RISK MANAGEMENT PLAN

Rationale:

This document is Group Colleges Australia's (GCA) Risk Management Plan (*including UBSS*) that identifies and assesses risks considered likely and relevant to GCA as a private education provider (iHEP), and further identifies risk treatment and mitigation strategies. The GCA Board is the custodian of risk management for GCA, with operational monitoring, stakeholder consultation and communication delegated to the Chief Executive Officer (CEO) and Senior Managerial staff. *An Executive Director on the GCA Board, Emeritus Professor Greg Whateley (Executive Dean, UBSS) is the designated Director responsible for the oversight and reporting of risk (including WHS).*

Definition of Risk Management:

A risk is defined by the Australia/New Zealand Standard for Risk Management (AS/NZS ISO 31000:2009) (1) as "the effect of uncertainty on objectives"; and further defines 'effect' as a deviation from the expected: positive and/or negative; "objectives" can have different aspects (such as the financial, health & safety and environment goals) and can apply at different levels (strategic, organisation wide, project, product and processes). Risk is often characterised with reference to *potential* events and *consequences* or a combination of these. Risk is often expressed in terms of a *combination of the consequences of an event and the associated likelihood of occurrences.* The AS/NZS ISO 31000:2009 has been used as a guide to develop this Risk Management Plan.

Risk Identification Process:

The GCA Risk Plan was developed by way of scoping the external and internal environment and identifying risks that are particular and considered relevant to the Australian Education environment and GCA, in particular, as a private provider (iHEP). The identified risks were then assessed in terms of the *likelihood of occurring* (RL) and their *impact factor* (RI). Mitigation strategies have been developed for each risk to treat or minimise them should they occur. This risk identification and treatment process is based on the Australian/New Zealand AS/NZS 4360:2004 - Risk Management (the Standard); the process flow is outlined in this document.

Risk Monitoring:

The Risks outlined in this Plan are current and are reviewed regularly. The formalisation of the plan was refreshed on September 15, 2017 and changes made are presented to the GCA Board via the sub-committee – the Audit and Risk Committee – at each meeting of the GCA Board. The operational risk managers indicated in the Risk Plan will monitor risks across their areas of responsibility. All meetings of GCA committees receive an update on risk management - *currently championed by the Executive Dean, UBSS*. Further, on the insistence of TEQSA (though not mandated by the Threshold Standards) a *Risk and Audit Committee* (a subj committee of the GCA Board) has been established and is chaired by Emeritus Professor Greg Whateley the Executive Dean (UBSS) and the Executive Director of the GCA Board *designated as the Director responsible for the oversight and reporting of risk (including WHS).*

Stakeholder Consultation and Communication:

The GCA Board is the *custodian* of risk management for GCA. The Executive Director and Executive Dean, UBSS is the designated Director *responsible for the oversight and reporting* of risk (including WHS). Stakeholder communication and consultation is the responsibility of the Chief Executive Officer (CEO) and/or members of the GCA Executive Committee, as delegated by the GCA Board, as detailed for each identified risk in the GCA Risk Plan.

Risk Delegation

Contents	Responsible
Regulatory Compliance	Emeritus Professor Greg Whateley (GW) Executive Dean, UBSS
External Market	Sir Gerard Newcombe (GN) GCA Marketing and Human Resources Director, Carlos Munoz (CM) Business Development and Admissions Director
Academic Matters	Emeritus Professor Greg Whateley (GW), Andrew West (AW) and Ashok Chanda (AC)
Staffing	Emeritus Professor Greg Whateley (GW) and Sir Gerard Newcombe (GN)
Finance and Sustainability	Paul Hauenschild (PH) Chief Financial Officer
Technical	Jason Whitfield (JW) Technical Services and Training Manager and Chair, WHS Committee
Physical Resources and WHS	Assistant Professor Jotsana Roopram (JR) , UBSS Sydney CBD Campus Provost and Jason Whitfield (JW) Technical Services and Training Manager and Chair, WHS Committee

Alan Manly (AM) as CEO has a watching Brief

Emeritus Professor Greg Whateley (GW) is the *designated Director responsible for the oversight and reporting of risk (including WHS) to GCA Board*

GCA Board Membership Endorsement

Alan Manly	Chair and CEO
Sir Greg Whitby	Independent Member
Paul Nicolaou	Independent Member
Emeritus Professor Greg Whateley	Executive Member
Alan Finch	Independent Member

Risk Register Endorsement History (2014 – current)

- Approved by GCA Board (28/02/14)
- Status Update (04/04/14)
- Reviewed and Updated (02/05/14)
- Reviewed and Updated (15/10/15)
- Reviewed and Updated (30/05/16)
- Reviewed and Updated 15/02/2017)
- Reviewed and Updated (15/09/2017)
- Reviewed and Updated (23/11/2017)
- Reviewed and Updated (14/03/2018)
- Reviewed and Updated (06/06/2018)
- Reviewed and Updated (05/09/2018)
- Reviewed and Updated (13/03/2019)

- Reviewed and Updated (05/06/2019)
- Reviewed and Updated (14/08/2019)
- Reviewed and Updated (30/10/2019)
- Reviewed and Updated (05/02/2020)
- **Reviewed and Updated (03/06/2020)**

External Environment Contributing to Risk: SWOT Analysis				
Customers	**Stakeholders**	**Competitors**	**Suppliers**	**Government and Society**
International Students Australian and International students Agents - local (Sydney-based) Agents – international Prospective employers	DET TEQSA DIBP Employer Sponsors (internships) CPA Australia IPA Australia ACPET COPHE General Community Banks: CBA and ANZ Auditor: Pitcher Partners	NUHEPs Public Higher Education Providers and particularly Sydney satellite campuses TAFE Australian offshore institutions Large consortiums of online education (Think, Open Universities, Open Colleges, Study Group)	Agents - local (Sydney-based) Agents –International GCA advertising: internet, billboards, print media Community and family referral MyQual International GCA Admissions Centre CampusQ	DIBP policies: student visas, migration, etc. SVP and impact on PEPS TEQSA: Threshold Standards Education Services for Overseas Students Act (ESOS) 2000 Higher Education Support Act 2003 (HESA) Tertiary Education Quality Standards Agency Act (2011) Tuition Assurance: Tuition Protection Scheme (TPS) National Code of Practice Training Industrial awards Commonwealth and State legislation including – Privacy, WHS, Access and Equity, Workplace Harassment, Victimisation and Bullying Australian dollar exchange rate

Internal environment Contributing to Risk: SWOT Analysis				
SWOT	**People**	**Processes**	**Technology**	**Govt, Society & Environment**
Strengths	Quality of expertise and experience on GCA Board Quality of expertise and experience on GCA Executive Committee Skilled & experienced academics to develop/deliver courses Commitment to staff professional development and scholarship Skilled marketing expertise and agent liaison A developing academic quality assurance culture	Continuous improvement and quality control in academic & operational matters evidenced via sound governance processes Archiving capability in Information management system Flexible content management system MOODLE Developed systems integration of MyGCA Ongoing automation of administrative processes Strong branding internationally Key contacts and processes in place to access government bodies	Quality eResourcing Technology infrastructure in place Commitment to use of Moodle for teaching & learning activities Capacity to design for purpose (Moodle, MyGCA) Computer: student ratio is very high per GCA: University Benchmark Web technology utilisation Consistent technology resource levels throughout classrooms MyGCA system: 24/7 student admin access Revitalised efficient student payment method Robust student management system Industry leader in technological utilisation teaching environment	Established in education industry for 30 years (GCA as proprietor) CBD location Modern, spacious facilities and classroom size

