City of Glasgow College

Board of Management

Date of Meeting	**Wednesday 4 December 2019**
Paper No.	**BoM3-C**
Agenda Item	**3.3**
Subject of Paper	**Strategic Risk Review**
FOISA Status	**Disclosable**
Primary Contact	**Paul Clark, College Secretary/Planning**
Date of production	**25 November 2019**
Action	**For Approval**

1. Recommendations

1. To review and approve the College Risk Register and supporting documentation.

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 the most recent review of strategic organisational risks, to November 2019. In particular, attention is drawn to highest scoring risks (High Likelihood, High Impact) and other significant changes to the Risk Register.

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 was conducted in the quarter to November 2019, involving senior Risk "owners", senior managers as appropriate, and Board Committees. All Risk MAPs were updated accordingly and reported to the respective Board Committees.

3.3 The Risk Register is attached, together with the Risk MAPs for the highest scoring risks, RAG-rated RED, and Risks with recent significant change to score. These are:

- 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). Reason – the Internal Audit of BCP was presented to the Audit Committee in November 2019, with an assurance rating of Good.
- Risk 25 – ■ Failure of IT system security. Changed from 15 (RED) to 10 (AMBER). Context: significant risk treatment (compliance with UK Government Cyber Essentials Plus) was not achieved to schedule (Oct '18). Now complete. FPRC agreed change of risk status at 2 October 2019.

3.4. The trend analysis of overall risk scores, illustrated on the Risk Register (table below Regiater) indicates a reduction of average risk score from June 2019 of 9.43 to 8.95.

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

Appendix 2: Risk Management Action Plans (MAPs) for high-scoring Risks and significant changes.

CITY OF GLASGOW COLLEGE

Risk Register: 21 November 2019

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
RISK DETAIL					**CURRENT EVALUATION**			**AIM and PROGRESS**			**RISK TREATMENT**	
Students	Failure to support successful student outcomes	1	1	VPSE	2	5	10	25	5		Risk 1 MAP.docx	Oct '19
Students	Failure to establish optimal pedagogical model	2	1	VPSE	1	5	5	20	5		Risk 2 MAP.docx	Sept '19
Students	Failure to achieve good student outcome/progression levels	3	1	VPSE	2	5	10	15	5		Risk 3 MAP.docx	Sept '19
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	Sept '19
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	Oct '19
Growth and Development	Failure to achieve improved business development performance with stakeholders	7	1	VPCDI	2	5	10	25	5		Risk 7 MAP.docx	Oct '19
Growth and Development	Failure to achieve improved performance	8	1	VPSE/DirP	2	5	10	20	5		Risk 8 MAP.docx	Sept '19
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
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	Nov '19
Processes and Performance	Failure of Compliance with the General Data Protection Regulations (GDPR)	24	1	DCS/CSP	3	4	12	25	5	Score incr. 12 from 8 AC 05/19	Risk 24 MAP.docx	Sept '19
Processes and Performance	Failure of Corporate Governance	11	1	Pr/CSP	1	5	5	20	5	Monitor IA actions AC 5/19	Risk 11 MAP.docx	Oct '19
Processes and Performance	Failure of Business Continuity	12	1	VPCS/ CSP	2	5	10	25	4	Score decr. 15 to 10: AC 11/19	Risk 12 MAP.docx	Nov '19
Processes and Performance	Failure of IT system security	25	1	VPCS	2	5	10	25	5	Score decr. 15 to 10: FPRC 02/19	Risk 25 MAP.docx	Oct '19
Processes and Performance	Failure to manage performance	13	1	VPSE/DirP	1	4	4	20	4		Risk 13 MAP.docx	Sept '19
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	3	3	9	25	4		Risk 15 MAP.docx	Sept '19
Finance	Failure to maximise income via diversification	16	1	VPCS/ VPCDI	4	3	12	20	4		Risk 16 MAP.docx	Oct '19
Finance	Failure to obtain funds from College Foundation	20	1	VPCS	1	4	4	20	4		Risk 20 MAP.docx	Sept '19
Finance	Negative impact of Brexit	22	1	VPCS/ DCS	5	2	10	tbc	5		Risk 22 MAP.docx	Sept '19
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	Sept '19

Note comment

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
DirP - Director of Performance
AC - Audit Committee

Risk Score Matrix

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

Trend

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	

1

Risk Management Action Plan

Risk Description: **Negative impact upon College reputation**

Risk ID: 6

Owned by: VPCDI   **Review Date: Oct 2019**

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:
1. An Associate Director for Brand & Communications has been appointed and is currently reviewing the operational elements and structure of the team to ensure that is fit for purpose to maintain and enhance the college brand.
2. College Complaints Procedure to be available and communicated to all employees; train staff, including managers in operation of college policies & procedures, including legal requirements.
3. Management monitoring and control supported by the work of the College internal and external auditors.
4. 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 team.
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 the Meltwater News platform the College continues to monitor its coverage, reputation and positioning within the marketplace on a daily basis
5. Ongoing press 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 2018/19, however this may be negatively impacted upon in the context of EIS Strike activity
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.

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

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

Impact					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	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: November 2019**

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 Business Continuity Plan v3.9.

Treatment:
1. Maintain current operational controls.
2. Create and regularly review Business Continuity Plan (BCP).
3. Communicate plan to all senior staff.
4. Ensure that local 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.

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

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 knows 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 2x5 = 10 AMBER.

