Audit Committee, May 2019).
- Risk 12 - ■ Failure of Business Continuity. Changed from 15 (RED) to 10 (AMBER) at November 2029. Reason – the Internal Audit of BCP was presented to the Audit Committee in November 2019, with an assurance rating of Good.

Consider increasing likelihood score of this risk as a result of potential disruption to ongoing operations related to Covid-19 outbreak.

4. Impact and implications

4.1 The effective management and control of risks is essential to the on-going stability and future growth of the College, with clear implications in terms of potential impact upon College students and staff, as well as the College's wider reputation. All strategic risks have potential strategic impact upon the College. The College Risk Register includes matters relating to legal compliance.

4.2 Several strategic risks are financial in nature, and potentially constitute a threat to the College's stated strategic priority to "Maintain our long-term financial stability".

4.3 Performance management and improving performance are identified as areas of strategic risk, due to the potential impact on reputation, the student experience, and funding.

4.4 Regional and sectoral considerations are included in the process of risk management, and are reflected in the risk documentation.

Appendices:

Appendix 1: Risk Register and selected Risk Management Action Plans

Risk Register: 4 March 2020

RISK DETAIL					CURRENT EVALUATION			AIM and PROGRESS			RISK TREATMENT	
Strategic Theme	Risk Name	Risk ID	Level	Risk Owner	Likelihood	Impact	Net Risk Score	Gross Risk Score	Target Risk Score	Risk Movement/Comments	Link to Risk Mgt Action Plan (MAP)	Date of last review
Students	Failure to support successful student outcomes	1	1	VPSE	2	5	10	25	5		Risk 1 MAP.docx	Mar'20
Students	Failure to establish optimal pedagogical model	2	1	VPSE	1	5	5	20	5		Risk 2 MAP.docx	Mar'20
Students	Failure to achieve good student outcome/progression levels	3	1	VPSE	2	5	10	15	5		Risk 3 MAP.docx	Mar'20
Students	Failure of the College's Duty of Care to Students	21	1	VPSE	1	5	5	20	4		Risk 21 MAP.docx	Sept '19
Growth and Development	Failure to realise planned benefits of Regionalisation	4	1	Pr/DPr	3	3	9	20	3		Risk 4 MAP.docx	Feb '20
Growth and Development	Negative impact upon College reputation	6	1	VPCDI	3	5	15	25	5	Amber to RED AC 05/19	Risk 6 MAP.docx	Jan '20
Growth and Development	Failure to achieve improved business development performance with stakeholders	7	1	VPCDI	2	5	10	25	5		Risk 7 MAP.docx	Jan '20
Growth and Development	Failure to achieve improved performance	8	1	VPSE/DirP	2	5	10	20	5		Risk 8 MAP.docx	Mar'20
Growth and Development	Failure to attract, engage, and retain suitable staff	9	1	VPCS	2	2	4	20	3		Risk 9 MAP.docx	Oct '19
Growth and Development	Failure to achieve taught degree awarding powers	26	1	VPCS	tbc	tbc	#VALUE!	20	3	New Risk (AC 02/20)	Risk 9 MAP.docx	Feb'20
Processes and Performance	Negative impact of statutory compliance failure	10	1	CSP/DCS	2	5	10	20	5	Monitor IA actions AC 5/19	Risk 10 MAP.docx	Feb'20
Processes and Performance	Failure of Compliance with the General Data Protection Regulations (GDPR)	24	1	DPr	3	4	12	25	5		Risk 24 MAP.docx	Jan'20
Processes and Performance	Failure of Corporate Governance	11	1	Pr/CSP	1	5	5	20	5	Monitor IA actions AC 11/19	Risk 11 MAP.docx	Feb'20
Processes and Performance	Failure of Business Continuity	12	1	VPCS/CSP	2	5	10	25	4	Score decr.. 15 to 10: AC 10/19	Risk 12 MAP.docx	Mar'20
Processes and Performance	Failure of IT system security	25	1	VPCS	2	5	10	25	5	Score decr.. 15 to 10: FPRC 10/19	Risk 25 MAP.docx	Feb'20
Processes and Performance	Failure to manage performance	13	1	VPSE/DirP	1	4	4	20	4		Risk 13 MAP.docx	Mar'20
Processes and Performance	Negative impact of Industrial Action	14	1	VPCS	3	4	12	25	4		Risk 14 MAP.docx	Oct '19
Finance	Failure to achieve operating surplus via control of costs and achievement of income targets.	15	1	VPCS	2	3	6	25	4	Score incr. 6 to 9 AC 02/20	Risk 15 MAP.docx	Feb'20
Finance	Failure to maximise income via diversification	16	1	VPCS/VPCDI	4	3	12	20	4		Risk 16 MAP.docx	Feb'20
Finance	Failure to obtain funds from College Foundation	20	1	VPCS	1	4	4	20	4		Risk 20 MAP.docx	Feb'20
Finance	Negative impact of Brexit	22	1	VPCS/DCS	5	2	10	tbc	5		Risk 22 MAP.docx	Feb'20
Finance	Failure to agree a sustainable model and level of grant funding within Glasgow Region	23	1	VPCS	3	4	12	25	5		Risk 23 MAP.docx	Feb'20

