Queen Mary University of London

Matters Arising

Outcome requested:	Audit and Risk Committee is asked to **note** the matters arising from the minutes of the meeting held on 16 March 2022.
Executive Summary:	N/A
QMUL Strategy: strategic aim reference and sub-strategies	The effective management of the Queen Mary's governance arrangements underpins the ability to achieve the strategic aims.
Internal/External regulatory/statutory reference points:	N/A
Strategic Risks:	N/A
Equality Impact Assessment:	Not required
Subject to prior and onward consideration by:	Considered by the Committee only.
Confidential paper under FOIA/DPA	No
Timing:	N/A
Author:	Nadine Lewycky, Assistant Registrar (Governance)
Date:	16 June 2022
Senior Management/External Sponsor:	Peter Thompson, Chair of Audit and Risk Committee

Actions from the meeting of 16 March 2022

Minute no.	Action	Person responsible	Progress
2021.038[j]	**Strategic Risk Register [ARC2021/33]** The Committee agreed that it should monitor environmental risks alongside the Strategic Risk Register and would like to receive reports on the university's resilience to major external risks in a format to be discussed between the Chair and Chief Governance Officer.	Chief Governance Officer and University Secretary	A report on external risks has been included with the papers.
2021.039[d]	**Bi-annual cyber security report [ARC2021/34]** The Committee said that it was encouraged by the programme of work and the progress that had been achieved in recent years. The Committee asked for an overarching risk assessment showing a clear picture of the size of the risk and risk target. We used JISC's framework to evaluate cyber security readiness which would be shared with the Committee. The residual risk rating for information compliance had reduced on the Strategic Risk Register	Chief Information Officer	A presentation on the JISC cyber security list has been appended to the matters arising.
2021.046[b]	***Draft agenda for the next meeting [ARC2021/39]** The Committee asked for a deep dive on careers and employability to be added to the agenda.	Chief Governance Officer and University Secretary	Due to the availability of staff, this will be scheduled for the next academic year.

Queen Mary
University of London

JISC Cyber Questions

Audit & Risk Committee Update

Date: 31st May 2022

Version: 2.2

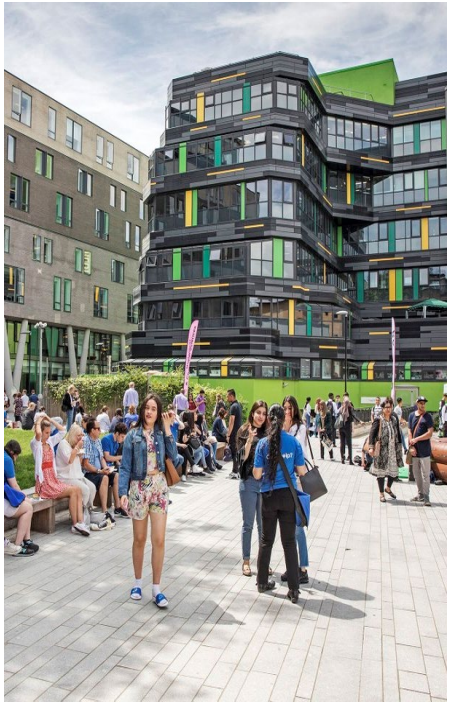
Document Owner: AD, Office of CIO

Background

The purpose of this presentation is to update the Senior Executive Team (SET) and the Audit and Risk Committee (ARC) following the issue of the JISC cyber security checklist sent to VCs by Paul Boyle (JISC Chair) in mid-November 2021.

