

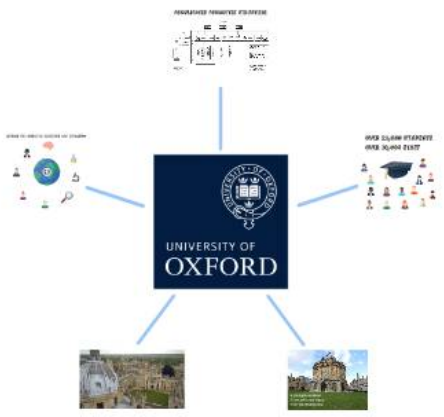
INFORMATION SECURITY CHALLENGES?



IMPROVING INFORMATION SECURITY



HOW TO SECURE A COLLEGIATE UNIVERSITY



RISK MANAGEMENT

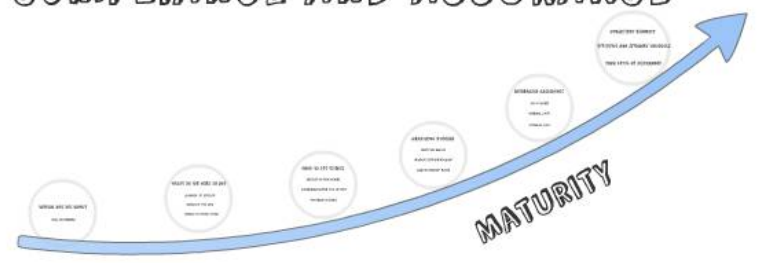


QUESTIONS

TOOLING



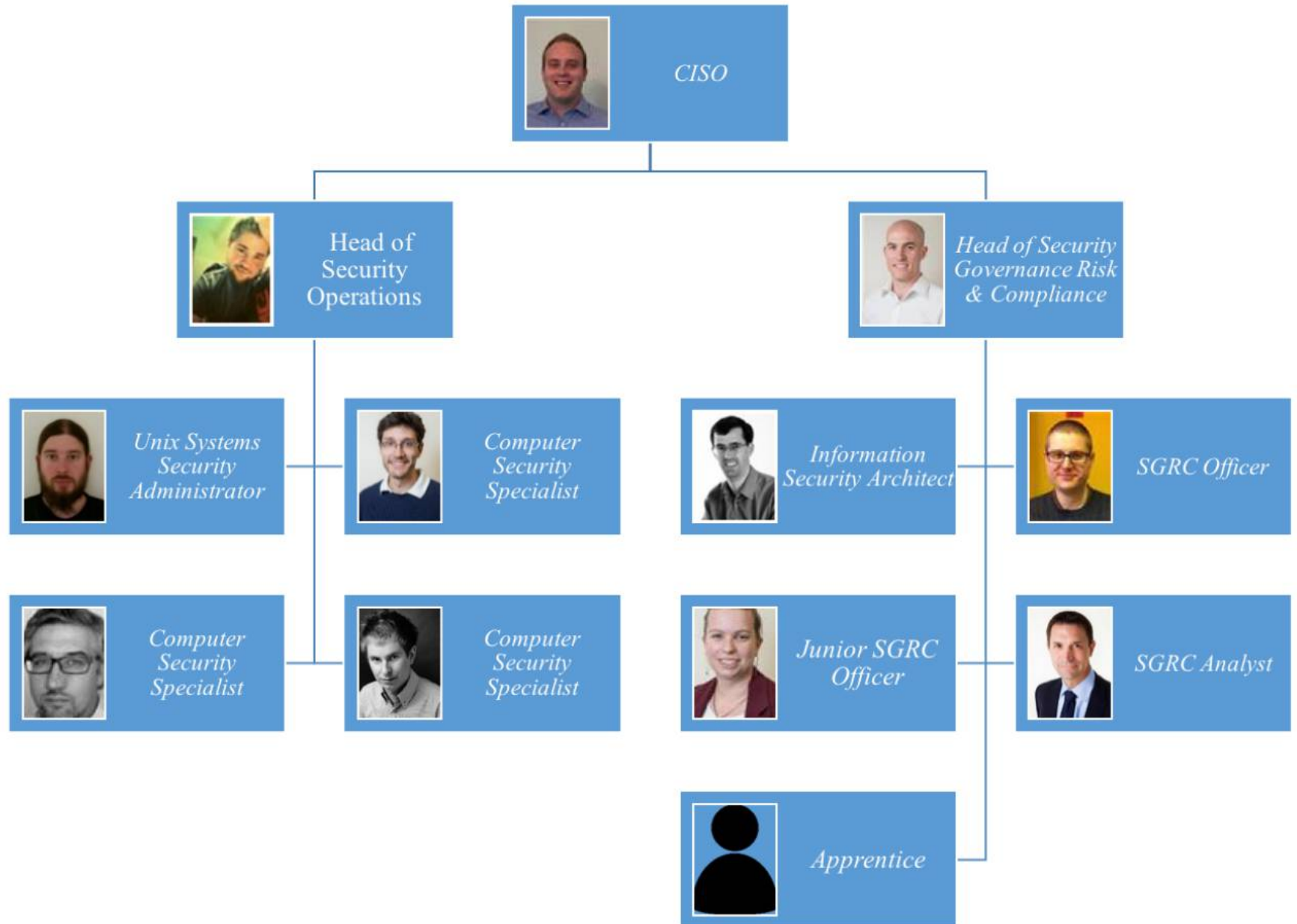
COMPLIANCE AND ASSURANCE



HOW TO SECURE A COLLEGIATE UNIVERSITY



INFORMATION SECURITY TEAM



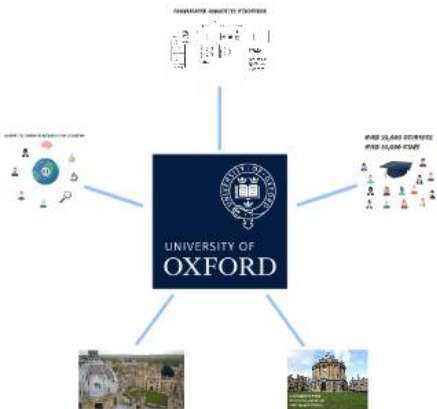
INFORMATION SECURITY CHALLENGES?