Internal environment contributing to Risk: SWOT Analysis				
SWOT	**People**	**Processes**	**Technology**	**Govt, Society & Environment**
Weaknesses	Manipulation by agents over student choice of provider and agent commissions	Ongoing costs	Ever-changing scenario and challenging of remaining current	Uncertainty of government policies Cost of Australia as an international education destination Challenges of monitoring the uncertainty of government change
SWOT	**People**	**Processes**	**Technology**	**Govt, Society & Environment**
Opportunities	Increase domestic student enrolments through UBSS Diversity current offerings Develop blended subjects for UBSS - initially at PG level Further develop MyQual for gathering marketing intelligence to enhance GCA's competitiveness	Develop Alumni for gathering educational outcomes data (ie Employment, diversity of offerings) Implement of Quality Management framework by undertaking benchmarking in academic and non-academic areas Consider FEE HELP	Further utilise Moodle to increase flexible delivery of existing courses Ability to enhance capability of MyGCA through ongoing user review and input.	Ability to obtain SVP assessment and Access to Chinese JSJ Relocation to CBD Measure employability skills / value of graduates (Internship surveys and employers (alumni)

Internal environment contributing to Risk: SWOT Analysis				
SWOT	**People**	**Processes**	**Technology**	**Govt, Society & Environment**
Threats	Changes in government migration/student visa policies Source country demographics changing - visa rules	Future of current campus location lease 5 year option Changes to TEQSA, and ESOS regulations governing course delivery and compliance Readiness for Random Audits: TEQSA, CRICOS Excessive time consuming compliance requirements (TEQSA, ESOS) threatening business operations	Obsolescence of eLearning resources External reporting requirement PARADIGM/PRISMS/HEIMS and data integrity	High number of local competitors - public and private Private providers with SVP approval Competition from established and large online education consortiums (Think, Open Unis, Open Colleges, Study Group) Universities /TAFE preferred over private education providers Perception that non uni HE courses are relatively new concept and & therefore perceived as less desirable/of poor quality Qualifications from private providers perceived to hold less status/ unknown by employers Cost of Australia as an international education destination

GCA Definition of Risk

After considering the definition of risk in the Australian/New Zealand Standard on Risk Management (AS/NZS ISO 31000:2009) the following definition of risk was adopted for the purpose of theme selection:

> ***Risk*** *refers to a feature of an organisation or its environment that may have an adverse effect on the organisation, including on the achievement of objectives. The term 'feature' includes actions, events or situations.* ***Risk*** *is also a measure of the possible adverse effects on an organisation of any action, omission, event or situation. This is sometimes referred to as the* ***degree of risk*** *inherent in a particular situation. It is expressed in terms of the* ***chance*** *(=likelihood, probability) of the effects occurring; and the* ***consequences*** *of the effects should they occur.* ***Academic risk*** *relates to the achievement of* ***academic*** *objectives.*

1. Likelihood of an event occurring

	Likelihood level
C	Almost certain
L	Likely
P	Possible
U	Unlikely
R	Rare

2. Consequence of event occurring

	Extent of consequence	**Financial**
5	Extreme	Insolvency or liquidation of business
4	Major	Annual NET profit after tax ($5m)
3	Moderate	$1m
2	Minor	$50k
1	Insignificant	$10k

3. Risk Impact Rating

Risk is rated by a combination of consequence and likelihood. For example the consequence of a particular event may be considered catastrophic but the assessment as to the likelihood of it happening may be rare. This approach would assess the particular event as a medium risk. This approach is set out in the following table. *Colour coding is used throughout the document for ease of identification of Likelihood and/or Impact*

Risk Level	Description
Very High	Requires ongoing executive level oversight. The level of risk warrants that mitigation measures be analysed in order to bring about a reduction in exposure.
High	Action plans and resources required. The level of risk is likely to endanger capability and should be reduced through mitigation strategies where possible.
Medium	This level of risk should not automatically be accepted for risk mitigation but rather a cost-benefit analysis is required to determine if treatment is necessary.
Low	Treatment when resources are available. The risk should be able to be managed via existing controls and normal operating procedures.

Risk Rating (Likelihood and Consequence) Matrix

Likelihood						
	C (Almost Certain)	Medium	High	High	Very High	Very High
	L (Likely)	Low	Medium	High	High	Very High
	P (Possible)	Low	Medium	Medium	High	High
	U (Unlikely)	Low	Low	Medium	Medium	High
	R (Rare)	Low	Low	Low	Medium	Medium
		1 (Insignificant)	**2 (Minor)**	**3 (Moderate)**	**4 (Major)**	**5 (Extreme)**
		Consequence				

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
1.0 Regulatory Compliance								
1.1 ESOS Act	Inability to implement and evidence Standards	Potential loss of CRICOS registration to deliver to international students	Rare	Extreme	Medium	Ongoing monitoring by the Office of the Executive Dean, UBSS measuring against audit and Threshold Standards	GW	Audit completed each trimester
1.2 ESOS Act	Inability to promptly respond to an external audit	Potential loss of CRICOS registration to deliver to international students	Unlikely	Major	Medium	Ongoing monitoring by the Office of the Executive Dean, UBSS	GW	Audit completed each trimester
1.3 HESA & Guidelines	Inability to implement and evidence Guidelines	Potential sanctions or deregistration by TEQSA	Unlikely	Major	Medium	Ongoing monitoring by the Office of the Executive Dean and measuring against the Threshold Standards	GW	Audit completed each trimester
1.4 TEQSA Threshold Standards	Failure to meet and evidence Threshold Standards for re-Registration for HE and ELICOS courses	Potential deregistration to offer Higher education courses	Possible	Moderate	Medium	Each trimester an audit committee consider compliance against the *New* Threshold Standards	GW	Ongoing – each Trimester an audit against the new TS is undertaken
1.5 Workplace Health & Safety (WHS) Act 2011	Failure to maintain WHS standards for students and staff	Potential legal action/medical costs; closure of premises	Unlikely	Moderate	Medium	Ensure WHS Committee and processes are maintained	JW	Quarterly formal WHS Audits conducted
1.6 Records Management	Failure to maintain staff and student related materials for required timeframes	Inability to meet audit requirements; produce	Unlikely	Moderate	Medium	Records are maintained via MyGCA or Moodle per GCA Records Management Policy based on the NSW State Records	GW	Ongoing