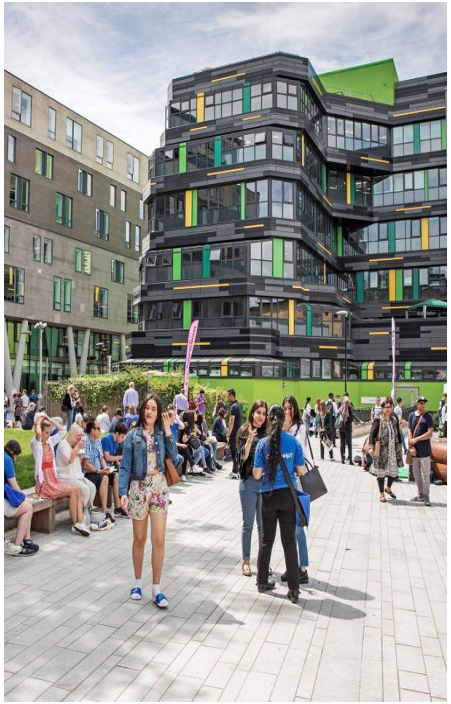
According to JISC, “these questions are designed to be used as part of a strategic approach to security and will help to determine what mitigations are in place or should be considered. It is a simple design and valuable starting point which Jisc can help you build on if required.”

It is envisaged that QM will want to expand these questions to reflect a more fit-for-purpose information security standard, such as ISO27001, which we are completing a current gap assessment against. In the mean-time we are reporting against the original 16.



Context

- The JISC 16 cyber security list is a broad-ranging set of questions covering a remit beyond ITS and touches on wider University capabilities / functions including data protection and business continuity.
- It is also worthwhile noting that achieving a ‘GREEN’ RAG status on these questions, does not represent a complete elimination of risk. It means that the risks have been reduced to an acceptable tolerance within the University’s risk appetite.
- Addressing the actions required to move the RAG status from RED, to AMBER, and finally to GREEN, will in many cases take a number of years. This is because the delivery of actions is dependent on the wider transformation goals within the ITS Enabling and Capital Plans.
- Some of the key multi-year programmes of work that are critical to successful delivery of these cyber security capabilities include the following:
  - ✓ Information Security strategy and programme
  - ✓ Journey to Cloud programme
  - ✓ Identity and access management programme
  - ✓ ITS Service Monitoring project
  - ✓ Managed Services Roll-out project
  - ✓ Business Continuity programme



RAG Definitions & Criteria

RAG Status	Criteria Description
GREEN	Risk appetite is within acceptable tolerance. There are no major outstanding issues that at this stage appear to threaten delivery.
AMBER	Risk appetite is outside of acceptable tolerance. Successful delivery appears feasible but significant issues already exist requiring management attention. These appear resolvable at this stage and, if addressed promptly, should not material into being an issue.
RED	Risk appetite is outside of acceptable tolerance. Successful delivery of the outcome appears to be unachievable. There are major risks or issues in a number of key areas. At this stage, these do not appear to be quickly manageable or resolvable. Urgent action is needed to ensure these are addressed and establish whether resolution is feasible. The outcome may need re-baselining and/or overall viability re-assessed.