IMPROVING INFORMATION SECURITY



HOW TO SECURE A COLLEGIATE UNIVERSITY



RISK MANAGEMENT

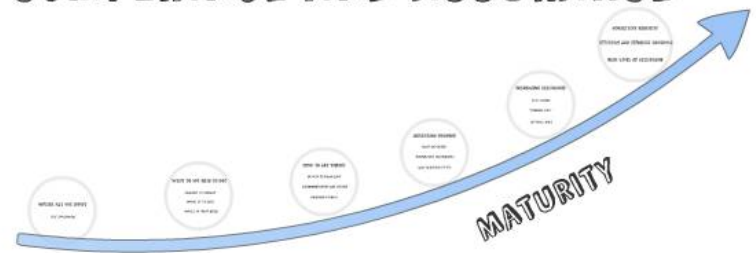


QUESTIONS

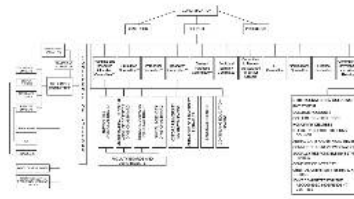
TOOLING



COMPLIANCE AND ASSURANCE



COMPLICATED COMMITTEE STRUCTURE



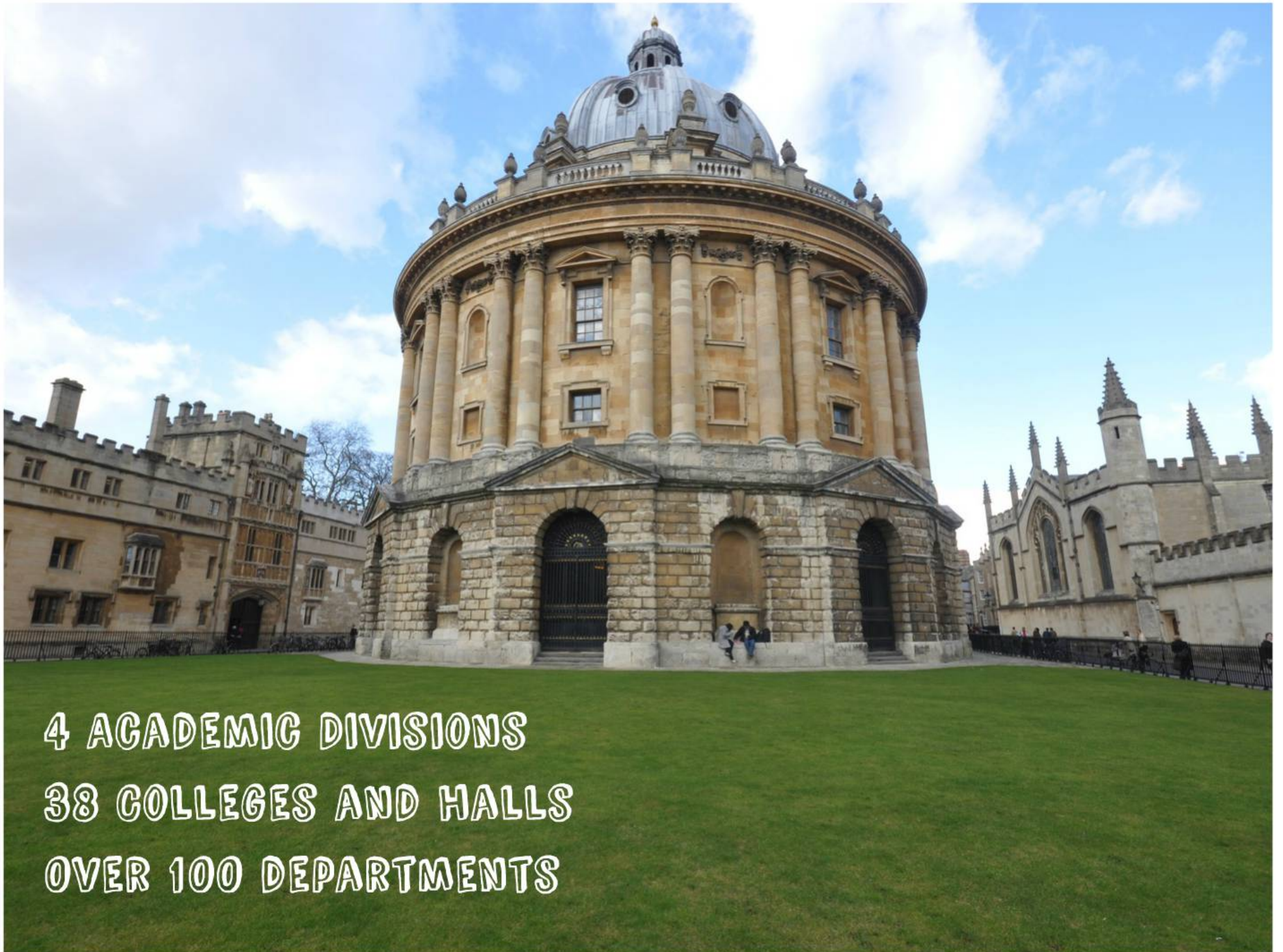
LEADING THE WORLD IN RESEARCH AND EDUCATION



**OVER 22,000 STUDENTS
OVER 10,000 STAFF**





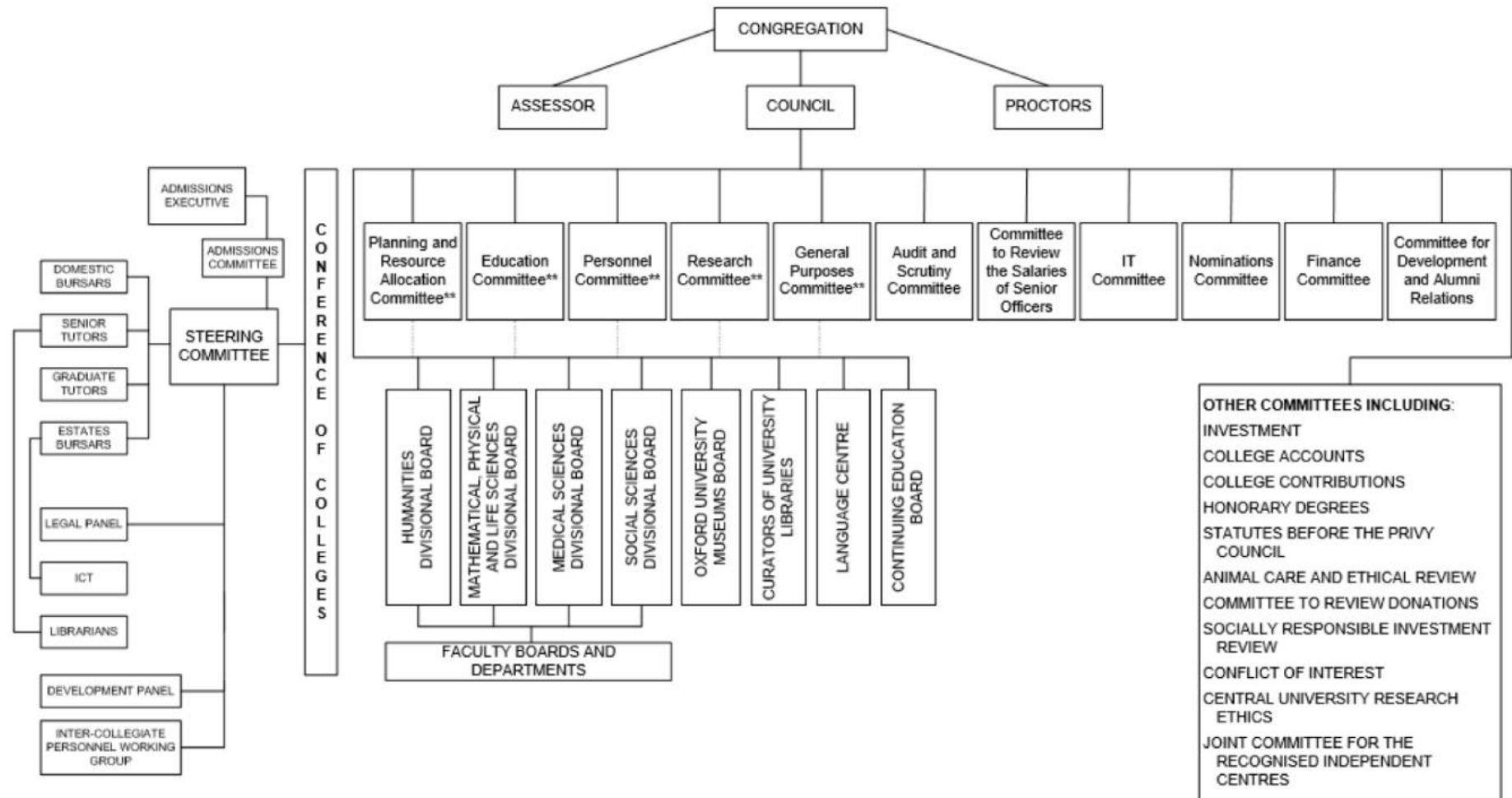


4 ACADEMIC DIVISIONS
38 COLLEGES AND HALLS
OVER 100 DEPARTMENTS

OVER 22,000 STUDENTS
OVER 10,000 STAFF



COMPLICATED COMMITTEE STRUCTURE



LEADING THE WORLD IN RESEARCH AND EDUCATION



INFORMATION SECURITY CHALLENGES?

CHALLENGING LANDSCAPE



REAL THREATS



REAL INCIDENTS



HEADLINE NEWS



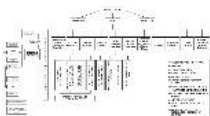
INDUSTRIAL REQUIREMENTS



WALKING A FINE LINE



COMPLICATED ORGANISATIONAL STRUCTURE



HOW TO SECURE A COLLEGE

CHALLENGING LANDSCAPE



REAL THREATS



REAL INCIDENTS



HEADLINE NEWS

Oxford University college sorry for rejection email errors

🕒 14 January 2017 | UK

🔗 Share



The rejection emails may have elicited more sighs than usual

An Oxford University college has apologised after sending rejected potential undergraduates details of all their fellow unsuccessful applicants.

Hertford College sent out rejection emails, but included copies of letters with the names, addresses and subjects of all the failed candidates.