		records/evidence for regulatory bodies, etc.				Act . All documentation is maintained in the M Drive.		
1.7 CPA & IPA Accreditation Standards	Failure to meet /maintain accreditation standards stipulated by professional bodies	Potential loss of professional accreditation, equalling loss of parity with other providers in the market	Possible	High	Medium	Program Director - Bachelor of Accounting to ensure compliance and maintain relationship with CPA and IPA (as well as CA)	GW	Ongoing
1.8 HEIMS (High Education Information Management System) deadlines not met.	Non-compliance with Federal Government Higher Education Fee help licence	Potential sanctions or loss of FEE HELP licence from Department of Education	Unlikely	Major	Medium	Process maintained by CIO and JW - supported by the Office of the Executive Dean, UBSS	GW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
2.0 External Market								
2.1	Failure of NUHEPs to be included with universities for low risk rating within the Simplified Student Visa Framework (SSVF)	Significant loss of market share to low rated SSVF approved providers	Almost certain	Insignificant	Low	GCA (including UBSS) is maintaining focus via HEPP_QN and iHEA membership Careful management of the offshore market	GN and CM	Upgraded on March 14 2018
2.2	Reliance on international students as primary source of enrolment and revenue	High risk revenue source that is reliant on government policy and affordability of Australia as a study destination	Rare	Extreme	Medium	FEE HELP has been established for Domestic HE with the intention of diversifying the student pool	GN and CM	Ongoing
2.3	Manipulation by agents over student's choice of provider	Decline in international student numbers to competitors offering better commissions or more streamlined admin	Rare	Major	Medium	High level of attention on communication with and visitation to agents	GN and CM	Ongoing
2.4	Competition from private HEPs located in Sydney offering comparable courses	Greater choice for prospective students and decline in GCA enrolments	Unlikely	Moderate	Medium	Maintain high awareness and remain competitive in offerings and pricing	GN and CM	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
2.5	Facilitation of admission of students by agents	Misinformation provided to students; potential breaches to admissions criteria	Rare	Extreme	Medium	Admissions Policies specify delegations to Agents. GCA Admissions Centre to conduct document verification for academic and ELP credentials	GN and CM	Ongoing
2.6	Competition from public universities and satellite campuses located in Sydney with comparable HE courses	Greater choice for prospective students and decline in UBSS numbers. Impact of uncapped University enrolments	Rare	Major	Medium	Maintain high awareness and remain competitive in offerings and pricing,	GN and CM	Ongoing
2.7	Competition from online education consortia (Think; Open Unis Australia; Open Colleges, Study Group)	Greater choice for prospective students and decline in GCA enrolments	Possible	Moderate	Medium	GCA (including UBSS) to maintain interest and vigilance in alternative delivery (ie blended mode).	GN and CM	Ongoing
2.8	Desirability of Castlereagh St (Sydney) as a study location	Reputation of location may affect choice of study	Rare	Insignificant	Low	Relocation to Sydney CBD	GN and CM	Downgraded on November 23, 2017

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
2.9	Loss of key staff members	The loss of key staff members with company knowledge	Rare	Minor	Low	A succession plan is in place to ensure key staff are either maintained or a succession plan is in place	GN	Ongoing with an annual review
2.10	Currency of promotional material	Breach of compliance of Standard 1 National Code 2018	Rare	Minor	Low	Promotional material is reviewed by Program Directors and Executive Dean annually, signed off by GN.	GN and CM	Ongoing with annual review

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
3.0 Academic & Student Matters								
3.1	Quality of courses articulating into UBSS	Maximise appropriate fit	Possible	Moderate	Medium	Strengthened credit transfer policy that is regularly reviewed	GW	Reviewed quarterly
3.2	Weak academic intervention process for non-performing students	High attrition, Low progression and Low Completion rates and non-compliance with ESOS Act and TEQSA	Rare	Major	Medium	Strengthened processes including early intervention, invigilated examinations, provision of support workshops	GW	Ongoing
3.3	English Language Proficiency	Unsatisfactory academic progression	Unlikely	Major	Medium	Selection processes ensured coupled with ongoing support	GW	Ongoing
3.4	Regular monitoring and maintenance of programs, subjects and academic integrity	Assurance and re-accreditation	Possible	Moderate	Medium	Monitoring of currency of programs and courses maintained Monitoring and management of academic integrity	GW	Annual Reviews conducted Academic Integrity Committee operations
3.5	Maintaining eResources	Impact on support for students	Rare	Moderate	Low	Maintaining high levels of eResourcing including eLibrary (ongoing expansion) and LMS The EZProxy system is used at GCA to allow transparent e-library access from any location.	GW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
3.6	Failure of students to complete within CoE due to poor timetabling and load enforcement	Breach of international student visa conditions; student may transfer to other providers with flexible timetabling	Unlikely	Major	Medium	Maintaining careful record of progression and students satisfying VISA conditions	GW	Ongoing
3.7	Academic quality assurance compromised due to an absence of benchmarking,	Negative impact on TEQSA accreditation outcomes	Rare	Major	Medium	Proactive involvement in a range of local, national and international benchmarking activities	GW	Ongoing
3.8	Failure to create positive esteem and confidence across the GCA student body	Students retention problems; negative impact on external reputation	Unlikely	Moderate	Low	Focus on success stories and profiling of institution - especially externally (ie QILT)	GW	Ongoing
3.9	Packaged pathway not properly managed	Student expectations mismanaged	Unlikely	Moderate	Medium	Management of pathways	GW	Ongoing
3.10	Lack of external assessment moderation to ensure quality assurance in assessments and standards.	Assessment items not moderated against subject learning outcomes which may impact rigour and quality of courses.	Rare	Major	Medium	Adherence to Assessment Moderation Policy	GW	Reviewed regularly

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
3.11	Poor QA and monitoring of Third Party Agreements (TPAs)	TPAs not established and monitored with provision for effective risk management, and QA/delivery provisions	Rare	Moderate	Low	No third party agreements currently in place	GW	Currently no third party arrangements in place
3.12	Student Harassment onsite	Students under duress	Unlikely	Moderate	Medium	Policies and procedures (including code of conduct) in place, student orientation is used to discuss issue, a designated employee is in place to support students	GW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
4.0 Staffing								
4.1	Inability to recruit & retain appropriately qualified teaching staff	Poor teaching/ academic standards and breach of accreditation standards	Rare	Major	Medium	Maintaining high levels of staff and ensuring AQF+1 or equivalent status. Staff surveys completed and monitored every trimester. Annual performance review of academic and administrative staff	GW and GN	Ongoing
4.2	Staff not recruited who embody the corporate values and mission of GCA	Staff expectations not aligned with those of GCA; poor job retention levels	Unlikely	Minor	Low	Ensure appropriate selection of staff. Staff surveys completed and monitored every trimester. 6 month probation	GW and GN	Ongoing
4.3	High student: staff ratios (SSR) as a result of increasing enrolments	Large class sizes and compromised learning environment; compliance breaches	Likely	Moderate	Medium	Ensuring SSR is managed and monitored	GW and GN	Ongoing
4.4	Balance of part-time and full time staffing Permanent FT, PT, Casual and Contract	Access to staff becomes an issue for students	Unlikely	High	Medium	Ensuring balance is considered without diminishing quality and experience	GW and GN	Ongoing– evidenced in SFUs and QILT outcomes
4.5	HR impact on closures for Central and Metro	Impact on individual staff	Likely	High	Medium	Employing the services of AFEI to ensure the closure of Metro and Central colleges are followed legally and efficiently.	GW and GN	13 December 2018