Key:
 Pr - Principal
 DPr - Depute Principal
 VPSE - Vice Principal Student Experience
 VPCS - Vice Principal Corporate Services
 VPCDI - Vice Principal Corporate Development/Innovation
 CSP - College Secretary/Planning
 DHR - Director of Human Resources
 DirP - Director of Performance
 DCS - Director of Corporate Support
 AC - Audit Committee

x	Likelihood				
Impact	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5

Note comment

Date	Jun-17	Dec-17	Jun-18	Dec-18	Jun-19	Dec-19	Jun-20	Dec-20
Average Risk Score	10	9.56	9	9	9.43	8.95		

N.B. Closure of low-scoring risks will upwardly impact upon average risk score.

Tolerance vs Risk Score	Acceptable Risk Score		Acceptable Risk Score		Acceptable Risk Score	
	1-3	4-5	6-9	10-12	15-16	20-25
Risk Management Level of Tolerance (Able to Accept)	1	2	3	4	5	6
	Low		Medium		High	

Risk Management Action Plan

Risk Description: Negative impact upon College reputation

Risk ID: 6

Owned by: VPCDI

Review Date: Jan 2020

Update

Full Description:

1. Failure to protect and maintain the brand.
2. Complaint to Scottish Public Services Ombudsman upheld
3. Significant breach of College policies & procedures.
4. Gross misconduct of a member / members of staff.

Treatment: (new text in red)

1. The Associate Director for Brand & Communications has reviewed the operational elements and structure of the team to ensure that is fit for purpose to maintain and enhance the college brand on social media platforms.
2. A new PR/Public Affairs company is being procured to assist with the ongoing promotion and public affairs positioning that the college requires.
3. College Complaints Procedure to be available and communicated to all employees; train staff, including managers in operation of college policies & procedures, including legal requirements.
4. Management monitoring and control supported by the work of the College internal and external auditors.
5. Embedding College values and behaviours supported by robust College policies & procedures.

Commentary (Update):

The College currently enjoys an excellent external reputation based on performance, facilities and the work of the Corporate Development and extended college staff.

1. New Complaints procedure agreed and implemented in line with developments in SPSO framework for FE.
2. The College Complaints Report is now published via the College Website, in line with SPSO requirements.
3. Further staff training now in place to support implementation of SPSO model complaints handling procedure.
4. Through various media monitoring platforms the College continues to monitor its coverage, reputation and positioning within the marketplace on a daily basis
5. Ongoing press/media enquiries relating to a wide range of areas are commonplace, including some relating to College operations at the City Campus. The College is also experiencing a high volume of FOISA requests at present, covering a wide range of areas from staff salaries and performance related

payments, campus events, overseas expenditure, student support, budgets, industrial action information, communications with politicians, etc.

6. Positive press coverage relating to a number of awards and events have continued each month in session 2019/20 with a total of almost 60 awards and accolades for the calendar year 2019.
7. The latest College Annual Report 2017-18, highlighting various College, student, and staff successes, published in February 2019.

At 8 May 2019:

An internal review has revealed some suspected fraudulent activity, reported to the Audit Committee (29/4/19), which is the subject of ongoing further detailed investigation and audit. All relevant parties have been informed, including the Police who are now treating this as a suspected criminal act. It is envisaged that there may be negative reputational impact near the completion of this investigation. The College is working on a PR/Crisis plan to mitigate reputational risk which will include working with the media to ensure that the key facts of this case are presented at the correct time.

At 15 May 2019

The Audit Committee received the Principal's report on the above matter, and agreed the recommendation to increase the risk score to 3x5= RED.

At Sept 2019

The Principal continues to keep the Committee and Board of Management up to date with ongoing investigations, and report due dates, as far as is known and appropriate for dissemination.

January 2020

Risk Treatment (1-2) and Commentary (3-6) updated above.