VARYING REQUIREMENTS



CYBER
ESSENTIALS

WALKING A FINE LINE



IMPROVING INFORMATION SECURITY

IDENTIFYING CROWN JEWELS



INFORMATION SECURITY TEAM



DEVELOPING RESILIENCE AND CAPACITY



PROVIDING DIRECTION AND SUPPORT



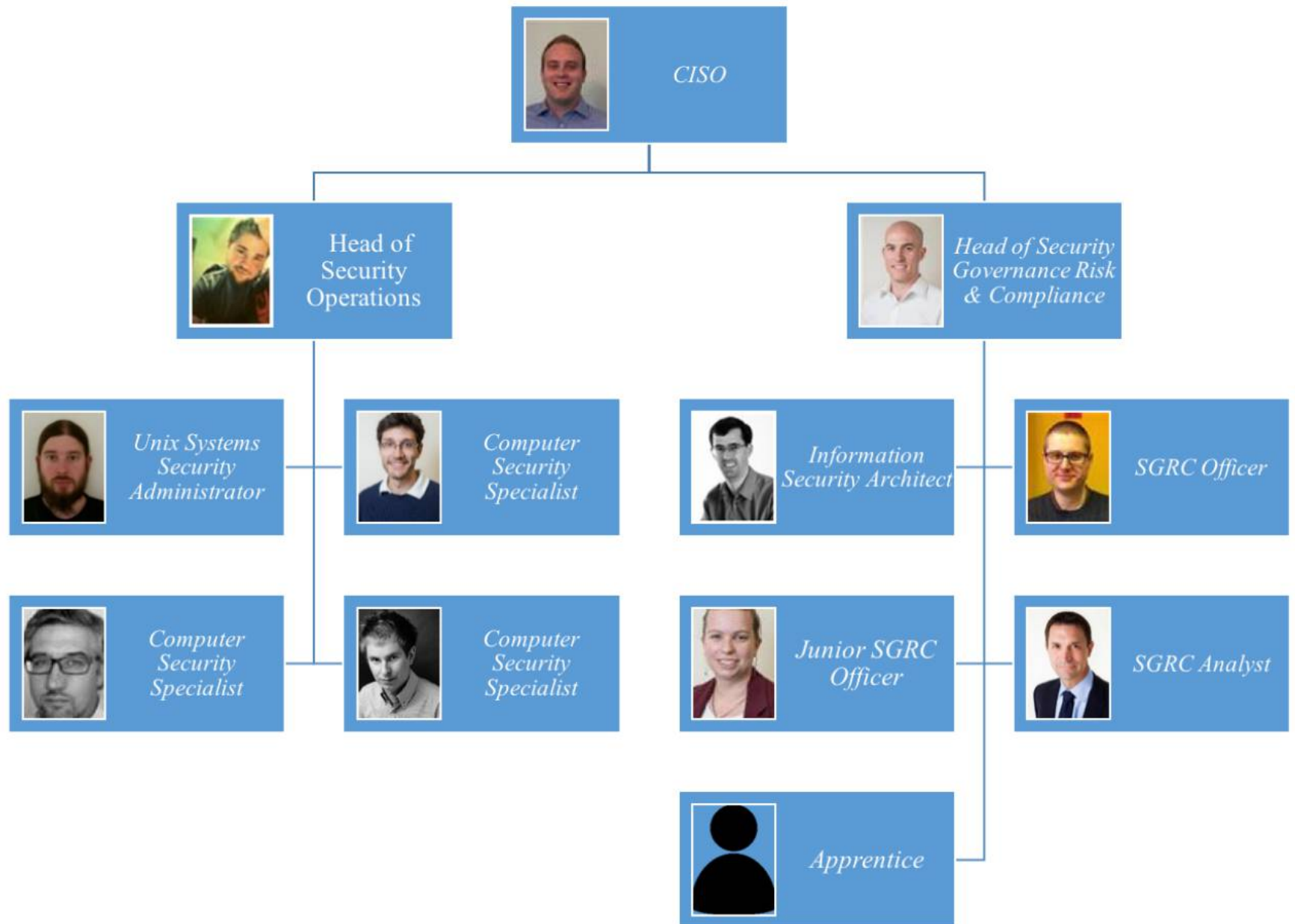
CREATING CONFIDENCE



IDENTIFYING CROWN JEWELS



INFORMATION SECURITY TEAM



DEVELOPING CAPABILITY AND CAPACITY



PROVIDING DIRECTION AND SUPPORT



CREATING CONFIDENCE



RISK MANAGEMENT

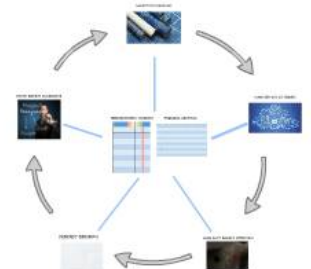
OLD APPROACH



FOCUS ON ACTION



BASELINE SECURITY CONTROLS



OLD APPROACH



FOCUS ON ACTION

The screenshot displays the Information Security website interface. At the top, there is a dark blue header with the 'Information Security' logo on the left, a search bar, and links for 'Report an Incident' and 'Contact Us'. Below the header is a navigation bar with 'GUIDANCE & POLICY' selected. The main content area features a breadcrumb trail: 'Home / Guidance & Policy / Working with Third Parties'. On the left, a sidebar lists various security topics, with 'Working with Third Parties' highlighted. The main heading is 'Working with Third Parties'. Below this, a text box explains the importance of third-party security. A sub-navigation bar includes 'Policy', 'Requirements' (which is active), and 'How to Comply'. The 'Requirements' section contains a list of four numbered points. To the right, there are three colored boxes: 'Tools & Resources' (green) with links to download various documents, 'Services' (orange) with a link to 'Third party information security', and 'Further Information' (blue) with links to 'ICO cloud computing guidance' and 'JISC cloud computing guidance'.

Information Security

Search

Report an Incident

Contact Us

GUIDANCE & POLICY | I WANT TO... | SERVICES | WHAT WE DO

Home / Guidance & Policy / Working with Third Parties

Management of Information Security

Working with Third Parties

Compliance

Training and Awareness

IT Security

Information Asset Management

Risk Management

Incident Management

Physical and Environmental

Working with Third Parties

A safe pair of hands or the weakest link? Before you entrust sensitive information to any partner or supplier, you need to be sure they can and will keep it safe from attack.

As a Head of Division, Head of Department or Faculty Board Chair, you have a responsibility to ensure third-parties who deal with University data don't expose the University and your division, department or faculty to unnecessary information security risks.

Policy | **Requirements** | How to Comply

In order to ensure that third-party partners and suppliers meet the standards of information security required by the University and your division, department or faculty, you must:

1. maintain an up-to-date record of all third parties that access, store or process University information on behalf of your division, department or faculty
2. ensure that, for all new agreements with third parties, due diligence is exercised around information security and that contractual arrangements are adequate
3. ensure that information security arrangements contained in existing agreements are reviewed and are adequate
4. monitor the compliance of third parties against your information security requirements and contractual arrangements

Tools & Resources

- Download Third Party Security Assessment (TPSA)
- Download TPSA Guidance Notes
- Download cloud security guidance
- Download cloud security checklist
- Download cloud information security considerations
- Download inventory template

Services

- Third party information security

Further Information

- Download ICO cloud computing guidance
- JISC cloud computing guidance



Policy



Requirements



How to Comply

In order to ensure that third-party partners and suppliers meet the standards of information security required by the University and your division, department or faculty, you must:

1. maintain an up-to-date record of all third parties that access, store or process University information on behalf of your division, department or faculty
2. ensure that, for all new agreements with third parties, due diligence is exercised around information security and that contractual arrangements are adequate
3. ensure that information security arrangements contained in existing agreements are reviewed and are adequate
4. monitor the compliance of third parties against your information security requirements and contractual arrangements



Tools & Resources

[Download Third Party Security Assessment \(TPSA\)](#)

[Download TPSA Guidance Notes](#)

[Download cloud security guidance](#)

[Download cloud security checklist](#)

[Download cloud information security considerations](#)

[Download inventory template](#)

Services

[Third party information security](#)

Further Information

[Download ICO cloud computing guidance](#)

[JISC cloud computing guidance](#)