Achievements – since Dec 2021

- ✓ Engagement of an information security partner with a full information security team now in place.
- ✓ Identity and access management (IAM) business case approved and programme of work initiated.
- ✓ Review and termination of dormant accounts (3,700) and admin rights (30) as part of IAM.
- ✓ Review of leavers' process as part of IAM.
- ✓ ITS business impact analysis completed and Business Continuity Plan approved.
- ✓ Disaster Recovery Planning initiated including the primary data centre restroration plan approved.
- ✓ Cyber essentials re-accreditation for a number of staff in the School of Economics and Finance secured.
- ✓ Re-launch of cyber security and GDPR online training. The tool has enhanced reporting and data visualisation capabilities. This also supports simulation of phishing exercises.
- ✓ Extension of the Security Operations Centre (SOC) and security information and event management solution (SIEM) to deliver additional security logging and near real-time alerting should indicators of compromise be identified.
- ✓ Critical information security vulnerabilities have been managed included high-profile widespread vulnerabilities (Log4J and Unix/Linux).
- ✓ Data matrix developed to support staff in understanding data classification policy and their application to individual data storage services. This has been endorsed by the Information Governance Group (IGG). Data matrix to be rolled-out to the University over the coming weeks.
- ✓ Review of the current crisis communications channels has been completed with tactical improvements agreed to enable rapid email and text services.
- ✓ Continued information security risks assessments and third party assurance thus minimising the introduction of new security risks to the university.
- ✓ Cyber desktop rehearsal completed with the ITS leadership and senior management team. This was externally facilitated with lessons learned shared. We will be implementing some improvements to the end-to-end cyber incident response plans as a result. A similar desktop exercise is planned with the Senior Executive Team (SET) to take place in late March 2022.
- ✓ Cyber insurance policy renewed with feedback from the Gallagher (brokers) Cyber Risk Management team (CyberAssist) concluding that "it was evident during our discussion with QM that they take the cyber-security of their organisation seriously and we have provided further explanation in this regard within this report. We believe that this client has a very strong cyber-security posture and therefore are a low risk for insurers in terms of a cyber-security threat."
- ✓ Delivery of fully managed Linux and Mac laptop builds – allowing for delivery of security patches and upgrades from central ITS.
- ✓ Replaced the legacy insecure Remote Desktop Service with a new secure service.
- ✓ Continue to work on the roll-out of managed devices across Faculties, including the research managed desktop service.

Overview Heat Map – Dec 2021

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?	2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?	3. Do we review user accounts and systems for unnecessary privileges on a regular basis	4.Do we enforce multi factor authentication for all systems and users?	5. Do we have tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?	6. How long will it take to recover critical business functions, assuming a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?
7. Can the business tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our business?	8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?	9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?	10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?	11. How would our organisation identify an attacker's presence on the network?	12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?
13.Are all staff aware of and participate in effective cyber risk management processes?	14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training, advice and guidance?	15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?	16. Do we adequately understand our business-critical services and functions and their associate data, technology and supply chain dependencies?		

Overview Heat Map - April 2022 – Reassessment

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?	2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?	3. Do we review user accounts and systems for unnecessary privileges on a regular basis	4.Do we enforce multi factor authentication for all systems and users?	5. Do we have tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?	6. How long will it take to recover critical business functions, assuming a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?
7. Can the business tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our business?	8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?	9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?	10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?	11. How would our organisation identify an attacker's presence on the network?	12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?
13.Are all staff aware of and participate in effective cyber risk management processes?	14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training, advice and guidance?	15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?	16. Do we adequately understand our business-critical services and functions and their associate data, technology and supply chain dependencies?		

Forecast Heat Map - Sept 2022 (at next ARC)

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?

2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?

3. Do we review user accounts and systems for unnecessary privileges on a regular basis

4.Do we enforce multi factor authentication for all systems and users?

5. Do we have tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?

6. How long will it take to recover critical business functions, assuming a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?

7. Can the business tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our business?

8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?

9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?

10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?

11. How would our organisation identify an attacker's presence on the network?

12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?

13.Are all staff aware of and participate in effective cyber risk management processes?

14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training, advice and guidance?

15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?

16. Do we adequately understand our business-critical services and functions and their associate data, technology and supply chain dependencies?

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Green

Current status:

- We have a data classification and storage scheme, needs more communications to raise awareness.
- This is underpinned by a "Data Matrix" with clear guidance on data classification and permitted data storage options. Worked closely with FMD
- Data Matrix completed and approved by CIO, IGG, and endorsed by PSLT.

Actions required to get to Green:

- Data classification policy needs further communicating and embedding.
- Data Matrix will be published / communicated more broadly to staff and students once approved – **Q3 (July) 2022.**
- QUIP are working to define the term Information Asset Owner (IAO), as one of a set of data related roles, and to identify IAO's across QM. Such work will be done in consultation with IGG **Q3 (July) 2022**. This work will help the individuals understand their responsibilities, but will not have an Information Asset Register by then.