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
4.6	All new staff to complete a detailed Staff Induction.	Failure to meet TEQSA requirements and non-compliance, staff disruption and a breach of WHS guidelines.	Likely	High	Medium	Ensuring uniformity, consistency and staff retention.	GW and GN	Ongoing
4.7	Adequate functionality is provided for both staff (working from home and working on campus) operational structures	Failure to ensure adequate infrastructure that would impact on productivity, WHS and staff welfare	Likely	High	Medium	Ensuring appropriate infrastructure is in place. Monitoring and safety checks on home working environments (WHS Working from Home checklist)	GW and GN	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
5.0 Finance & Sustainability								
5.1	Reliance on international student market as primary revenue source across UBSS and other Colleges	Changes to government policy may reduce applications and enrolments	Likely	Moderate	Medium	Maintain interest in market diversity	PH	Quarterly and Ongoing
5.2 **To be removed**	Inability to rectify deficit equity position for GCA	Financial insolvency and closure; High financial risk rating by TEQSA	Unlikely	Major	Medium	Maintain quality management of finances	PH	Quarterly and Ongoing
5.3	Inability of GCA to maintain adequate operating surpluses and cash liquidity	Financial insolvency and closure; high financial risk rating by TEQSA	Unlikely	Major	Medium	Maintain quality management of finances. Regular financial reporting and forecasting	PH	Quarterly and Ongoing
5.4	Increasing operating and lease costs not being matched by course price increases and student break even numbers	Inability to cover operating costs	Rare	Medium	Low	Maintain quality management of finances Regular financial reporting and financial analysis	PH	Quarterly and Ongoing
5.5	Intercompany loans to related companies not repaid	Potential write-off of loan in GCA	Possible	Moderate	Low	Maintain quality management of finances	PH	Quarterly and Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
5.6	Failure to continually automate staff and student administrative procedures using available technology to reduce overhead costs	Increased employment expenses and negative impact on profitability	Rare	Insignificant	Low	Maintain vigilance in automation and eSolutions	PH	Quarterly and Ongoing
5.7	Inability to comply with the ESOS Act and requiring safeguard of student fees paid in advance and student refunds	GCA unable to appropriately refund students within 28 days and manage the prepaid fees designated bank account	Unlikely	Moderate	Low	Establishment of designated bank account in accordance with ESOS Act Tuition Protection Scheme (TPS) in place	PH	June 2012 Annual Renewal
5.8	Poor documentation and procedures related to corporate succession planning	Procedures not available in case of critical illness, death or incapacitation of CEO in terms of business continuity across GCA.	Possible	Moderate	Medium	Maintain focus on succession planning and sharing of information across the company	PH	Quarterly and Ongoing

5.9	Fraud	Financial misappropriation	Possible	Moderate	Medium	Internal controls including delegating authorities; separation of duties; and two-factor authentication for payment approval.	PH	Ongoing