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** Change from 4x5=20 approved by Audit/BoM March 2018	Likelihood 5/5 Impact 5/5 Risk Score 25/25

Risk Appetite (Willing to accept):	Risk Tolerance (Able to accept):
Low Medium High	Category: Business Continuity **Low** Medium High **1** 2 3 4 5 6

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				

Impact

Risk Management Action Plan

Risk Description: Failure of IT System Security

Risk ID: 25

Owned by: VPCS   **Review Date: Oct 2019**

Update

Full Description:
1. Cybercrime
2. Other emergency circumstances resulting in main service failure, and threatening the operation of the college as described in Business Continuity Plan.

Treatment:
1. Maintain current operational controls.
2. Review Business Continuity Plan (BCP).
3. Ensure that IT Disaster Recovery plans are developed and reviewed.
4. Test and Review at local and College level.
5. Complying with GDPR.
6. Adoption and compliance with UK Government Cyber Essentials Plus recommendations.
7. Enhance security cyber defence and response capability within college IT services.

Commentary (Update):

Cybercrime:
The college network infrastructure remains effective in utilising defensive and detection measures to mitigate the risk of cyber attacks. However, the persistent and constantly evolving threat of criminal and malicious activity, along with emerging vulnerabilities, new technologies and the rise of nation state actors in this arena, require an ongoing programme to maintain a diligent defence to potential threats.

- Antivirus software to counter malware / ransom ware
- Centralised management and configuration of devices
- Active network monitoring tools
- Web and email filters to quarantine suspicious material
- Intruder prevention / detection measures to counter active hackers
- Port filtering and automated defence measures against network attacks (e.g. Distributed Denial of Service)
- Protection against data & web vectors (e.g. SQL injection)
- Awareness raising programmes, policy and guides to counter social engineering / Phishing
- Role based permissions and segregation of access to minimise risk of

accidental damage and internal attacks
- Encryption to defend against data loss / theft.

To reduce the likelihood of a failure the college has taken the following additional measures:
- The College has renewed subscriptions for two of the leading antivirus providers (Bitdefender and Sophos). This means that the College benefits from a multi-vendor approach to security across campus.
- The College physical IT estate (classroom and staff PCs) has been refreshed with the latest version with an improved management platform for Sophos to enable quicker alerting to incidents.
- The College VDI platform has been updated to use Bitdefender due to better "on demand" scanning for VDI.
- The College is configuring servers to scan central file storage using both versions of AV to ensure that any zero day exploit risk is minimised.
- The College continues to monitor and apply security patches to desktop machines, network devices and server infrastructure.
- The College has a clear plan for ensuring GDPR compliance including a review of data and systems with associated recommendations for improvements. (There is a standalone risk plan for Data Protection – Risk MAP 24).
- The IT have reviewed and updated the IT Disaster Recovery plan in line with the new College template and preventative measures are in place.
- The College is reviewing and updating our Information Security policy to reflect changing requirements.
- The College will achieve and maintain UK Government Cyber Essentials Plus accreditation to demonstrate high standards of security governance.
- A new state-of-the-art network Firewall has been installed and configured
- A number of vulnerable older applications and devices have been removed from the College's IT estate

The following measures are also proposed to enhance the depth and scope of our cyber resilience capability:

- The College will seek to identify IT security competencies within existing staff and consolidate to share best practice. We will also seek to formally identify specialist IT security responsibilities to be assigned to specific posts as part of the current Leadership restructure.
- The College will develop and extend our Cyber Essentials programme towards the adoption of ISO 27001 IT Security standards (existing strategic target to evaluate options by 2020).
- Improvements to incident response / reporting through Operations Desk to reduce the impact of potential breaches.
- Alignment of the college capital investment programme with security infrastructure lifecycles to maintain a viable cyber resilience environment.
- The College will evaluate measures for the effective management and remote support of external assets such as mobile devices and laptops to improve

standardisation of security measures and reduce risk from theft or loss.

September 2019 Update

The IT Team have focussed our resources in completing the remedial work across the entire IT estate to position us to pursue the Cyber Essentials Plus accreditation audit which is 90% complete at the time of writing and anticipated that we will be compliant imminently. To date during our Cyber Essentials Plus audit, the College network has passed the following tests: an external network scan showing no current vulnerabilities, anti-malware scan which was passed successfully, an email malware scan that was passed successfully and a web-based (internet accessed) malware scan that was also passed successfully.

A new state-of-the-art network Firewall has been installed and configured to further improve the College's cyber defence. Further external network penetration tests are planned during the academic year and internal network scanning software will be evaluated with a view to procurement which further improves resilience against "insider threat" alerting the Team to "unusual" patterns of network activity which requires further investigation.

In partnership with our Organisational Development colleagues, the IT Team will be supporting the imminent rollout of an email "phishing" simulation programme over the next 12 months to both test and educate our end users. The objective of this project is to test the likelihood of our end users to pass on their personal data to a "phishing"/fake email supplied by our Technology partner to measure our current exposure/risk. Every user, whether they click the fake email link or not, will be taken to a short 2 minute "gamification" training video highlighting the dangers of email "phishing", offering advice on how to spot these fake emails and what to do if you click the link. By running this project over a 12 month period we hope to educate our end users and see the number of "clicks" drop significantly from our initial simulation test and identify any staff areas who perhaps require further awareness training/support.

October 2019
Reported to Finance and Physical Resources Committee – 2 October: Cyberessentials+ accreditation achieved. IT Operational Plan in place. FPRC agreed revision of risk score to 2x5=10.

Current Risk Score:	Gross Risk Score (assuming no treatment)
Likelihood 2/5	Likelihood 5/5
Impact 5/5	Impact 5/5
Risk Score 10 /25	Risk Score 25/25
RAG Rating: AMBER	
(Changed by FPRC from RED at October 2019)	

Target Score: 5	
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

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