BASELINE SECURITY CONTROLS



ARCHITECTURE PRINCIPLES



CLOUD SECURITY ASSESSMENT



TECHNICAL CONTROLS

ORGANISATIONAL CONTROLS

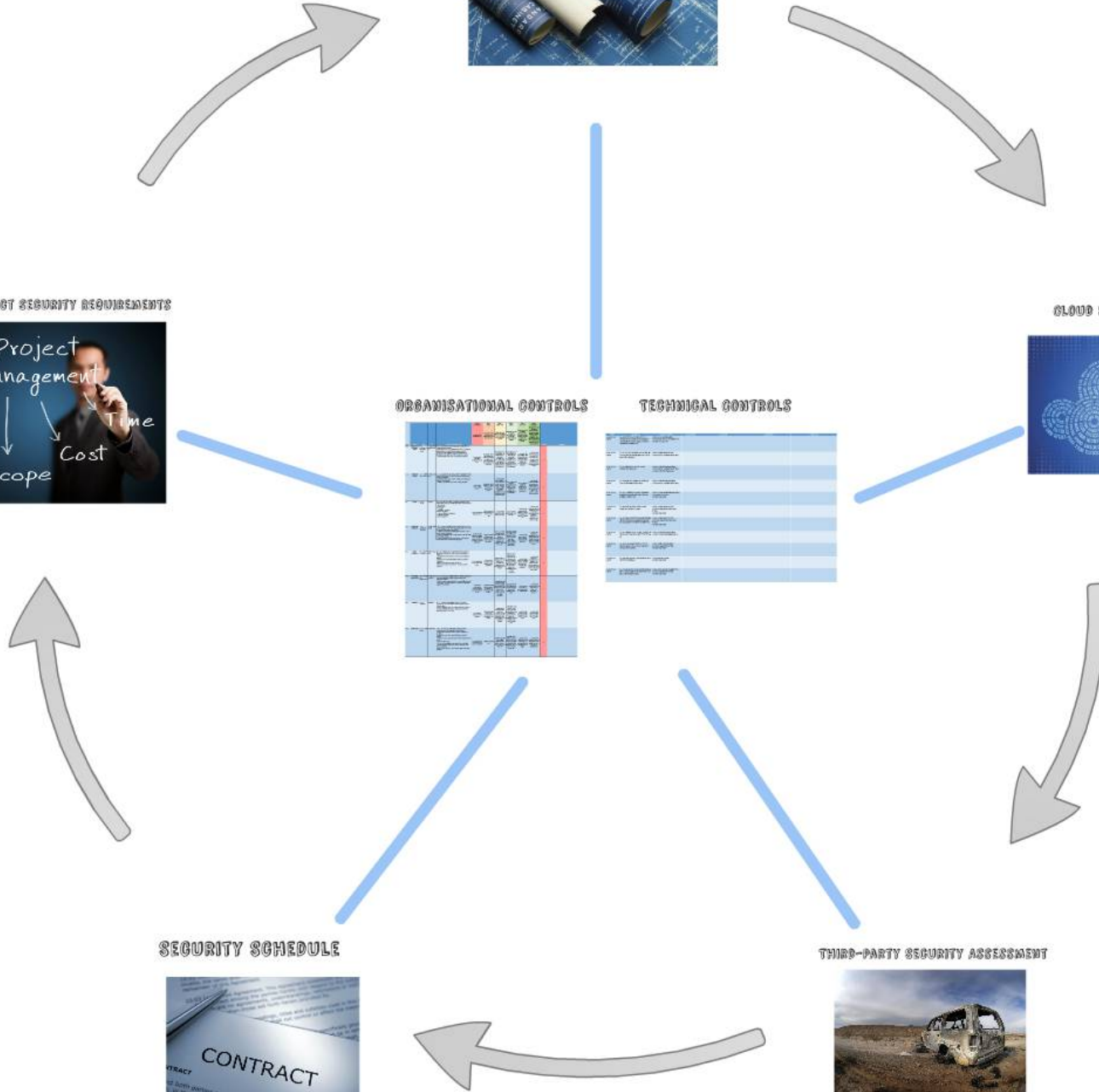
PROJECT SECURITY REQUIREMENTS



THIRD-PARTY SECURITY ASSESSMENT



SECURITY SCHEDULE



ANISATIONAL CONTR

			LEVEL 0 NON-EXISTANT	LEVEL 1 INITIAL	LEVEL 2 REPEATABLE	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISED		
	Tags	DESCRIPTION OF REQUIREMENTS	No controls in the description exist	Some of the controls exist but are not applied consistently across the unit	All controls are in place to some degree but are not all applied consistently across the unit	All controls exist and are applied consistently across the unit but assurance of controls is ad-hoc	All controls exist and are applied consistently across the unit; assurance activities take place to confirm the effectiveness of controls	All controls exist and are applied consistently across the unit; assurance activities take place to confirm the effectiveness of all controls and evidence exists to demonstrate improvements from lessons learned	UNIT LEVEL	
Management of Information Security	ManagementOfInformationSecurity	MIS.01 Assign overall ownership of information security within your division, department or faculty: - Define and document any specific information security, regulatory or legal requirements for your division, department or faculty; - Identify and assign specific roles and responsibilities related to Information Security within your division, department or faculty; - Embed Information Security into your management framework.	No management ownership of information security exists.	Information security responsibilities are included in some job descriptions and issues are considered by management on an ad-hoc basis.	Information security responsibilities are included in most relevant job descriptions and issues are considered by management regularly. Regulatory requirements have been articulated.	Information security responsibilities are included in all relevant job descriptions and security issues are considered by management termly. All requirements have been articulated.	As at Level 3, with responsibilities within job descriptions and information security requirements being reviewed by management on an annual basis.	As at Level 4, with evidence that output from reviews has been acted upon. Assurance over the effectiveness of controls is provided through independent review.	0	
Training and Awareness	TrainingAndAwareness	TAA.01 Arrange and annually repeat a compulsory information security awareness training to ensure staff fully understand their Information Security responsibilities: - Include information security awareness training as an integral part of the process for new joiners; - Maintain up-to-date records of awareness training completion.	No information security training exists.	Information security training exists but it is not part of the process for new starters.	Some information security training exists and is part of the process for new joiners. Refresher training is available and completion records are maintained but not all staff regularly receive equivalent training.	All new staff complete equivalent information security training. There is annual refresher training and completion records are maintained.	As level 3, with staff periodically completing and passing a test to monitor their understanding.	As level 4, with additional activities to test awareness (e.g. phishing campaigns). Training offerings are adjusted based on the responses to awareness activities and current threats.	0	

S

TECHNICAL CONTROLS

TITLE	DESCRIPTION	EXPECTED TESTING	IMPLEMENTED	COMMENTS	CONSTRAINTS	MITIGATION
ACC.01 Access Control	ACC.01 Restrict access to all systems to authorised users and admins for appropriate and authorised activities only. In accordance with business requirements.	<ul style="list-style-type: none"> - Review access control policies - Examine roles and access requirements - Interview management 				
ACC.02 Access Control	ACC.02 Set access control systems to 'deny-all' access by default and only allow access that is specifically authorised.	<ul style="list-style-type: none"> - Review vendor documentation - Examine system configuration settings 				
ACC.03 Access Control	ACC.03 Authenticate access via secure authentication protocols.	<ul style="list-style-type: none"> - Review authentication procedures - Examine system configuration settings - Observe authentication process 				
ACC.04 Access Control	ACC.04 Ensure that sessions are terminated after a defined period of inactivity.	<ul style="list-style-type: none"> - Review authentication procedures - Examine system configuration settings 				
ACC.05 Access Control	ACC.05 Use individual accounts with unique identifiers for the identification of all users, including administrators.	<ul style="list-style-type: none"> - Review account provisioning procedures - Examine list of accounts - Interview personnel 				
ACC.06 Access Control	ACC.06 Disable or delete default vendor, anonymous and guest accounts.	<ul style="list-style-type: none"> - Review vendor documentation - Examine configuration and account settings - Interview personnel 				
ACC.07 Access Control	ACC.07 Change all default passwords, including administrator or root passwords, and ensure new passwords meet minimum requirements.	<ul style="list-style-type: none"> - Review vendor documentation - Examine configuration and account settings - Interview personnel 				
ACC.08 Access Control	ACC.08 Configure system settings to enforce the change or creation of passwords at the first log-on.	<ul style="list-style-type: none"> - Review authentication procedures - Observe account provisioning process 				
ACC.09 Access Control	ACC.09 Use passwords which are at least 12 characters long OR have at least equivalent strength and complexity.	<ul style="list-style-type: none"> - Review policies and procedures - Examine configuration settings - Interview personnel 				
ACC.10 Access Control	ACC.10 Document users with authorised system administrator privileges.	<ul style="list-style-type: none"> - Examine documentation - Interview personnel 				
ACC.11 Access Control	ACC.11 Manage all access via security groups or roles to ensure alignment between their access rights and their job functions.	<ul style="list-style-type: none"> - Review roles and access requirements - Examine configuration settings - Interview personnel 				

TECHNICAL CON

TITLE	DESCRIPTION	EXPECTED TESTING	IMPLEMENTED	COMMENTS
ACC.01 Access Control	ACC.01 Restrict access to all systems to authorised users and admins for appropriate and authorised activities only, in accordance with business requirements.	<ul style="list-style-type: none">- Review access control policies- Examine roles and access requirements- Interview management		
ACC.02 Access Control	ACC.02 Set access control systems to 'deny-all' access by default and only allow access that is specifically authorised.	<ul style="list-style-type: none">- Review vendor documentation- Examine system configuration settings		
ACC.03 Access Control	ACC.03 Authenticate access via secure authentication protocols.	<ul style="list-style-type: none">- Review authentication procedures- Examine system configuration settings- Observe authentication process		
ACC.04 Access Control	ACC.04 Ensure that sessions are terminated after a defined period of inactivity.	<ul style="list-style-type: none">- Review authentication procedures- Examine system configuration settings		
ACC.05 Access Control	ACC.05 Use individual accounts with unique identifiers for the identification of all users, including administrators.	<ul style="list-style-type: none">- Review account provisioning procedures- Examine list of accounts- Interview personnel		