6.0 Technical								
Risk Category & Item	**Risk Description**	**Impact Scenario**	**Risk Likelihood**	**Risk Consequence**	**Risk Impact Rating**	**Risk Mitigation Strategy**	**Risk Owner**	**Status**
6.1	Failure / performance degradation of internet connection between GCA and Amazon Cloud	Inability of GCA staff and students to access any IT resources	Unlikely	Major	Medium	Two independent internet connections exist between the main GCA site (UBSS) and the Amazon EC2 cloud environment. Each connection is capable of independently handling the required traffic load. All GCA traffic can be instantly switched from one connection to the other if necessary. All network routing is automatically updated when connections are switched. IT staff are instantly alerted when a connectivity issue exists on either connection. Ping time and packet loss between all GCA sites and Amazon EC2 are constantly monitored. IT staff are instantly alerted if ping time or packet loss fall outside of acceptable limits.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.2	Failure / data corruption of one or more GCA servers	Inability of GCA staff and students to access affected IT resources	Unlikely	Major	Medium	All GCA servers (with the exception of the firewall) reside within the Amazon EC2 Cloud Computing environment. EC2 servers reside in a secure, environmentally controlled off-site data centre. EC2 servers are automatically restarted on new hardware in the event of a hardware failure (EC2 Instance Auto-Recovery). All volumes attached to all EC2 servers have data snapshots taken every day. One week of daily snapshots are taken (rolling window), and independent snapshots are taken on Jan-1 and Jul-1 each year. Any server snapshot can be used to restore a server to the exact state that it was at when the snapshot was taken. A server can be restored from a snapshot in around 10 minutes. EC2 snapshots are automatically mirrored across different EC2 Availability Zones and data centres, eliminating a single point of failure. All database instances used by GCA (with the exception of Oracle) are located within the fault-tolerant Amazon RDS managed database system. The Oracle instance used by GCA is located within the Amazon EC2 environment. Amazon have a Service Level Agreement which states that they will maintain their systems to achieve a minimum of 99.99% uptime each month. All GCA databases have daily snapshots taken, stored with in the fault-tolerant Amazon S3 storage system. Due to the low cost of S3 storage, all snapshots are retained indefinitely, regardless of their age.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.3	Failure of GCA servers / workstations to receive timely system updates	GCA servers / workstations remain vulnerable to security flaws that have already been patched by the software vendor These security flaws could be used to cause a denial of service, or the unauthorised access to GCA data	Possible	Moderate	Medium	All GCA servers and workstations operate on operating systems that are currently supported by the software vendor, and therefore receive regular updates (Windows 10 LTSC) All GCA servers and workstations that operate on the Windows platform have updates for Microsoft software deployed via Windows Server Update Services (WSUS). IT staff are notified when new updates are available for deployment. IT staff regularly check WSUS to see if any updates are pending, or any update installation failures were reported. IT staff are given an up to date count of the number of systems that have not had an update installed in the last 30 days. A custom script runs every 60 seconds, which alerts IT staff if any running system has not installed the latest approved WSUS updates. A custom script runs every 60 seconds, which alerts IT staff when new updates have been released by Microsoft into WSUS. IT staff can then approve the updates after testing. McAfee Virus Definitions automatically update when new versions are available. Checks are performed every 30 minutes and immediately after a PC starts up.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.3 (continued)						A custom script runs every 60 seconds, which alerts IT staff if any running system does not have the latest AV definitions installed, or has not reported to the McAfee ePO server in the last 24 hours. Other software (Dropbox, Google Chrome, Firefox, Adobe Acrobat, etc) auto-updates without any user intervention. The GCA WSUS and ePO servers are externally accessible via a VPN, allowing GCA systems that are operating outside of the internal network to continue to receive updates. All workstations at GCA use the LTSC (Long Term Servicing Channel) edition of Windows 10. This edition ensures a consistent operating environment, and guarantees a 10 year supply of security updates.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.4	Software updates to GCA servers / workstations causing a system failure or adversely affecting system operation	Inability of GCA staff and students to access affected IT resources	Rare	Moderate	Low	All GCA servers and workstations that operate on the Windows platform have updates deployed via Windows Server Update Services (WSUS). All updates made available within WSUS must be approved by IT staff before they are deployed. Updates are deployed onto a test PC for testing prior to deployment. Server snapshots are taken prior to any updates being deployed. The server can then be rolled back its previous state in the event that the update causes a failure.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.5	Failure / data corruption of one or more GCA workstations	Inability of one or more GCA students or staff to access any IT resources If a classroom workstation fails, inability of the lecturer to carry out their teaching	Possible	Minor	Medium	One standardised Windows disk image is used for all Windows based workstations at GCA (Windows 10 LTSC). Workstations can be swapped with others without affecting functionality. Staff and student workstations can be swapped without affecting functionality. Any configuration differences between staff, student, and classroom workstations are automatically handled via Windows Group Policy. Spare pre-configured workstations are ready to be swapped in place of a defective one. No GCA data is stored on the local hard disk of any workstation (apart from roaming profile caches and the local user profile). Failure of a workstation will therefore never result in data loss. Some workstations are thin-client terminals, which have no moving parts. This dramatically reduces the likelihood of a hardware failure. Thin-client terminals are all remotely configured from a central server, resulting in quick deployment.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.6	Failure / data corruption of an on-site GCA firewall server	Inability of all GCA staff and students at the relevant site to access any IT resources	Unlikely	Major	Medium	Only one live server exists at each GCA site. Each live on-site server is covered by a 24x7x365 hardware maintenance plan supplied by Interactive Systems Availability. This maintenance plan covers all hardware components of the server, and ISA guarantee a maximum 2 hour response time. At the main GCA site (UBSS), a second server exists, running the vSphere Replication system. This replication server constantly keeps a snapshot of the configuration of the live servers at all other GCA sites. Historical snapshots are also kept (5 snapshots at 60 minute intervals on a rolling window), allowing a previous server snapshot to be used if the data corruption occurs. If any on-site server were to irreparably fail, the replication server could be switched into the place of the live server, allowing normal operation to resume. The on-site server rooms are fitted with temperature and humidity monitoring devices. IT staff are alerted if the temperature or humidity exceed normal levels. The hardware status of all on-site servers is constantly monitored, alerting IT staff when any status error occurs. Each on-site server features redundant power supplies, and RAID disk arrays (with at least one hot spare).	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.6 (continued)						The hot-spare is automatically utilised in the event of a disk failure, and IT staff are alerted. All configuration information for the on-site server (DHCP, file shares, firewall configuration) is stored within Amazon EC2. This allows for the on-site server to be manually rebuilt as a last resort. The age of the configuration backup file is monitored to ensure that the most recent backup is never older than 24 hours. A UPS is used to maintain power to the on-site sever, and all core network switches in the event of a power failure or brownout. The UPS status is constantly monitored, alerting IT staff when the UPS has activated, or when it requires a battery replacement. The UPS internal temperature is also monitored to ensure that it remains within normal limits.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.7	Failure of periodic data export tasks to execute successfully	Inability of GCA databases to be restored to previous versions if required. Inability of GCA databases to be recovered in the event of data corruption.	Unlikely	Moderate	Medium	A custom script runs every 60 seconds, checking for the existence of backup files associated with all GCA database instances. The script also checks the age of the most recent backup. As each backup is made once a day, the latest backup should not be more than 24 hours old. If the backup is missing, incomplete, or too old, IT staff are alerted. The age of the configuration backup file for the on-site firewall is monitored to ensure that the most recent backup is never older than 24 hours. The age of the configuration backup file for the on-site file server mount point is monitored to ensure that the most recent backup is never older than 24 hours.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.8	Failure of periodic Amazon EC2 server snapshots tasks to execute successfully	Inability of GCA servers to be restored to previous versions if required. Inability of GCA servers to be recovered in the event of data corruption.	Unlikely	Moderate	Medium	A custom script runs every 60 seconds, checking for the existence of snapshots associated with all Amazon EC2 servers. The script also checks the age of the most recent snapshot. As each snapshot is generated once a day, the latest snapshot should not be more than 24 hours old. If the snapshot is missing, incomplete, or too old, IT staff are alerted. The number of snapshots for each volume are also checked - if too few exist, IT staff are alerted.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.9	Malicious / unauthorised software executing on any GCA workstation or server	Loss or corruption of data on GCA workstations / servers Data being encrypted by malicious software and held for ransom (ransomware) GCA workstations / servers being used as peers in a botnet (denial of service attacks)	Rare	Moderate	Low	All users of all GCA systems run as a Windows limited user. No staff run as an Administrator or Power User. Only IT staff have Administrative rights, and they are only used when required. IT staff run as a limited user by default, and elevate to Administrative rights via User Account Control only when required. Any application that is not pre-installed by an Administrator cannot be executed. Any application that resides on any removable media (including CD / DVD / USB / external HDD) cannot be executed. Applications cannot be executed from any folder to which a standard Windows user has write access (this includes the user profile folder) McAfee VirusScan Enterprise is installed on every Windows based GCA workstation and server. McAfee VirusScan Enterprise is configured to scan all executable and document files for both read and write access across all drives. McAfee VirusScan Enterprise is configured to scan the memory of each workstation and server for malicious software and rootkits every 60 minutes.