Current Risk Score:	Gross Risk Score (assuming no treatment)
Likelihood 3/5	Likelihood 5/5
Impact 5/5	Impact 5/5
Risk Score 15/25	Risk Score 25/25
RAG Rating: RED	
(increased from AMBER – Audit Committee 15/5/19).	
Target Score: 5	

Risk Appetite (Willing to accept):	Risk Tolerance (Able to accept):
<u>Low</u> Medium High	Category: Reputation <u>Low</u> Medium High 1 2 3 4 5 6

Impact	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
x	Likelihood				

Risk Management Action Plan

Risk Description: Failure of Business Continuity

Risk ID: 12

Owned by: VPCS/CSP

Review Date: March 2020

Update

Full Description:

1. Severe Fire/Flood
2. Terrorist attack
3. IT Systems Failure (incl Cybercrime) - See Risk MAP 25.
4. Other emergency circumstances resulting in main service failure, and threatening the operation of the College as described in Incident Management Plan (Business Continuity) v4.3.
5. **Impact of Coronavirus Covid-19 outbreak (2020)**

Treatment:

1. Maintain current operational controls.
2. Create and regularly review Incident Management Plan (Business Continuity).
3. Communicate plan to all senior staff.
4. Ensure that local Business Recovery Plans are developed and reviewed.
5. Test and Review at local and College level.

Commentary (Update):

1. Current operational controls are in place with responsibility transferred to GLQ via the NPD contract. Responsibility for communication remains with the College.
2. The BCP emergency incident procedure is currently under review to include recent government guidelines outlined by the CONTEST statutory duty. The BCP has been reviewed with a revised disaster recover plan for all technology systems, and the College has also revised all fire evacuation procedures and identification of incident control rooms at City and Riverside (hard copy BCP located at these locations and at Reception Desks). The BCP has been revised (as at January 2018) in consultation with VP Infrastructure and Head of Facilities Management, with updated contact details of contractors, senior staff etc. and located on Connected (BCP v3.9). The BCP has recently been successfully invoked (7th and 21st November 2017) and found to be effective (see incident report below). SMT has subsequently reviewed and approved the latest version (v3.9) of the BCP.
3. GLQ has an extensive business continuity plan to which the College BCP refers, given that the knowledge of all business critical systems lies with GLQ. These systems are subject to a 25 year maintenance agreement/project agreement. As our operational relationship with the onside contractors continues to develop, we will further refine our BC planning to reflect detailed responsibilities. All heating, cooling, power, air conditioning etc is part of the NPD contract with all risk transferred to GLQ, with commensurate business continuity responsibility. GLQ would therefore be

responsible for repurposing space disrupted by systems failure. The College remains responsible for re scheduling of activity affected by disruption.

4. IT Disaster Recovery Plan (See Risk MAP 25 for updates from October 2017).

Cybercrime: The network infrastructure designed as part of the new build meets the latest filtering and access control technical requirements. In order to test the College's infrastructure, this will be included in the Internal Audit of infrastructure (brought forward to 2016-17 in the light of this priority) This included IT security and was completed as "Satisfactory". It should be noted that this threat is largely related to business disruption, as the college business can be maintained in alternative modes.

In May 2017, following the cyber attacks affecting the Scottish NHS, the Infrastructure section was involved in an IT Network Arrangements/Security audit, and timeous on-going work on our Business Continuity strategy and Disaster Recovery Plans. This was presented to the full Board in June 2017, and included the following detail of the mitigations taken:

- Patching around 9% of our end-user devices which were considered potentially vulnerable. Consideration that a percentage of these are in Staff and Students own hands and not physically present in College.
- Patching many of our critical servers whilst still providing continuous service.
- Proactive monitoring of network services and network traffic.

The general malware attack known as WCry/WarCry, is not the only malware/security threat that the College is attending to at this time. Furthermore, Industry researchers are anticipating the techniques discovered and hoarded by the NSA, of which Wcry was one, will be used with malicious intent in the near future. The College remains diligent to potential threats.

Incident Reports

1. On November 7th 2017 incident - loss of water supply at City Campus - involving the invocation of the Business Continuity Plan by VP Infrastructure in agreement with VP Student Experience. The incident was due to a failure of a water valve restricting water supply. The Emergency Response Team met immediately upon the incident being reported, and followed the appropriate BCP checklists and processes including Team Leader Emergency Response and Loss of Water checklists. The Emergency Response Team undertook an assessment of the incident level (Level 2, BCP P16), and management of the incident. The incident was assessed as critical to ongoing business at City Campus, and the Emergency Response Team decided to curtail the majority of College activity for the day, while maintaining a reduced staff complement.

2. On Tuesday 21 November 2017, a suspicious unattended package was identified on College premises at City Campus at 19.45hrs. The Duty Manager called the emergency services, and a special disposal unit was consequently in attendance to control the incident. Some evening classes were in progress at that time, and staff and students were safely evacuated from the building. The item was found to be harmless, and was identified as a custom-built device left by an employee of FES during a routine window battery installation.

The incident was followed up with FES by the VP Infrastructure and the Principal to ensure that no similar incidents happen in future.