Owner: ARC / IGG

2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- Disabling IT accounts immediately when HR staff on payroll leave QM.
- Departments who need to continue relationships with their staff are advised to set up alternative contracts (e.g. honorary) well in advance of formal end of colleague's permanent contract.
- Service Desk received a weekly report of staff leavers from HR systems which is processed immediately.
- Identity and Access Management (IAM) project approved at ITSB with recruitment underway for a delivery team.
- Review of inactive accounts and closure of dormant accounts completed as part of IAM programme with over 3,700 accounts closed.
- Mapping of the AS IS leavers process has been completed as part of the IAM programme with an understanding of how this process can be significantly enhanced to terminate accounts within 72 hours of staff leaving.

Actions required to get to green:

- Review of Joiners, Movers, Leavers (JML) policy as part of security policies and standards review **– Q4 2022.**
- Tactical design of an enhanced 'leavers process' as part of IAM programme **– Q3 2022.**
- Discovery and design component of Identity and Access Management (IAM) programme completed **– Q3 2022.**
- Strategic review of the joiner, leavers, and movers process as part of Identity and Access Management (IAM) programme **– Q2 2023.**

Owner: ITS / HR

3. Do we review user accounts and systems for unnecessary privileges on a regular basis?

Current RAG Status	Forecast RAG Status (Sept 2022)
Red	Amber

Current status:

- IT managed services admin accounts are now being reviewed on a regular basis. Further work is required to define the scope and implementation plan to deliver and embed this capability.
- Privileged Access Management included within scope of Identity and Access Management project and in security partner tender deliverables.
- Initial review and termination of 'IT domain admin accounts' has been completed with 28 privileged admin accounts and 2 service accounts removed.

Actions required to get to amber:

- Privileged users policy review required as part of security policies and standards review **– Q3 2022.**
- Strategic review and scoping of the 'AS I'S QM Privileged Access Management (PAM) including domain, application, and local device admin rights as part of IAM **– Q3 2022.**
- A further 44 'IT domain admin accounts' are being reviewed and rationalised as part of IAM – **Q3 2022.**

Actions required to get to green:

- Design and implementation of new Privileged Access Management (PAM) capabilities including people, process and technology as part of IAM programme – **Q4 2023.**
- Reviewing and addressing application level and local admin rights **– Q4 2023.**

Owner: ITS Security team

4. Do we enforce multifactor authentication for all systems and users?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- MFA rolled out in late 2020 to staff and students.
- There are about 17 accounts (May 2022) exempt from MFA, for a number of reasons. Work ongoing to reduce this further.
- We enforce MFA for major systems, more work to do on smaller ones. Email service still allows to use legacy authentication, without MFA. There are about 850 accounts using this method.
- MYSIS MFA pilot for a small number of users.

Actions required to get to green:

- Address MFA for remaining exempt accounts, or rationalise the reason for being exempt **– Q3 2022.**
- Definition and guidance of SSO / MFA for applications **– Q2 2022.**
- Address legacy authentication for email **– Q3 2022.**
- Review of legacy authentication / MFA solutions (e.g. Open LDAP and ID Check) and look to move to Azure AD **– Q3 2023.**
- Address Gold applications not yet under MFA e.g. Agresso or mitigate where SSO not possible **– Q4 2022.**

Owner: ITS

5. Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- ITS backup data to tape and between Data Centres for the managed estate. However, further assurance is required for "software as service" solutions as these are dependent on third parties.
- We cannot provide assurance for the self-managed or unmanaged estate.
- We haven't conducted a large scale test and restore for this service.