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.9 (continued)						McAfee VirusScan Enterprise is configured to scan the entire boot drive of every workstation once per week. All GCA workstations and servers check every 30 minutes (and immediately after startup) for updated AV definitions from McAfee. A custom script runs every 60 seconds, which alerts IT staff if any running system does not have the latest AV definitions installed, or has not reported to the McAfee ePO server in the last 24 hours. IT staff are alerted if any workstation or server generates a McAfee AV detection event. All Windows based workstations and servers receive timely updates from Microsoft (via WSUS), reducing the likelihood of a remote code execution exploit. A custom script runs every 60 seconds, which alerts IT staff if any running system has not installed the latest approved WSUS updates. A custom script runs every 60 seconds, which alerts IT staff when new updates have been released by Microsoft into WSUS. IT staff can then approve the updates after testing. All GCA servers have data snapshots taken daily (see section 6.2). This allows for corrupted / encrypted data to be rolled back to an older version.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.9 (continued)						All GCA workstations have their web traffic filtered by the Cisco Umbrella (OpenDNS) filtering system. This system updates in real time, and blocks malicious websites from being loaded, along with websites that fall into categories that are considered to be undesirable. A custom script runs every 60 seconds, which alerts IT staff if the network DNS resolvers are not using OpenDNS. Alerts are also sent out if the incorrect web filtering rules are being used within OpenDNS. Software Restriction Policies have been defined for all GCA workstations, whereby the execution of all software is blocked by default – exclusions are then added for the software that is required. All E-mail traffic to and from any GCA address is protected by the Office 365 Advanced Threat Protection system. This system scans all email links to identify those that are malicious, and also monitors email traffic to identify emails that impersonate key GCA staff members. All GCA workstations can only access the servers and ports that are required for normal operation. This limits the effect of any malicious software that does manage to execute on a workstation.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.10	GCA servers / network infrastructure not having adequate capacity to support the prevailing load	Loss of performance for affected GCA IT resources Inability of GCA staff and students to access affected IT resources	Unlikely	Moderate	Medium	Key performance metrics of all GCA servers are constantly monitored (CPU usage, memory usage, ping time, packet loss, disk usage, disk queue length, network bandwidth, TCP packet retransmission rate, event log errors) IT staff are alerted when any metric exceeds a predefined warning threshold, and again if the metric exceeds a predefined alarm threshold. All GCA servers reside within Amazon EC2, and can therefore have their performance levels changed at any time without any loss of data. Server disk capacity and performance can be expanded at any time without incurring any downtime. Server CPU and memory capacity can be changed at any time (downtime is incurred). Software-specific performance metrics are also monitored on all GCA servers to indicate software level performance issues. GCA Remote Desktop Servers operate in a load balanced server farm, allowing capacity to grow and shrink in accordance with demand. All GCA VLANs use bandwidth limiting / bandwidth reservation to ensure that bandwidth is always available for key GCA systems. All GCA database instances are monitored for the number of active and rejected connections to ensure that the connection limit is not reached. All GCA database instances are monitored for any wait or lock conditions to ensure that database transactions are not delayed.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.10 (continued)						The memory usage and thread count for the main Oracle database instance are monitored. The CPU utilisation, memory utilisation, fan status and port bandwidth usage for all network switches is monitored via SNMP. Alerts are sent out if any parameter exceeds normal values. All network switches are monitored for any packet transmission errors (CRC, packets dropped, jabber, undersize / oversize packets). Alerts are sent out if any of these conditions are detected. The CPU utilisation, memory utilisation and number of associated clients for all wireless access points is monitored via SNMP. Alerts are sent out if any parameter exceeds normal values. All GCA workstations use Solid-State Disks (SSDs) as their boot drives to ensure good system performance.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.11	GCA servers not running key system services / processes	Inability of GCA staff and students to access affected IT resources	Rare	Moderate	Low	Current running processes and system services are monitored on all GCA servers, to ensure that the services responsible for providing the applicable IT resources are active. IT staff are alerted when any monitored process or system service is not running. Critical processes / system services are automatically restarted in the event of a failure. Persistent database connections from key system processes are monitored to ensure that they are re-established in the event of a database connection issue or outage. The scheduled Moodle Cron task is monitored for all Moodle instances to ensure that it has run on schedule. The card printer database is checked every 60 seconds to ensure that is has correctly synchronised with the main myGCA database (daily synchronisation task).	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.12	Unauthorised access to physical infrastructure (server room)	Physical damage to IT infrastructure Theft of IT related equipment Inability of GCA staff and students to access affected IT resources	Unlikely	Major	Medium	The server rooms at all GCA sites have no signage nor windows to indicate the contents / purpose of the room. The server rooms at all GCA sites are physically secured by two Bi-Lock locks (one of which is a deadbolt). The server room at the UBSS site has an internal camera which records all detected motion. IT staff are immediately alerted if motion is detected on the camera, and snapshots are sent along with the alert.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.13	Unauthorised access to internal GCA network (rogue devices)	Loss of connectivity between affected GCA devices and the network A heightened risk of attacks being launched against GCA servers Data loss or corruption within affected GCA systems	Unlikely	Moderate	Medium	All DHCP assigned network addresses must have a pre-set reservation, locking an IP address to a hardware address. Any device that does not have a matching network address is prevented from communicating with our firewall (and any servers). IT staff are immediately alerted if a device attempts to claim an IP address without a corresponding reservation. IT staff are immediately alerted if an IP address conflict develops between any GCA server and another device. GCA network devices that can cause network issues due to instability are isolated from the main GCA network via a physical VLAN. The open wireless network (for guest use) is isolated from the main GCA network via a physical VLAN. All GCA network devices can only access the servers and ports that are required for normal operation. The only workstations that have full network access are the designated IT management workstations. All domain accounts are set to automatically lock for a 2 hour period if 20 incorrect password attempts are detected in 1 10 minute period. IT staff are alerted if any domain account becomes locked.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.14	Unauthorised access to internal GCA network (console access to servers)	Loss of connectivity between affected GCA devices and the network A heightened risk of attacks being launched against GCA servers Data loss or corruption within affected GCA systems	Rare	Major	Medium	All server administration passwords are unique, randomly generated, and meet Amazon's password complexity requirements. IT staff are immediately alerted when any direct console access is obtained to any GCA server (regardless of the access level). Only local administrative accounts are permitted to log onto GCA servers (domain accounts are blocked by default). Only designated IT management workstations can connect to servers via RDP. All domain accounts are set to automatically lock for a 2 hour period if 20 incorrect password attempts are detected in 1 10 minute period. IT staff are alerted if any domain account becomes locked.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.15	Unauthorised access to internal GCA network (file system access to servers)	Loss of connectivity between affected GCA devices and the network A heightened risk of attacks being launched against GCA servers Data loss or corruption within affected GCA systems	Rare	Moderate	Medium	Newly created GCA accounts have no access to any shared network resources. Required resources are provided only when necessary. For GCA servers that do not have available file shares, the number of open files and file sharing sessions are monitored. IT staff are immediately alerted if files are opened via a file share session.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.16	Unauthorised access to internal GCA network (from outside)	Loss of connectivity between affected GCA devices and the network A heightened risk of attacks being launched against GCA servers Data loss or corruption within affected GCA systems	Possible	Moderate	Medium	All GCA servers have external access restricted via the Amazon Security Group (firewall). Only ports that are required for public access are opened (HTTP / HTTPS, etc). Servers that are only used internally have no publicly accessible ports. Servers that require external access only for specific GCA staff are only accessible from a set range of source IP addresses. On-site GCA servers (firewalls) have no publicly accessible ports. All internal network traffic which passes between any GCA site and Amazon EC2 is encrypted within an IPSec VPN tunnel (50 character random pre-shared key). VPN endpoints are only visible to the corresponding tunnel endpoint via IP address filters. Any changes to the file system of any GCA website are logged, and IT staff are alerted. All GCA websites utilise an independent worker process, and an independent file system access user. This ensures that if one site is compromised, it cannot access data on any other site.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.16 (continued)						All GCA websites run with a limited user account which can only read the file system data for that site. If the user account requires read/write access to the file system, it is granted at the most granular level possible. All domain accounts are set to automatically lock for a 2 hour period if 20 incorrect password attempts are detected in 1 10 minute period. IT staff are alerted if any domain account becomes locked. All PHP website execution errors are logged and IT staff are alerted. Any failed login attempts to the GCA Remote Access Gateway server are logged, and IT staff are alerted. The number of attempted connections to the GCA Remote Access Gateway are monitored to ensure that the gateway does not become unavailable due to repeated connection attempts exhausting the number of available TCP sockets. IT staff are alerted when a connection is made to any GCA database instance from an unauthorised IP address. All GCA domain names are checked every 60 seconds to verify that they resolve (via DNS) to the correct IP address. Failure to resolve to the correct address indicates that the DNS records have been compromised.		