3. On Wednesday 22 November, there was a temporary loss of electrical supply at Riverside Campus, due to an external power outage. There were no injuries, and no requirement for the emergency services. As a consequence, the operation of lifts management was reviewed, and FES staff training for release of lifts was implemented.

These incidents were reviewed and recorded on the appropriate BCP Incident Report form, including lessons learned and improvement actions implemented.

Strategic Review of Business Continuity Management: 2018 Report

This review was undertaken by Ashton Resilience in March 2018, for the College insurers UMAL, by arrangement with the Infrastructure team. The review looked at the activities and operations of the College, its current recovery capability and the degree to which BCM has been implemented. A draft report was forwarded to the College on 16 April 2018, with detailed findings and recommendations.

In summary the report found that the College had a “well-developed operational response to incidents, however there was a need for all departments “to develop, implement and maintain a functional recovery process”. This will involve firstly conducting a business impact analysis then documentation of business recovery plans for each area, based upon coherent recovery strategies.

The report stated that:

“ The high priority recommendations in this report are that the City of Glasgow College should:

- Conduct a business impact analysis and service impact analysis for key processes right across the College.
- Identify recovery time objectives for critical business activities and IT services.
- Identify recovery resources, dependencies and strategies for operational recovery.
- Complete the creation of new departmental business continuity / recovery plans to cover all critical areas of the College, using the business impact analysis data as the base.”

An implementation plan to address the report recommendations is under development for approval by ELT/SMT (August 2018);

It is proposed that this risk score remains RED until the key recommendations are enacted. (August 2018).

November 2018

The responsibility for infrastructure (and associated impact analyses/recovery resource assessment) has now passed to the VP Corporate Services.

Head of Facilities Management has undertaken sample business recovery plan, including data sheets, floorplans, and timetables for RoomC.10.005 to inform roll out across all campus locations.

The Audit Committee of November 2018 noted that ELT had agreed to provide additional resource to progress a College-wide business impact analysis to enable business recovery planning. This initiative was supported by the Committee.

January 2019

Business Continuity specialist Ashton Resilience has been engaged to conduct a full cross-college Business Impact Analysis, to inform the development of detailed Business Recovery Planning across all college teaching and support functions. Initial meeting scheduled for 7th February 2019.

February 2019

Ashton Resilience to undertake Business Impact Analyses for each faculty and service area, followed by development of Business Recovery Plans (BRPs) for each. To begin with Faculty of Hospitality and Leisure and HR. Once BRPs are in place, a scenario-based exercise will be conducted for each campus, to include medium and long-term planning and recovery. To be completed by end June 2019.

April 2019

Business Impact Analysis meetings currently underway throughout the College, between managers from all faculties and service areas with Ashton Resilience.

September/October 2019

This risk has been scored RED due to lack of Business Recovery Plans across the College. Ashton Resilience has been engaged to undertake Business Impact Analyses for each faculty and service area, followed by development of Business Recovery Plans (BRPs) for each. This work is now complete, and has been the subject of an Internal Audit of Business Continuity (report due to Committee in November 2019). A new BCP Policy has been drafted, and endorsed by SMT for approval by the Finance and PR Committee. Update: BCP Policy approved by FPRC 2 October 2019.

November 2019

The Internal Audit Report of Nov 2019, indicates a level of assurance of Good, with one level 3 recommendation. In the context of this report, the Audit Committee re-assessed the score for this risk as $2 \times 5 = 10$ AMBER.

February 2020

The above internal Audit identified one Low Level Priority 3 recommendation to ensure that a planned scenario testing exercise is undertaken to compare all BRPs. This will further ensure that each individual plan is achievable based on documented interdependencies. This action to be completed by April 2020. A proposal to undertake this exercise with an external specialist consultant will be considered by the Finance and Physical Resources Committee (February 2020).

February/March 2020

SMT is monitoring closely government and NHS advice with regard to the Coronavirus Covid-19 outbreak, including restrictions to international travel to affected areas. An all staff email has been circulated (26 Feb.) including guidance on infection prevention and control, and key infection prevention and control messages. Specifically staff have been advised of the symptoms of Covid-19, and reminded of the NHS advice to self-isolate and contact NHS24 for medical advice where such symptoms are shown.

Consider increasing likelihood as a result of potential disruption to ongoing operations.

Current Risk Score:	Gross Risk Score (assuming no treatment)
Likelihood 2/5 Impact 5/5 Risk Score 10/25 RAG Rating: AMBER Reduced from 15 (RED) following Internal Audit Report, November 2019. Target Score: 5	Likelihood 5/5 Impact 5/5 Risk Score 25/25
Risk Appetite (Willing to accept):	Risk Tolerance (Able to accept):
<u>Low</u> Medium High	Category: Business Continuity <u>Low</u> Medium High 1 2 3 4 5 6

Impact	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
x	Likelihood				