Actions required to get to green:

- Disaster recovery plans under development for gold services – **Q3 2022.**
- As part of 'Journey to the Cloud' programme:
  - Failover testing for gold infrastructure and applications – **Q4 2022.**
  - Large scale test and restore of back up for gold services – **Q2 2023.**
  - Review of backup arrangements– **Q3 2022.**
  - DC2 migration to Azure providing enhanced back-up services – **Q3 2022.**

Owner: ITS

6. How long will it take us to recover critical business functions, assuming a loss of all infrastructure? What's the business impact of a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- The Likelihood of all digital infrastructure being unavailable is low (hence Amber Rating), however in that scenario most if not all schools and faculties will be unable to operate, however teaching could be continued physically if there is no reliance on digital material.
- Disaster Recovery plans are under development for gold applications, and gold research and infrastructure services.
- Approved end-to-end restoration plan for Data Centre 1 (DC1).
- ITS Business Continuity Plan is approved by CIO.
- Other depts. in QM currently assessing their dependence on digital infrastructure through their BIAs
- BCM governance structure (Steering & Working Group) operational. Providing strategic and tactical oversight and direction and compliance against existing BC policy.
- Faculties / Directorates BIAs highlight large scale dependency on key IT systems. Workarounds currently limited.

Actions required to get to green:

- Development of disaster recovery plans for gold services – Q3 2022.
- Testing of above DR plans – Q4 2022.
- Testing of DC1 restoration plan – Q2 2023 (TBC).
- Develop DR plans for critical Silver Infrastructure - Q4 2022
- Completion of BIAs by QM schools and departments Q2 2022
- Completion of BCP plans by Faculties/ Directorates – Q3 2022.
- Exercising of Faculty/ Directorate BC Plans – Q4 2022.
- Develop a Crisis Management instruction including; crisis comms; standard operating procedures; roles & responsibilities – Q2 2022.
- QM crisis management exercise – Q4 2022.

Owner: ITS /Business Continuity Group under EAF

7. Can the business tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our business?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- Based on BIAs the university could not tolerate a recovery period lasting weeks or months.
- QM wide Business Continuity Plans (BCP) being developed through the Business Continuity Group with delivery plans identified and shared with SET.
- Crisis management framework developed where Gold crisis management team would be activated to respond to the lengthy recovery period.
- BCP Steering Group in place to ensure the Working Group develop BIAs and BCP for QM.

Actions required to get to green:

- Dependency on Gold Level Strategic planning (e.g. mutual support with other institutes in the higher education Sector).
- A rolling programme of BCP table top exercises being developed with first one planned for **Q2/Q3 2022**.
- Strategic planning crisis management exercise planned to take place in **Q4 2022.**

Owner: Business Continuity Group under EAF

8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- Cyber Incident exercise delivered in Feb 2022 for the ITS Leadership Team and for SET in March 2022.
- An end-to-end cyber incident response plan under development.
- Engagement with the business continuity team and programme to manage inter-dependencies.
- Crisis management communications plan and channels in place.

Actions required to get to green:

- Finalise and sign off end to end cyber incident response process – **Q2 2022.**
- Plan and start to execute a series of ITS cyber exercises based on scenarios in above process – **Q3/Q4 2022.**
- Business continuity desktop exercise being managed through Business Continuity Group with first one planned for **Q2 2022** and a crisis management exercise **in Q4 2022.**

Owner: ITS / Business Continuity

9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?

Current RAG Status	Forecast RAG Status (Sept 2022)
Red	Red

Current status:

- 11,000 Critical and high vulnerabilities identified in the managed estate. We can only state "no assurance" for the unmanaged and self-managed estates within schools and faculties. Third party application patching project being tested.
- Addressing vulnerabilities for EECS (8 remediated from 11 identified) and Maths servers (to be remediated).
- Managed Research Desktop Service being developed to allow managed devices with freedom to research with limited risks.
- PatchMyPC has been rolled out on the managed Windows desktop estate to manage the updating of 3rd party applications like Chrome, Firefox, Adobe Reader, etc.
- Well rehearsed process for managing vulnerability alerts and advisory notes from external parties including JISC and NCSC.