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.17	Unauthorised access to third party provider portals (DNS, domain names, SSL Certs, email, cloud hosting)	Loss of connectivity between affected GCA devices and the network A heightened risk of attacks being launched against GCA servers Data loss or corruption within affected GCA systems	Unlikely	Major	Medium	Two-factor authentication is enabled for all third party administration portals that support it. This includes Amazon EC2, Office 365, Dyn Managed DNS, Cisco Umbrella, and GoDaddy SSL Certs. The use of an authenticator app is preferred over the use of SMS (where supported).	JW	Ongoing
6.18	Use of master / over-privileged access credentials for automated system tasks	Loss of master administration credentials to GCA systems Data loss or corruption within affected GCA systems	Rare	Minor	Low	Special access accounts / keys are created for automated system tasks, granting only the required set of access permissions. These accounts / keys can be revoked / disabled if it is found that they have leaked. Access credentials / keys are not stored in plain text within administration scripts (wherever possible)	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.19	Insufficient Remote Desktop Client Access Licences (CALs)	Inability of GCA staff to remotely access any IT resources Inability of GCA staff / students to access any IT resources via thin client terminals	Unlikely	Moderate	Medium	Device CALs are used instead of User CALs. This ensures that GCA always complies with the licencing agreement, as devices cannot function without a valid Device CAL. The number of available Device CALs are monitored every 60 seconds via a custom script. If less than 5 Device CALs are available for use, IT staff are alerted. An order can then be placed for additional CALs, or unused devices can have their CALs revoked.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.20	Internally generated e-mail or SMS messages not reaching their intended recipients	GCA staff and students may miss important written communications. IT staff may miss important status notification and alert messages.	Unlikely	Minor	Low	All internal GCA systems that send emails use one or more mail relays. Each mail relay has an outbound mail queue, and a failed mail queue. Every 60 seconds, a custom script monitors the length of these queues across all mail relays, and alerts IT staff if the outbound mail queue reaches a set level. Mail that remains in the outbound queue indicates an issue with the mail delivery system that needs attention. If any mail reaches the failed mail queue (repeated delivery attempts all failed), IT staff are also alerted. Once the delivery issue has been resolved, the outbound mail queue will automatically clear. Mail that is present in the failed queue can be manually moved to the outbound queue by IT staff once the delivery issue has been resolved. The SMS credit balance for both SMS providers used by GCA is constantly monitored, and IT staff are alerted if the balance falls below a set threshold.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.21	Data submitted to GCA websites being intercepted and captured	Leakage of private data from GCA staff / students. GCA website data being changed by unauthorised persons.	Rare	Moderate	Low	All GCA websites (including those only used internally) operate on the HTTPS protocol. Any attempt to access any GCA website via HTTP results in an immediate redirection to HTTPS. HTTP Strict Transport Security (HSTS) is enabled for all GCA websites with a 12 month validity period. All GCA websites operate on the TLS 1.2 connection protocol (SSL protocols are disabled, and the TLS 1.0/1.1 protocols are still enabled for backward compatibility). All GCA websites have attained either an A or A+ rating from the Qualys SSL Labs SSL test (https://www.ssllabs.com/ssltest/) All GCA domains have a CAA record containing the approved issuers of SSL certificates for that domain. A custom script runs every 60 seconds, alerting IT staff if the SSL certificate for any GCA website is due to expire in less than 30 days. This ensures that certificate warnings are never displayed. Any changes to the file system of any GCA website are logged, and IT staff are alerted.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.21 (continued)						The Google Password Checkup extension is deployed to all installed instances of Google Chrome (via Group Policy), to alert users if their passwords have been compromised.		
6.22	Inability to access deleted emails from a GCA staff or student account	Inability to access important historical data	Rare	Minor	Low	Emails deleted from any GCA staff or student account first move into the Deleted Items folder, from which they can be retrieved easily. If the Deleted Items folder it itself cleared, those emails can be recovered for a further 30 days. If more than 30 days has existed between the clearout of the deleted items folder and the recovery attempt, the GCA Mail Journal can be used to recover the message. The GCA Mail Journal is a separate mail server (within Amazon EC2), which stores a copy of each and every email that is either sent from or received by any GCA (Office 365) mail account. Only IT staff can access this Journal, and it therefore cannot be affected by individual users deleting their own emails.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.23	Inability to access deleted files from a GCA staff or student account	Inability to access important historical data	Rare	Minor	Low	The GCA file storage repository utilises the Amazon Storage Gateway cloud storage system. Daily snapshots are taken of the file system, which are stored in the fault-tolerant Amazon S3 storage facility. One week of daily snapshots are taken (rolling window), and independent snapshots are taken on Jan-1 and Jul-1 each year. Any snapshot can be mounted onto an Amazon EC2 server for file retrieval in around 15 minutes.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.24	Accounts for inactive GCA staff or students remaining active	Unauthorised access to GCA data and systems Data loss or corruption within affected GCA systems	Possible	Moderate	Medium	GCA student accounts are automatically deactivated when the student no longer has an active course within GCA, or if they become non-financial for an extended period of time. GCA staff accounts are deactivated (or created) by IT staff only when written instructions are received from the Accounts Department. Every 6 months, IT staff compile a list of active staff accounts, and match this against the list of current GCA staff. Any outstanding accounts are deactivated. Automated account management scripts and checklists used by IT staff ensure that access accounts for all IT systems are deactivated at the same time. If any active system account has not been used for a 60 day period, IT staff are alerted.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.25	Reported IT issues not being handled in a timely manner	Delays in selected GCA staff / students being able to utilise IT resources	Unlikely	Moderate	Medium	A trouble ticket lodgement and monitoring system (Redmine) is used by all GCA staff. Staff lodge a ticket when any IT related issue is found. IT staff are notified when a ticket is lodged, and any updates to the ticket are logged within Redmine. IT staff can easily see what items are outstanding, which items require feedback from the reporter, and which items have been resolved.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.26	Inability to access the HEPCAT (higher education reporting software) when required	Inability of GCA to meet its reporting obligations to the Federal Government	Rare	Major	Medium	In order to report the higher-education student data to the Federal Government, a specific program (HEPCAT) must be used. This program maintains a locally stored database on whatever PC it is running on, and therefore can only be installed and used on a single PC. All GCA staff who need to use HEPCAT would normally be forced to all use the same PC, and remote access to HEPCAT would therefore be impossible. As the database is locally stored, any failure of the PC would result in the loss of HEPCAT data. This risk has been mitigated by installing HEPCAT onto a Windows Remote Desktop server, located in Amazon EC2. This server can be accessed by any authorised person, from any location via Remote Desktop Services. As the server now resides in Amazon EC2, the data is backed up via the Snapshot system (see section 6.2). This ensures that the HEPCAT data is secure and backed up.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.27	Failure of a non-workstation IT related device	Inability of GCA staff and students to access affected IT resources	Possible	Moderate	Medium	All network devices are monitored every 60 seconds for their reachability. IT staff are immediately alerted if any network device fails to respond. Spare devices are kept on-site to replace any faulty ones (network switches, VOIP handsets, projectors, card scanners etc…) The fan status and power supply status for all network switches is monitored via SNMP. Alerts are sent out if any parameter exceeds normal values. The status of all data projectors is monitored via SNMP to retrieve the status of the device and lamp hour count. IT staff are alerted if any projector shows a warning or alert condition, or if the lamp hours have exceeded the replacement interval. This allows for the lamp to be replaced during normal downtime without causing an unexpected failure. All printers and copiers are constantly monitored via SNMP to retrieve the status of the device and level of all consumables. This allows for printer consumables to be replaced during normal downtime without causing an unexpected failure.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.27 (continued)						The display settings for all data projectors are automatically reset when a user logs in to ensure that the projectors and interactive whiteboards can be used properly.		
6.28	Internal GCA systems taking part in denial of service attacks against other networks	Major loss of system performance and internet bandwidth capacity for GCA staff and students	Rare	Moderate	Low	Unauthorised programs cannot be executed on any GCA workstation (see section 6.9) Outbound TCP / UDP ports which are not required for normal operation are blocked for all GCA workstations. No GCA workstations can send outbound mail on SMTP port 25 (regardless of the firewall setting) unless specially configured. All internal GCA mail relays can only be accessed by specific internal IP addresses, and their queue length is constantly monitored.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.29	Unauthorised access to internal GCA network via Wi-Fi	Unauthorised access to GCA data and systems Data loss or corruption within affected GCA systems	Rare	Moderate	Low	Two separate Wi-Fi networks are in use at GCA - one open network, and one encrypted network. The open network is physically isolated from the main GCA network (separate Access Points, switches, etc). No data can physically traverse from the open network to the main GCA network. The encrypted network is only available for internal GCA network devices. The encrypted network utilises WPA2-PSK encryption (AES cipher), with a random PSK which is 64 characters long (the maximum length). All Access Points have the latest manufacturer's firmware installed. A custom script runs every 60 seconds, checking for new firmware and alerting IT staff if a new version is available. The open network is only available for use during working hours. Any user of the open network must accept the Terms and Conditions of Use before access is granted. The open network only allows for public internet traffic (HTTP and HTTPS). All other outbound ports are blocked. IT staff are immediately alerted if the internal GCA network is bridged with the open Wireless LAN for any reason.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.30	Unauthorised access to GCA systems by external contractors of GCA	Unauthorised access to GCA data and systems Data loss or corruption within affected GCA systems	Unlikely	Minor	Low	The configuration of all access points is monitored to ensure that encryption is enabled when required. No "guest" or temporary access accounts exist within the GCA network. Any accounts required for external contractor access are only created once written approval is received from the relevant department head. All such accounts have an expiry date set, after which the account will automatically disable itself. The default access level for any newly created account is the minimum required. Additional access is only granted once written approval is received from the relevant department head.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.31	Unauthorised access to GCA systems via venerable IoT (Internet of Things) devices	Unauthorised access to GCA data and systems Data loss or corruption within affected GCA systems	Unlikely	Moderate	Medium	All IoT devices used at GCA are installed on a physically separated VLAN (CCTV cameras, VOIP phones, card scanners, temperature sensors, printers etc). To ensure that bandwidth is always available for IoT devices (CCTV / VOIP), each class of devices have their own physical VLAN. IoT devices cannot access the Internet - nor can they access any other VLAN. They can only access the server (and the specific ports) to which they need to communicate. None of the IoT devices used at GCA use their default access credentials. All IoT devices use the latest firmware that is available. A custom script runs every 60 seconds, checking for new firmware and alerting IT staff if a new version is available. All IoT devices connect to servers that are hosted and controlled by GCA.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.32	CCTV cameras failing to record for an extended period of time	Loss of visual evidence of any incident that were to occur at GCA Inability to identify unauthorised persons who entered GCA property	Rare	Minor	Low	A custom script runs every 60 seconds, checking for the existence of recording files associated with each CCTV camera. If a camera has not recorded to disk in the last 48 hours, IT staff are immediately alerted.	JW	Ongoing
6.33	System database instances becoming full and incapable of storing additional data	Failure of myGCA system or any other system that utilises a database instance	Rare	Moderate	Medium	A custom script runs every 60 seconds, checking the amount of free space within the Oracle USERS tablespace. If the available space drops below 10%, IT staff are alerted, and can then manually add another file to the tablespace. For other database instance types (MySQL and MS-SQL), the amount of free space on the storage volume is checked every 60 seconds. If the available space drops below 10%, IT staff are alerted and can then manually expand the volume size.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.34	TEQSA document submission portals becoming unavailable	Failure of GCA to submit documents to TEQSA within the set timeframe. GCA being in breach of our obligations to TEQSA.	Possible	Moderate	Medium	If a TEQSA portal is unavailable, GCA will inform TEQSA in writing and seek confirmation from TEQSA that the issue is with their systems. GCA will then seek confirmation from TEQSA that if the submission deadline is missed, it will NOT be the fault of GCA.	JW	Ongoing
6.35	User credentials being compromised due to “phishing” emails being opened by GCA staff	Unauthorised access to GCA systems Loss of data from GCA systems Malicious manipulation of data within GCA systems	Possible	Moderate	Medium	All E-mail traffic to and from any GCA address is protected by the Office 365 Advanced Threat Protection system. This system scans all email links to identify those that are malicious, and also monitors email traffic to identify emails that impersonate key GCA staff members. All GCA workstations have their web traffic filtered by the Cisco Umbrella (OpenDNS) filtering system. This system updates in real time, and blocks malicious websites from being loaded, along with websites that fall into categories that are considered to be undesirable.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
6.36	VOIP extensions being taken over by unauthorised persons	Inability of affected VOIP extensions to make or receive calls Unauthorised call charges being incurred against the GCA VOIP account	Unlikely	Minor	Low	All VOIP extensions have passwords that meet the Office 365 complexity requirements. All fixed VOIP extensions are locked down to a specific IP. Any device that attempts to register from a different IP will be rejected, even if the password is correct. This includes any external VOIP extensions that connect from a static IP address. External VOIP extensions that do not connect from a static IP address, but connect from a static internet connection have their IP addresses locked down to the range that the ISP uses. The IP addresses that external extensions are registered from are constantly monitored. IT staff are alerted if any extension registers from an IP address that is not located within Australia. If any external VOIP extension is configured for unrestricted access (from any source IP), IT staff are alerted. If a source IP attempts to register an extension but fails, the entire /24 IP range is blocked from communicating with the PBX.	JW	Ongoing

