Activities	Council	University Executive Board	Audit & Risk Committee	Senior Information Risk Owner	General Counsel	Chief Digital Technology Officer	University Leadership Team	IT Leadership	Data Protection Officer	Senior Risk & Resilience Manager	HR team	Cyber Security Manager	Cyber Security & Compliance Analyst	Auditor	Information System Owners/Administrators	All Users	Line Managers	Information Asset Owners
Ensuring that information security is integrated into decision making by the University Executive Group (UEG)	A	R	R	C			C		C							I	C	C
Ensuring information security resources are in place to protect the confidentiality, integrity and availability of information	A	R	R	R		R	C		C			C						
Ensuring compliance with all legislative and regulatory requirements relating to data protection and information security, including PCI DSS obligations	I	I	R	R	A		C		R									
Ensuring regular, independent audits of implementation of the Information Security policy are undertaken, and appropriate actions are taken to correct any deficiencies found	I	A	R	I		C	C							R				
Providing assurance to Council on the overall effectiveness of information security within the University	I	A	R	R		C			C									
Ensuring that the Data Protection Officer has appropriate levels of autonomy, as well as access to necessary support and resources to fulfil the role	I	A	I		R				C									
Approving the Information Security strategies, policies, and requisite architectures ensuring they are aligned with the University's Statement of Risk Appetite and Tolerance	A	R	C	R		R	I	C	C	C		C			I			
Reporting to the Audit and Risk Committee (ARC) on any changes required to the risk appetite and tolerance	A	R	I	R		C				C								
Agreeing, implementing and reviewing the University's Risk Management Framework and Statement of Risk Appetite and Tolerance; Ensuring information security risk assessment criteria is aligned to the University Risk Appetite and Tolerance	I	A	R	R			C		I	C		I						
Monitoring performance against agreed information security key performance indicators based on agreed metrics	I	I	R	A		C	C		C			C						
Driving a culture valuing, protecting and using information for University success and for the benefit of its staff and students	I	C	C	A			R									R		
Provide clear direction, commitment and visible support for initiatives	I	A	I	R			R		C							I	R	
Overall implementation management including creation of the Information Security and subsidiary policies, ensuring regular reviews to confirm the policies remain fit for purpose	I	A	I	R			I											
Proposing required changes to the Information Security and subsidiary policies to the University's Executive Group for approval	I	A	I	R				I	C			C						
Ensuring appropriate information security controls are implemented across the University	I	A	R	R	C	R	R		R	R	R	R			R		R	R
Ensuring organisational training to support information security requirements is identified, implemented and effective	I	A	R	R		C	C		C		R	C			C	I	C	C
Ensuring information security risks and incidents are appropriately managed	I	A	R	R		R	R	C	R			C						
Providing status updates to ARC on high priority information security risks to the University	I	A	I	R		R	C		C	R		C			C			
Monitoring compliance with data protection requirements and for advising on data protection obligations under Information Security and subsidiary policies	I	A		C					R									
Implement and develop the University's approved data protection initiatives	I	A		I			C		R									
Authorising legal access to users' personal data to investigate suspected breaches of University regulations or the law	I	A		C	C				R									
Monitoring and managing any breaches of data protection legislation and, where appropriate, passing notice of data breaches to the supervisory authority – Information Commissioners Office (ICO)	I	A	I	C	C				R									
Providing advice and guidance to ensure personal and special category data is always handled and processed correctly	I	A	I	C					R									
Ensuring information technology services used by the University are procured, designed, implemented and maintained in such a way as to support the Information Security and subsidiary policies in line with the University's risk appetite and tolerance levels	I	A	I	C		R	C	C	C			C			R			
Ensuring that Information Technology security related training is delivered, and advice is available as required on information technology security matters	I	I	I	A		R		C	C			C						
Authorising access to personal or restricted information for specific operational reasons	I	I	I	A		R			C									
Ensuring risk assessments of information technology services and assets are undertaken to determine the probability and impact of security failures and recommending appropriate mitigation	I	I	I	A		R	C		C	I		C	C		R			
Adhering to the University's Project lifecycle framework, ensure security risks are identified and mitigated where possible, in line with the University's Risk Management framework				A		R	C	R	C	I		C	C					
Ensuring that all IT staff understand their responsibility towards information technology security and know how to identify and assess risks, opportunities, hazards and threats	I	I	I	A		R				C		C	C		R			R
Ensuring reported information technology security incidents and/or risks are investigated and responded to appropriately				A		R		R	C	I		C	C		C			C