Actions required to get to Amber

- Rollout of managed Mac / Linux laptop service **– ongoing.**
- Upgrade of Active Directory – **Q3 2022.**
- Managed Service rollout - SBCS & SPA completed; IOD / Blizzard **– Q4 2022.**
- Managed Service rollout - **SEF & EECS - TBC**
- Transfer of management of **SEF security patching and application management** from **Donald WU (SEF) to ITS - TBC**
- Removal of all insecure remote access systems other than ITS's remote desktop service (RDS) **- TBD**
- Managed Research Desktop Service – pilot starting **– Q3 2022.**
- External vulnerability scans to identify vulnerable internet facing machines – ongoing with service fully operational as part of security plan **– Q4 2022**.
- High priority placed on replacing obsolete hardware and software **– ongoing.**
- Structured documentation of as-is application architecture, highlighting any **technical debt** requiring to be addressed **– Q3 2022.**

Actions required to get to green:

- Implementation of key projects within ITS Capital Plan including asset management; IT service management tool; security programme; managed service rollout **– Q4 2024.**

Owner: ITS / Schools and Faculties

10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?

Inherent RAG Status	Forecast RAG Status (Sept 2022)
Green	Green

Current status:

- Yes, our network is segmented into ‘security domains’ that separate devices with different security requirements from each other. This ensures that if an attacker gets access to one device they will have limited access to more sensitive services / data.

Maintenance actions required:

- Internal pen test to ensure effectiveness of segmentation – **Q4 2022**.
- Architectural standards to ensure segmentation remains effective – **Q4 2022**.
- Further micro-segmentation in data centres to enhance this capability – **Q3 2022**.

Owner: ITS

11. How would our organization identify an attacker's presence on the network?

Inherent RAG Status	Forecast RAG Status (Sept 2022)
Red	Red

Current status:

- We have implemented a Security Operations Centre (SOC) and Security Incident and Event Management (SIEM) including log-ins from inside and outside the University. Further work required to extend the scope of the service.
- We have Cisco Umbrella which provides a certain level of intrusion detection and prevention.
- Low confidence in our ability to detect a stealth infiltration on our network pre-attack, but we do have a 24/7 security operation centre (SOC / SIEM) in place.

Actions required to get to amber:

- Install honeypots – a dummy server that appears to be legitimate but has no real data and is watched carefully **– Q4 2022.**
- Phase 2 of SIEM tool "Alien Vault" log collection and analysis **– Q4 2022.**
- Implementation of improved IDS / IPS through the Core Network Replacement project **– Q3 2022.**
- Knowledge share session with sector colleagues with good practice i.e. UCAS **– Q3 2022.**

Actions required to get to green:

- Longer term action plan to be covered as part of the development of the security strategy and roadmap **– Q3/Q4 2022.**

Owner: ITS

12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Amber

Current status:

- We report information security risks at an institute level and ITS level including to SET and the Audit and Risk Committee.
- In the past the 6 months the security function evaluated and developed a security risk management and third party assurance process which is live at present. A security team is now in place to manage this process but further work and capacity is required to ensure these risks are being owned and mitigated at the right level.
- In addition to the ITS strategic risk register, which is reviewed on a quarterly basis, a security risk register has been created and is managed through the security team.

Actions required to get to green:

In conjunction with SPO/ARCS:

- CIO communication to all staff on risk management good practice, and completion of cyber security and GDPR training **– Q2 2022.**
- Governance process to be reviewed and implemented as part of security partnership contract **– Q3 2022.**
- Review of security standards / policies to be covered as part of the development of the security strategy and roadmap **– Q3 2022.**

Owner: ITS / SPO/ ARCS

13. Are all staff aware of and participate in effective cyber risk management processes?

Inherent RAG Status	Forecast RAG Status (Sept 2022)
Red	Red

Current status:

- Although information security risk assessment and third party assurances processes have been developed and implemented within ITS, we haven't communicated this widely and staff are not trained on specific cyber risk management processes with the exception of the Cyber Security and GDPR training.