PROJECT SECURITY REQUIREMENTS



ARCHITECTURE PRINCIPLES



CLOUD SECURITY ASSESSMENT



THIRD-PARTY SECURITY ASSESSMENT



SECURITY SCHEDULE



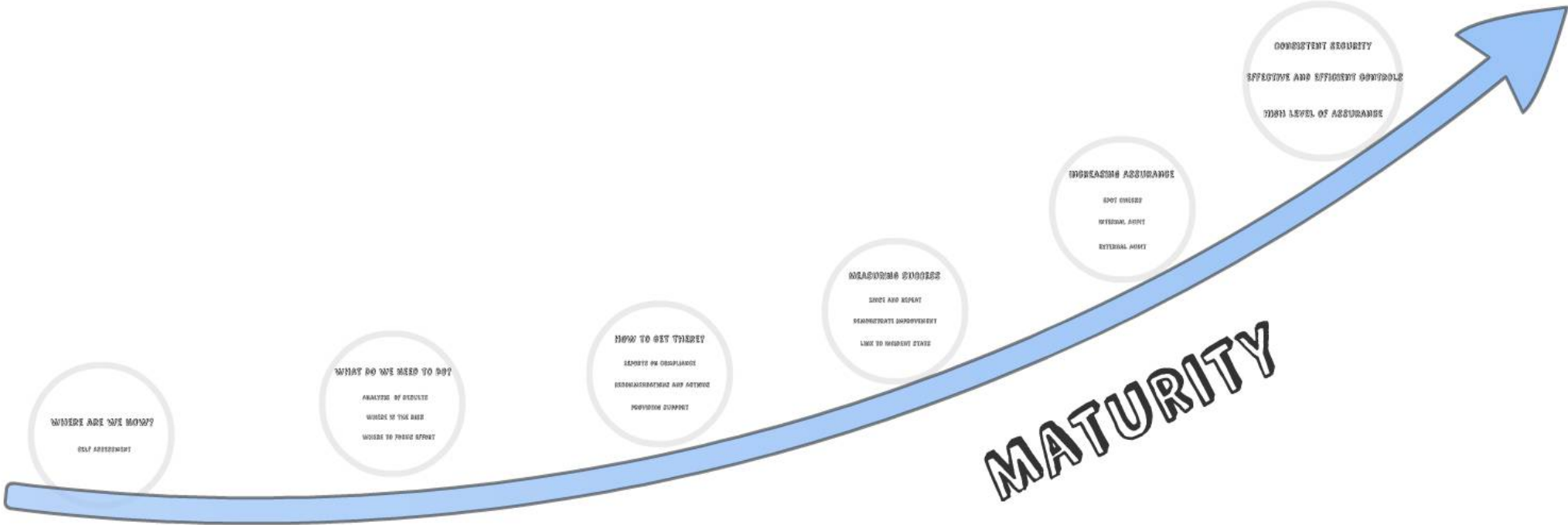
ORGANISATIONAL CONTROLS

Control ID	Control Name	Control Description	Control Type	Control Category	Control Status	Control Owner	Control Review Date	Control Effectiveness
AC101	AC101 - Board Governance	The Board of Directors is responsible for the overall governance of the organization, including the approval of the strategic plan, the appointment and oversight of senior management, and the monitoring of the organization's performance.	Organizational	Board Governance	Active	Board of Directors	Annual	Effective
AC102	AC102 - Executive Management	Senior management is responsible for the day-to-day operations of the organization, including the implementation of the strategic plan, the management of resources, and the oversight of the organization's performance.	Organizational	Executive Management	Active	Senior Management	Annual	Effective
AC103	AC103 - Internal Control Framework	The organization has established a comprehensive internal control framework that covers all aspects of its operations, including financial reporting, risk management, and compliance.	Organizational	Internal Control	Active	Internal Control	Annual	Effective
AC104	AC104 - Risk Management	The organization has established a risk management framework that identifies, assesses, and mitigates the organization's risks, including financial, operational, and reputational risks.	Organizational	Risk Management	Active	Risk Management	Annual	Effective
AC105	AC105 - Compliance	The organization has established a compliance framework that ensures the organization is compliant with all applicable laws, regulations, and industry standards.	Organizational	Compliance	Active	Compliance	Annual	Effective
AC106	AC106 - Human Resources	The organization has established a human resources framework that covers all aspects of its workforce, including recruitment, compensation, and performance management.	Organizational	Human Resources	Active	Human Resources	Annual	Effective
AC107	AC107 - Information Security	The organization has established an information security framework that protects the organization's information assets from unauthorized access, disclosure, and destruction.	Organizational	Information Security	Active	Information Security	Annual	Effective
AC108	AC108 - Environmental and Social Governance	The organization has established an environmental and social governance framework that addresses the organization's environmental and social impacts, including climate change, human rights, and community relations.	Organizational	ESG	Active	ESG	Annual	Effective

TECHNICAL CONTROLS

Control ID	Control Name	Control Description	Control Type	Control Category	Control Status	Control Owner	Control Review Date	Control Effectiveness
AC201	AC201 - Access Control	Access to information systems is restricted to authorized users, and access is granted based on the user's role and responsibilities.	Technical	Access Control	Active	IT Security	Annual	Effective
AC202	AC202 - Data Encryption	Sensitive data is encrypted both at rest and in transit, ensuring that the data is protected from unauthorized access.	Technical	Data Encryption	Active	IT Security	Annual	Effective
AC203	AC203 - Patch Management	Information systems are regularly updated with security patches to address known vulnerabilities and prevent the exploitation of weaknesses.	Technical	Patch Management	Active	IT Security	Annual	Effective
AC204	AC204 - Incident Response	The organization has established an incident response plan that outlines the procedures for identifying, investigating, and resolving security incidents.	Technical	Incident Response	Active	IT Security	Annual	Effective
AC205	AC205 - Business Continuity	The organization has established a business continuity plan that ensures the organization can continue to operate in the event of a disaster or other major disruption.	Technical	Business Continuity	Active	IT Security	Annual	Effective
AC206	AC206 - Network Security	The organization's network is protected from unauthorized access and attacks through the use of firewalls, intrusion detection systems, and other security measures.	Technical	Network Security	Active	IT Security	Annual	Effective
AC207	AC207 - System Monitoring	Information systems are monitored for suspicious activity and security events, allowing the organization to detect and respond to threats in real-time.	Technical	System Monitoring	Active	IT Security	Annual	Effective
AC208	AC208 - Data Backup and Recovery	Information systems are regularly backed up, and the organization has a robust disaster recovery plan in place to restore data in the event of a loss.	Technical	Data Backup and Recovery	Active	IT Security	Annual	Effective
AC209	AC209 - Security Awareness	The organization provides regular security awareness training to all employees, ensuring that they are equipped with the knowledge and skills to recognize and prevent security threats.	Technical	Security Awareness	Active	IT Security	Annual	Effective
AC210	AC210 - Vendor Risk Management	The organization has established a vendor risk management framework that assesses and mitigates the risks associated with third-party vendors and suppliers.	Technical	Vendor Risk Management	Active	IT Security	Annual	Effective

COMPLIANCE AND ASSURANCE



MATURITY



CONSISTENT SECURITY

EFFECTIVE AND EFFICIENT CONTROLS

HIGH LEVEL OF ASSURANCE



WHERE ARE WE NOW?

SELF ASSESSMENT





WHAT DO WE NEED TO DO?

ANALYSIS OF RESULTS

WHERE IS THE RISK

WHERE TO FOCUS EFFORT

HOW TO GET THERE?

REPORTS ON COMPLIANCE

RECOMMENDATIONS AND ACTIONS

PROVIDING SUPPORT

MEASURING SUCCESS

RINSE AND REPEAT

DEMONSTRATE IMPROVEMENT

[LINK TO INCIDENT STATS](#)