Ensure that an effective monitoring and reporting framework is established with regards to information security compliance, and that information asset and system owners are designated, perform their roles and report regularly on information security compliance in relation to their respective information assets and schools/professional service areas	I	A	I	R		C	R								C			C
Communicating University policy and information about the risk management programme to all staff and other stakeholders as necessary			I	A			C		C	R		C						
Maintaining the University's risk management framework and processes by monitoring local arrangements within Schools and Professional Services Divisions and raising awareness of the expected standards	I	I	I	A			C		C	R		C						
Providing continuity specialist advice IT teams, to ensure alignment of University recovery expectations		I		A		I	C	R		R		C			C			
Ensuring information security is considered in all Business Continuity and Recovery responses			A				C			R							I	
Ensuring all information in their work area is managed in conformance with the Information Security and subsidiary policies		I	I	A			R							C			I	
Ensuring all staff, students, associates and visitors (for whom they have management or contractual responsibility) are made aware of the Information Security and subsidiary policies and their obligations and are given appropriate support and resources to comply with these		I	I	A			R				C						R	
Ensuring that consistent local processes and procedures are developed, documented, implemented, followed and regularly reviewed		I	I	A			R			I					R		R	R
Nominate Information System Owners for key systems to ensure that information security is embedded and maintained in the daily operation of those systems. Systems can be electronic and/or manual				A		I	R		I	I					I			C
Having an overview of how information is handled and processed with their work area, including the repositories that hold data				I			A		C						C		R	R
Having a broad understanding of information security threats and where there is a need to conduct an information security risk assessment for either existing or new activities				I			A		C						C		C	R
Ensuring that the Information Asset Register reflects all information assets within their work area and how data is processed				I			A		C						C			R
Understanding where and when data is shared with third parties, and whether that is covered by contractual or data sharing arrangements		A			C		R		I									R
Creating, developing and supporting information assets in line with the Information Security and subsidiary policies and Cyber Security Principles ensuring that information assets are operated and deployed based on agreed information security and data protection controls				I		I	A	R	C			C			R			
Communicating any information security deficiencies or weaknesses in the system and operating environments			I	A		C		C							R	R		
Determine whether certain changes/abnormal behaviour(s) in the environments or systems of the operation require involvement of the Cyber Security & Compliance Analyst and/or Data Protection Officer			I			C	A	R	C			I	C		R			
Determine whether changes in the technical environments or technical systems require involvement of the Cyber Security & Compliance Analyst and/or Data Protection Officer			I	A		R	R	R	C			C			R			C
Ensure that joiners, movers and leavers procedures address security requirements and are adhered to			I	A				R	C		C	C			R		I	
Reporting any personal data breach immediately to the Data Protection Officer				A					I							R	I	
Reporting any physical information security incidents or risks to Sussex Estates and Facilities				A												R	I	
Reporting any information technology security incidents or risks to the IT Service desk immediately				A									I			R	I	
Complying with the Information Security and subsidiary policies				A												R		
Completing any information security training as required by the University				A												R		

R is for Responsible. A responsible role is accountable for the performance of a service, process or task. A person that is responsible does the work to achieve a task.

A is for Accountable. The accountable role is the role that is ultimately responsible for an activity. For instance, process owner is accountable for a process and service owner is accountable for a service. Although accountability does not necessarily mean that the person in the role is, in fact, performing the activity. He is the ultimately responsible for the activity. Only one person must be accountable for an activity.

C is for Consulted. A consulted role should be involved in a task as a subject matter expert who provides information or input about regarding the task. These people are not directly involved in the activity. But they can provide inputs that will enable the responsible person to do the task more efficiently and effectively.

I is for Informed. An Informed role must be kept informed about the status of the task or activity. These people receive outputs from a process or are kept up-to-date on progress. They are often only informed when the task or deliverable has been completed. Unless of course, there is a severe problem that prevents the task or activity to progress or to deliver.