Actions required to get to amber:

- ITS "design principles" and "service introduction process" being presented to PSLT and SET **– Q2 2022.**
- Review fitness of risk management tools and the extent to which they embed cyber risk management processes **– Q4 2022.**
- Communications, engagement and training on cyber risk management processes to staff and students – **Q4 2022.**
- Cyber risk management processes need embedding in project management and service delivery processes. These need to become a part of day-to-day functional delivery **– Q4 2022.**
- Training for Service Desk staff in line with the Cyber Incident Response Plan **– Q3 2022.**

Actions required to get to green:

- Longer terms action plan to be covered as part of the development of the security strategy and roadmap – **Q2 2022.**
- Specific cyber risks management e-learning module as part of Metacompliance offering **– Q4 2022.**

Owner: ITS / SPO

14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training advice and guidance?

Inherent RAG Status	Forecast RAG Status (Sept 2022)
Amber	Green

Current status:

- Cyber security and GDPR training rolled-out to staff and students in 2020. Completion rates are 42% for GDPR and 43% for Cyber Security (May 2022).
- New Power BI cyber security and GDPR training reporting dashboard completed and released to all managers with QM with clear visibility of staff who have or have not completed the training.
- The security team provide security advice through the review of risks and third party assurance for specific requests, initiatives and projects. SharePoint site is used to manage requests.
- An annual cyber security awareness plan has been developed with intention to have a focussed awareness raising event regularly.

Actions required to get to green:

- Target completion rates to be agreed with PSLT – **Q2 2022.**
- Phishing simulation exercise to be undertaken – **Q2 2022.**
- Additional modules on MetaCompliance portal on a termly basis for both students and staff – **Q3 / Q4 2022.**
- Liaise with Schools / Faculties and Research Ethics on targeted training and awareness to compliment the e-learning modules on MetaCompliance – **Q4 2022.**

Owner: ITS / PSLT

15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?

Current RAG Status	Forecast RAG Status (Sept 2022)
Amber	Green

Current status:

- SCCM is capturing all our managed estate software / hardware.
- All IT equipment purchased through the IT Service Catalogue is asset tagged and included in the CMDB.
- Two ITS projects on software and hardware licence and asset management are underway. This has provided a record of ITS managed devices, but it currently there is no clear record of assets within the unmanaged estate.

Actions required to get to green:

- The campaign to capture un-managed data (using Lansweeper) is underway and target to complete **– Q2 2022.**
- The Asset Management project is undertaking an asset reconciliation exercise aimed at making the CMDB records more accurate **– Q3 2022.**
- Software and hardware asset management capabilities under review including the need for potential integrated solutions for capturing the data **– Q3 2022.**
- Asset management also being captured as part of the Managed Desktop roll-out project – **Ongoing**.
- Structured documentation of as-is application architecture, will create definitive inventory of application assets **– Q3 2022.**
- Managed Service rollout - SBCS & SPA completed; SEF & EECS (TBC); IOD / Blizzard **– Q4 2022.**
- ITS Service Monitoring project to define and map Gold services into smaller granular pieces – **Q2 2022**.

Owner: ITS

16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?

Current RAG Status	Forecast RAG Status (Sept 2022)
Red	Red

Narrative:

Current status:

- We have defined our business-critical services through an ITS Service Portfolio with definition of gold, silver, and bronze service levels but need more work on dependencies.

Actions required to get to Amber:

- Creation of a Service Management Office with ITS following appointment of Head of Service Management – **Q2 2022**.
- Creation of an ITS Service Governance Board to regularly review the service portfolio and introduction of new services – **Q3 2022**.
- Structured documentation of as-is **application architecture**, will set out the technology components underpinning each application – **Q3 2022**.
- ITS Service Monitoring project to define and map Gold services into smaller granular pieces, agreed with team – **Q2 2022**.

Actions required to get to Green:

- Mapping of the AS-IS technology estate and dependencies through the newly established enterprise architecture function – **Q2 2023**.

Owner: ITS

Next Steps

- Present update to Audit & Risk Committee meetings in June and Sept 2022.


Do you have any questions?

Thank you

Queen Mary
University of London