INCREASING ASSURANCE

SPOT CHECKS

INTERNAL AUDIT

EXTERNAL AUDIT

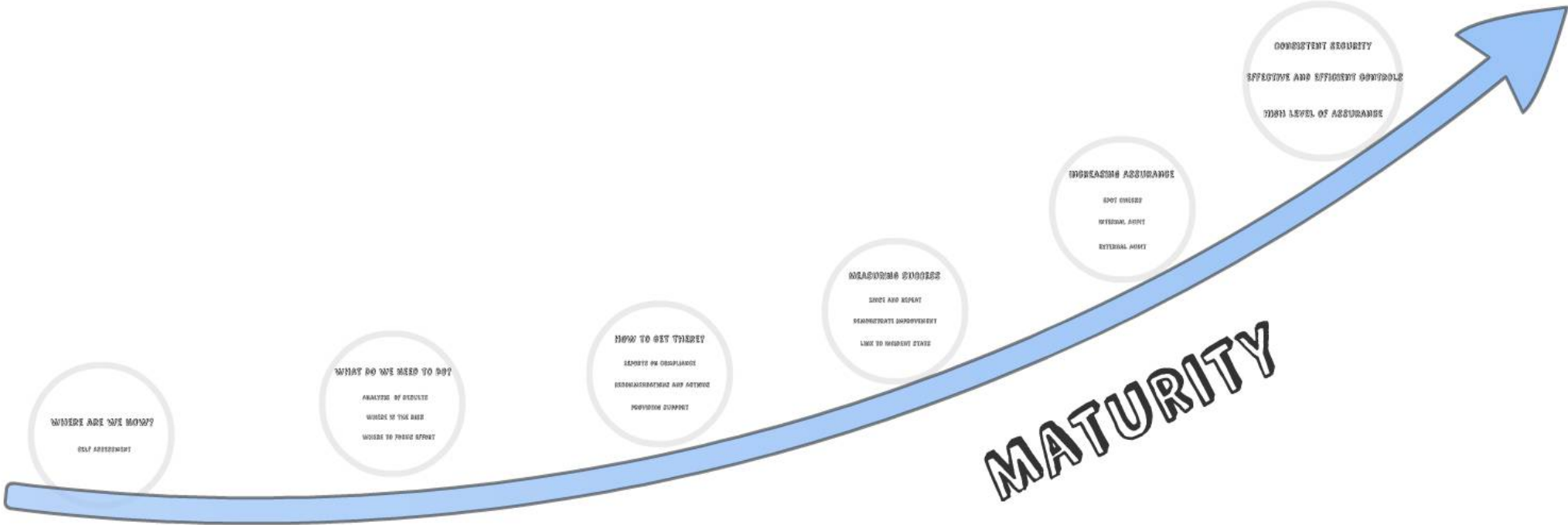


CONSISTENT SECURITY

EFFECTIVE AND EFFICIENT CONTROLS

HIGH LEVEL OF ASSURANCE

COMPLIANCE AND ASSURANCE



MATURITY

TOOLING



verinice.



DATABASE OF AUDITS AND COMPLIANCE

The screenshot displays the 'Information Security Model' software interface. On the left, a tree view shows the hierarchy of controls under 'Baseline High Level Maturity Assessments' and 'Baseline Technical Level Security Assessments'. The 'ACC.01 Access Control' control is selected. The right pane shows the detailed view for this control, including fields for Title, Abbreviation, Tags, Document, Implementation status, Explanation, Objective, Implementation date, Statement of Applicability, Greenbone GSM, Control Strength, and Relations to.

Information Security Model

- Assessments and Audits
 - Baseline High Level Maturity Assessments
 - 2017
 - _Template Audit (Copy Me)
 - Controls
 - HLMA.HUM.OxfordMartin
 - Controls
 - COM.01 Compliance [HLMA.HUM.OxfordMartin.2017.csv]
 - INC.01 Incident Management [HLMA.HUM.OxfordMartin.2017.csv]
 - ITS.01 IT Security [HLMA.HUM.OxfordMartin.2017.csv]
 - MIS.01 Management of Information Security [HLMA.HUM.OxfordMartin.2017.csv]
 - MOB.01 Mobile Devices [HLMA.HUM.OxfordMartin.2017.csv]
 - PAE.01 Physical and Environmental [HLMA.HUM.OxfordMartin.2017.csv]
 - TAA.01 Training and Awareness [HLMA.HUM.OxfordMartin.2017.csv]
 - WTP.01 Working with Third Parties [HLMA.HUM.OxfordMartin.2017.csv]
- Baseline Technical Level Security Assessments
 - 2017
 - _Template Audit (Copy Me)
 - TLSA.HUM.OxfordMartin
 - Controls
 - ACC.01 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.02 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.03 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.04 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.05 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.06 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.07 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.08 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.09 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.10 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.11 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.12 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.13 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.14 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.15 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.16 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.17 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.18 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACC.19 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.01 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.02 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.03 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.04 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.05 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.06 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.07 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.08 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]
 - ACQ.09 System Acquisition Development and Maintenance [TLSA.HUM.OxfordMartin.2017.csv]

 Baseline High Level Maturity Assessments









 2017

 _Template Audit (Copy Me)

 Controls

 HLMA.HUM.OxfordMartin

 Controls

-  COM.01 Compliance [HLMA.HUM.OxfordMartin.2017.csv]
-  INC.01 Incident Management [HLMA.HUM.OxfordMartin.2017.csv]
-  ITS.01 IT Security [HLMA.HUM.OxfordMartin.2017.csv]
-  MIS.01 Management of Information Security [HLMA.HUM.OxfordMartin.2017.csv]
-  MOB.01 Mobile Devices [HLMA.HUM.OxfordMartin.2017.csv]
-  PAE.01 Physical and Environmental [HLMA.HUM.OxfordMartin.2017.csv]
-  TAA.01 Training and Awareness [HLMA.HUM.OxfordMartin.2017.csv]
-  WTP.01 Working with Third Parties [HLMA.HUM.OxfordMartin.2017.csv]





 Baseline Technical Level Security Assessments

 2017

 _Template Audit (Copy Me)

 TLSA.HUM.OxfordMartin

 Controls

-  ACC.01 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
-  ACC.02 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
-  ACC.03 Access Control [TLSA.HUM.OxfordMartin.2017.csv]
-  ACC.04 Access Control [TLSA.HUM.OxfordMartin.2017.csv]

CREATING QUERIES

Edit Data Set - Data Set

Create a report query

Load Query Save Query

Relations All Change...

Move Up Move Down Add Empty Duplicate Last Remove

<input type="radio"/>	Audit	.	Title				
<input type="radio"/>	Audit	>	Controls	>	Control	.	Title
<input type="radio"/>	Audit	>	Controls	>	Control	.	Tags
<input type="radio"/>	Audit	>	Controls	>	Control	.	Implemented
<input type="radio"/>	Audit	>	Controls	>	Control	.	Explanation

?

OK Cancel

GENERATING REPORTS

The screenshot displays the BIRT Report Designer interface. The main workspace shows a report design with a table and a footer row. The table has the following structure:

Audit Title	Control Title	Control Group	Implementation	Explanation	Division	Unit
[Audit Title]	[Control Title]	[Control Group]	[Implementation]	[Explanation]	[Division]	[Unit]
Footer Row						

The left sidebar contains the Palette and Outline. The Outline shows the following structure:

- TLSA.rptdesign
 - Data Sources
 - Data Sets
 - Data Set
 - Audit Title
 - Control Title
 - Control Group
 - Implementation
 - Explanation
 - Division
 - Unit
- Data Cubes
- Report Parameters
- Variables
- Body
- MasterPages
- Styles
- Embedded Images

The bottom right pane shows the Property Editor for the selected Data Set:

General	General
Comments	Name: Data Set
Event Handler	Element ID: 8
Advanced	Data Source: Data Source

GENERATING REPORTS

V. Report [Window Title Bar: Minimize, Maximize, Close]

Generate report

Create a report with data from verinice. Reports can contain malware or other security hazards. Only use reports from sources that you trust.

Choose Report: (L) TLSA

Top level element: QUERY_TEST_TLSA

Output Format: Excel Format (XLS)

Output File: C:\Users\dunca\Documents\TLSA_QUERY_TEST_TLSA_2017-01-27.xls [Browse...](#)

Use date in file name

Always use this directory

[Reset reportcache](#)

[OK](#) [Cancel](#)