Risk Category & Item	Risk Description	Impact Scenario	Risk Likelihood	Risk Consequence	Risk Impact Rating	Risk Mitigation Strategy	Risk Owner	Status
7.0 Physical Resources								
7.1	Damage to the campus (classrooms, facilities, etc.)	Loss of teaching time; cancellation of classes; loss of staff productivity; high expenses to repair damage	Rare	Moderate	Low	Maintain current vigilance	JR and JW	Ongoing
7.2	Poor implementation and awareness of business continuity and disaster recovery processes	Inability to respond to an emergency relating to IT systems failure, physical damage to premises; respond to injury/death of students and staff; deal with impact of pandemic	Rare	Moderate	Low	Maintain current vigilance	JR and JW	Ongoing
7.3	Public relations disaster e.g. negative media attention	Key staff not identified who have authority to speak to the media. These staff not trained in appropriate protocol.	Possible	Moderate	Medium	CEO is the authority supported by the ED	AM	Ongoing

7.4	Impact of pandemic (COVID-19)	Loss of business and impact on operations	Likely	Major	High	Migration of classes from face-to-face to online classes. Retraining of staff to deliver online classes Upgrade of IT infrastructure to support online classes Transition for selected staff from onsite to working from home Use of online collaboration software for online meetings	JW and JR	From February 2020 onwards

15 SEPTEMBER 2017 UPDATE REVISION (INPUT) LOG

Professor Greg Whateley	**Executive Dean and Provost, UBSS**	**31 August, 2017**
Professor Ian Bofinger	**Executive Dean, AMPA**	**3 September, 2017**
Associate Professor Craig Ellis	**Dean, APIC**	**3 September, 2017**
Professor Ray Hayek	**Executive Dean, AIHW**	**5 September, 2017**
Associate Professor Andrew West	**Director, Centre for Entrepreneurship**	**5 September, 2017**
Professor Greg Whateley	**Executive Dean and Provost**	**6 September, 2017**
Alan Manly	**Chair, GCA Board of Directors**	**7 September, 2017**
Sir Gerard Newcombe	**GCA Marketing and Human Resources Director**	**8 September, 2017**
Scarlett Burns	**Principal, Central College**	**8 September, 2017**
Doris Leung	**Director of Studies, Metro English College**	**8 September, 2017**
Graham Lock	**GCA, Chief Financial Officer**	**8 September, 2017**
Jason Whitfield	**GCA, Technical Services and Training Manager and Chair, WHS Committee**	**8 September, 2017**
James Manly	**GCA, Communications Manager and Campus Manager**	**8 September, 2017**
Professor Greg Whateley	**Executive Dean and Provost, UBSS**	**11 September, 2017**
Alan Manly	**Chair, GCA Board of Directors**	**15 September, 2017**
Paul Nicolaou	**Independent Director, GCA Board**	**15 September, 2017**
Sir Greg Whitby	**Independent Director, GCA Board**	**15 September, 2017**
Professor Greg Whateley	**Executive Director, GCA Board**	**15 September, 2017**

Alan Manly	Chair	15 September, 2017	
Sir Greg Whitby	Independent Director	15 September, 2017	
Professor Greg Whateley	Executive Director	15 September, 2017	

Paul Nicolaou	Independent Director	9 November, 2017	