GENERATING REPORTS

Audit Title	Control Title	Control Description	Maturity	Maturity Comment	Division	Department
HLMA/MPL-Hogwarts	CCM:01 Compliance	CCM:01 - Perform regular compliance reviews of your division, department or faculty's information security arrangements against University policy. - Report on compliance within your division, department or faculty to your Divisional Information Security Working Group and the Joint Information Security Advisory Group.	2		MPL	Hogwarts
HLMA/MPL-Hogwarts	INC:01 Incident Management	INC:01 Ensure local procedures are in place for the management of information security incidents within your division, department or faculty: - formal incident response procedures exist to reduce the impact of incidents; - procedures exist for the communication of incidents to relevant stakeholders; - incidents are investigated to identify root causes; - incidents are recorded along with lessons learned to prevent re-occurrence.	2	We are alert to the need to report incidents but our procedures are not as formalised as required at level 3. We have acted on lessons learned though including initiating a division-wide training session following an incident.	MPL	Hogwarts
HLMA/MPL-Hogwarts	ITS:01 IT Security	ITS:01 Ensure all systems within your division, department or faculty comply with the University's 'baseline' information security controls for: - Access Control - Network Security - IT Operations - Vulnerability Management - Incident Management - System Acquisition and Development - Monitoring and Logging - Change Management	2	See technical assessment for further details.	MPL	Hogwarts
HLMA/MPL-Hogwarts	MIS:01 Management of Information Security	MIS:01 Assign overall ownership of information security within your division, department or faculty: - Define and document any specific information security, regulatory or legal requirements for your division, department or faculty; - Identify and assign specific roles and responsibilities related to information security within your division, department or faculty; - Embed information security into your management framework.	1	The importance of information security is recognised at Senior Management level. Issues are considered by management regularly but further work is required to embed a systematic approach including aspects such as listing information security responsibilities in job descriptions.	MPL	Hogwarts
HLMA/MPL-Hogwarts	MOB:01 Mobile Devices	MOB:01 - Ensure that any mobile devices within your division, department of faculty have appropriate controls in place: - Prohibited from unauthorised access by at least a 4-digit PIN or a passphrase; - Configured to ensure they automatically lock after a period of inactivity; - Configured in such a way that they can be remotely wiped in the event of loss; - Data is encrypted at rest; - Only have trusted applications from reputable sources installed; - Currently receiving software updates from the manufacturer and other 3rd parties; and - Receive software updates for security patches within a reasonable timeframe.	0	Our practice has been to give advice and provide services such as encryption for laptops. We are in the process of formalising this advice into a policy which will be communicated to all members of the Department.	MPL	Hogwarts
HLMA/MPL-Hogwarts	PAE:01 Physical and Environmental	PAE:01 - Ensure that any IT facilities within your division, department or faculty have appropriate environmental and physical security arrangements in place: - Obtain assurances, where third parties have responsibility for hosting or processing University information on your behalf, that appropriate arrangements are in place.	3		MPL	Hogwarts
HLMA/MPL-Hogwarts	TAA:01 Training and Awareness	TAA:01 Arrange and annually repeat a compulsory information security awareness training to ensure staff fully understand their Information Security responsibilities. - include information security awareness training as an integral part of the process for new joiners; - Maintain up-to-date records of awareness training completion.	2	We are finding it difficult to move from level two to three because of limited resources. Monitoring and reminding individuals would take staff time. It would be helpful if the monitoring reports from the system were robust and even better if the system could send annual reminders.	MPL	Hogwarts
HLMA/MPL-Hogwarts	WTP:01 Working with Third Parties	WTP:01 - Exercise a due diligence process, including a risk assessment, around information security when engaging third-parties to ensure that new contractual arrangements are adequate: - Maintain up-to-date records of all third parties that access, store or process University information; - Monitor and periodically review existing agreements with third-parties to ensure their adequacy; - Monitor the compliance of third-parties against your Information Security requirements and contractual arrangements.	0	We do have the need for third party services e.g. electronic lab notebooks and other cloud services. We are concerned about our lack of compliance in this area but resource and expertise is a real issue for us.	MPL	Hogwarts

Audit Title	Control Title	Control Description	Maturity	Maturity Comment	Division	Department
HLMA.MPL.Hogwarts	COM.01 Compliance	COM.01 - Perform regular compliance reviews of your division, department or faculty's information security arrangements against University policy: - Report on compliance within your division, department or faculty to your Divisional Information Security Working Group and the Joint Information Security Advisory Group.	2		MPL	Hogwarts
HLMA.MPL.Hogwarts	INC.01 Incident Management	INC.01 Ensure local procedures are in place for the management of information security incidents within your division, department or faculty: - formal incident response procedures exist to reduce the impact of incidents; - procedures exist for the communication of incidents to relevant stakeholders; - incidents are investigated to identify root causes; - incidents are recorded along with lessons learned to prevent re-occurrence.	2	We are alert to the need to report incidents but our procedures are not as formalised as required at level 3. We have acted on lessons learned though including initiating a division-wide training session following an incident.	MPL	Hogwarts
HLMA.MPL.Hogwarts	ITS.01 IT Security	ITS.01 Ensure all systems within your division, department or faculty comply with the University's 'baseline' information security controls for: - Access Control - Network Security - IT Operations - Vulnerability Management - Incident Management - System Acquisition and Development - Monitoring and Logging - Change Management	2	See technical assessment for further details.	MPL	Hogwarts
HLMA.MPL.Hogwarts	MIS.01 Management of Information Security	MIS.01 Assign overall ownership of information security within your division, department or faculty: - Define and document any specific information security, regulatory or legal requirements for your division, department or faculty; - Identify and assign specific roles and responsibilities related to Information Security within your division, department or faculty:	1	The importance of Information Security is recognised at Senior Management level. Issues are considered by management regularly but further work is required to embed a systematic approach including aspects such as listing information security responsibilities in job descriptions.	MPL	Hogwarts

CREATING WRITTEN REPORTS



Executive Summary

Overview

This report summarises the baseline self-assessments completed by the sections of IAS as part of the Information Security Team (IST) review of Information Security maturity across the college university. These assessments measured each section's current maturity level against a 5-point scale for each of 8 security domains. The assessments will be repeated on an annual basis to enable the university to demonstrate steady improvements to information security maturity.

IAS maturity

The average maturity of all IAS sections in each of the security domains is between 1 and 3 out of 5 with an overall average of 2.2. It is not envisaged that the IST will make the assessment process with a university until over the long run and the average score was roughly comparable. It is also important to note that a realistic initial goal is to raise overall maturity to a 3 across the entire college university.



Specific maturity scores varied significantly, both across sections for security domains and across security domains for individual sections, with many in status of extremely low and high levels of maturity. Despite this, average maturity scores for sections do not differ by large amounts but rather show the same 1 to 3 maturity rating observed previously.



Individual scores are summarised in the heat map below:

	Security	Compliance	IT Security	Management of Information Security	Mobile Devices	Physical and Environmental	Working with External Parties	Working with Third Parties	Average
Compliance	2	2	2	2	2	2	2	2	2.0
Incident Management	2	2	2	2	2	2	2	2	2.0
IT Security	2	2	2	2	2	2	2	2	2.0
Management of Information Security	2	2	2	2	2	2	2	2	2.0
Mobile Devices	2	2	2	2	2	2	2	2	2.0
Physical and Environmental	2	2	2	2	2	2	2	2	2.0
Working with External Parties	2	2	2	2	2	2	2	2	2.0
Working with Third Parties	2	2	2	2	2	2	2	2	2.0
Average for Section	2.2	2.2	2.2	2.2	2.2	2.2	2.2	2.2	2.2



Incident management

Requirements

Incident response procedures are in place for the management of information security incidents within each division, section or faculty.

- Formal incident response procedures exist to reduce the impact of incidents.
- Incidents exist for the operationalisation of incidents to relevant stakeholders.
- Incidents are investigated to identify root causes.
- Incidents are recorded along with lessons learned to prevent re-occurrence.

Results

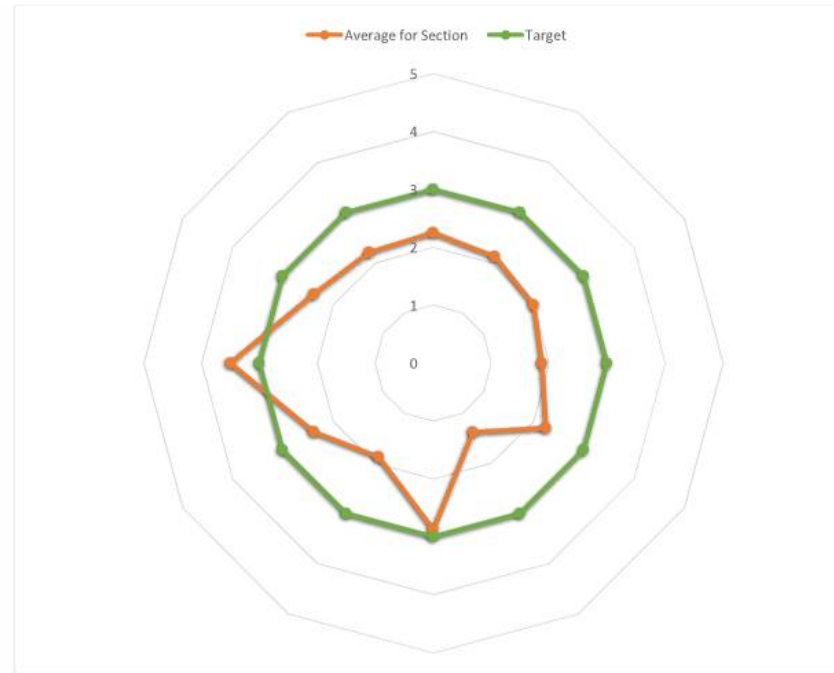
Maturity Level	Description	Section
Level 5: Optimal	Incident response plans are in place	Section
Level 4: Good	Security incident procedures are in place but are not formalised	Networks, Com
Level 3: Satisfactory	Incident response procedures exist and incidents are investigated and reported to senior management on an ad hoc basis	Networks
Level 2: Fair	Incident response procedures are documented and followed by all. Records of incidents are made and along with root causes and lessons learned, incidents are periodically reported to senior management	Compliance
Level 1: Poor	Partial meet with evidence of operational incident detection and response (e.g. triggering alerts, logging events)	Networks
Level 0: Not met	As at least, with evidence of a response process. No policies and formal incident response plans and procedures. Documented evidence of lessons learned and adjusted plans	Networks

Comments

Overall maturity is generally high in this area, though the IST has identified that there is no formal IAS incident management process for sections to follow.

Actions

Action	Owner	Target
Take forward the actions in individual reports from the IST and report back to the baseline working group	All sections	July 2017
Continue to develop incident management procedures and work with IT Services to ensure they are followed to normalise incident response reporting of incidents with IT Service Desk and to replace software	IST	July 2017
Follow up on review of good practice and disseminate this information across the wider of IAS	IST	July 2017



Individual scores are summarised in the heat map below:

	Hogwarts	Aartsverk	Endeavour	St. Barnaby's	Science department	Cardinal's College	Foxe College	Jordan College	Queen Phillipas	Wordsworth	Shakespeare	Average
Compliance	0	0	1	1	0	2	3	0	3	0	1	1.0
Incident Management	1	3	2	3	4	1	4	2	3	5	4	2.9
IT Security	2	2	2	2	2	1	2	3	2	2	2	1.9
Management of Information Security	3	2	2	2	4	2	3	2	1	4	1	2.4
Mobile Devices	3	3	2	1	0	1	2	2	3	5	2	2.2
Physical and Environmental	4	4	3	3	3	2	4	2	3	4	4	2.9
Training and Awareness	4	2	2	2	2	1	3	1	0	4	4	2.3
Working with Third Parties	1	1	2	1	3	1	2	3	4	4	1	2.1
Average for Section	2.3	2.1	2.0	1.9	2.3	1.4	2.9	1.9	2.4	3.5	2.4	2.2

Executive Summary

Overview

This report summarises the baseline self-assessments completed by the sections of UAS as part of the Information Security Team (IST) review of information security maturity across the collegiate university. These assessments measured each section's current maturity level against a 5-point scale for each of 8 security domains. The assessments will be repeated on an annual basis to enable the university to demonstrate steady improvements to information security maturity.

UAS maturity

The average maturity of all UAS sections in each of the security domains is between 1 and 3 out of 5 with an overall average of 2.2. This is not unexpected: the IST trialed the assessment process with 6 university units over the long vacation and the average score was roughly comparable. It is also important to note that a realistic initial goal is to raise overall maturity to a 3 across the entire collegiate university.



Specific maturity scores varied significantly, both across sections for security domains and across security domains for individual sections, with many instances of extremely low and high levels of maturity. Despite this, average maturity scores for sections do not differ by large amounts but rather show the same 1 to 3 maturity rating observed previously.

Information Security Team Baseline High Level Security Assessment



Incident management

Requirements

Ensure local procedures are in place for the management of Information Security incidents within your division, Section or faculty:

- formal incident response procedures exist to reduce the impact of incidents;
- procedures exist for the communication of incidents to relevant stakeholders;
- incidents are investigated to identify root causes;
- incidents are recorded along with lessons learned to prevent re-occurrence.

Results

Maturity Level	Description	Sections
Level 0: Non-existent	No security incident response plans are in place.	
Level 1: Initial	Security incident procedures are in place but are not formalised.	Wordsworth, Foxe
Level 2: Repeatable	Incident response procedures exist and incidents are investigated and reported to senior management on an ad-hoc basis.	Howwarts
Level 3: Defined	Incident response procedures are documented and followed by all. Records of incidents are maintained along with root causes and lessons learned. Incidents are periodically reported to senior management	Cardinal's
Level 4: Managed	As at level 3, with evidence of validation of incident detection and response (e.g. triggering alerts, testing plans).	Aardvark
Level 5: Optimised	As at level 4, with evidence of a repeatable process to validate and test incident response plans and procedures. Documented evidence of lessons learned and adjusted plans.	Wykeham

Comments

Overall maturity is generally high in this area, though the IST has identified that there is no formal UAS incident management process for sections to follow.

Actions

Action	Owner	Target
Take forward the actions in individual reports from the IST and report back to the divisional working group	All sections	July 2017
Formalise and document incident management procedures and work within IT Services to ensure they are followed to internally	IST	July 2017
Investigate future recording of incidents within planned Governance Risk and Compliance software	IST	July 2017
Follow-up on areas of good practice and disseminate this information across the whole of UAS	IST	July 2017

Shakespeare	Average
1	1.0
4	2.9
2	1.9
1	2.4
2	2.2
4	2.9
4	2.3
1	2.1
2.4	2.2

CREATING WRITTEN REPORTS



Executive Summary

Overview

This report summarises the baseline self-assessments completed by the sections of UAS as part of the Information Security Team (IST) review of Information Security maturity across the college university. These assessments measured each section's current maturity level against a 5-point scale for each of 8 security domains. The assessments will be repeated on an annual basis to enable the university to demonstrate steady improvements to information security maturity.

UAS maturity

The average maturity of all UAS sections in each of the security domains is between 3 and 3 out of 5 with an overall average of 3.2. This is not unexpected - the IST initiated the assessment process with a maturity level of 3 as a realistic initial goal to raise overall maturity to a 3 across the entire college university.



Specific maturity scores varied significantly, both across sections for security domains and across security domains for individual sections, with many in status of extremely low and high levels of maturity. Despite this, average maturity scores for sections do not differ by large amounts but rather show the same 1 to 3 maturity rating observed previously.



Individual scores are summarised in the heat map below:

	Security	IT Security	Management of Information Security	Mobile Devices	Physical and Environmental	Working with Third Parties	Working with Students	Average
Compliance	3	3	3	3	3	3	3	3.0
Incident Management	3	3	3	3	3	3	3	3.0
IT Security	3	3	3	3	3	3	3	3.0
Management of Information Security	3	3	3	3	3	3	3	3.0
Mobile Devices	3	3	3	3	3	3	3	3.0
Physical and Environmental	3	3	3	3	3	3	3	3.0
Working with Third Parties	3	3	3	3	3	3	3	3.0
Working with Students	3	3	3	3	3	3	3	3.0
Average for Section	3.2	3.1	3.0	3.1	3.1	3.1	3.1	3.2



Incident management

Requirements

Incident response procedures are in place for the management of information security incidents within each division, section or faculty.

- Formal incident response procedures exist to reduce the impact of incidents.
- Incidents exist for the operationalisation of incidents to relevant stakeholders.
- Incidents are investigated to identify root causes.
- Incidents are recorded along with lessons learned to prevent re-occurrence.

Results

Maturity Level	Description	Section
Level 5: Optimal	Incident response plans are in place.	Section
Level 4: Good	Security incident procedures are in place but are not formalised.	Academics, Com
Level 3: Reasonable	Incident response procedures exist and incidents are investigated and reported to senior management on an ad hoc basis.	Network
Level 2: Deficient	Incident response procedures are documented and followed by all. Records of incidents are made and along with root causes and lessons learned, incidents are analysed by senior management.	Central's
Level 1: Unacceptable	Local staff, with evidence of operational incident detection and response (e.g. triggering alerts, logging events).	Academics
Level 0: Not Assessed	As at present, with evidence of a response process. No incident response plans exist and procedures are not documented or reviewed and updated plans.	Academics

Comments

Overall maturity is generally high. In this area, though the IST has identified that the role is to formalise UAS incident management process for sections to follow.

Actions

Action	Owner	Target
Take forward the actions in individual reports from the IST and report back to the baseline working group.	All sections	July 2017
Continue to develop incident management procedures and work with IT Services to ensure they are followed to formalise incident response procedures.	IST	July 2017
Investigate future reporting of incidents with IT Services to formalise and improve reporting.	IST	July 2017
Follow up on review of good practice and disseminate this information across the whole of UAS.	IST	July 2017

LOOKING AHEAD

BETTER AUTHENTICATION SUPPORT

IMPROVED WEB INTERFACE

PER-SCOPE RISK ASSESSMENTS

MORE COMPLEX REPORTING OPTIONS



QUESTIONS



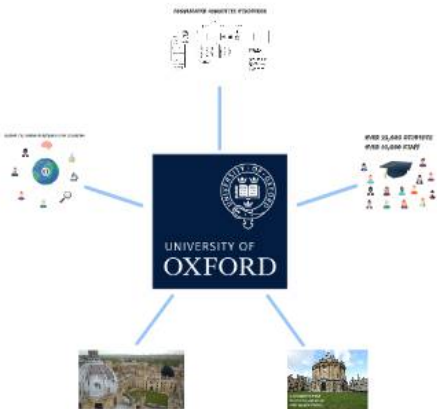
INFORMATION SECURITY CHALLENGES?



IMPROVING INFORMATION SECURITY



HOW TO SECURE A COLLEGIATE UNIVERSITY



RISK MANAGEMENT



QUESTIONS

TOOLING



COMPLIANCE AND ASSURANCE

