CQUEST - Cyber Resilience Questionnaire

			Answers				Response
			A	B	C	D	
Governance and Leadership	1	Does a formally documented cyber security strategy exist and who is it approved by within the organisation?	A cyber security strategy has been approved at senior executive level and is reviewed at least annually.	A cyber security strategy has been approved by senior executives. This is reviewed at set intervals, but not in the last 12 months.	A cyber security strategy has been approved by an operational or technology lead and is reviewed at set intervals.	There is no formally documented cyber security strategy.	
	2	Does a formally documented framework (including policies, standards and delivery programme) exist to maintain your security posture and to deliver the cyber security strategy?	A documented cyber security framework exists with all supporting components. It is aligned to industry-recognised standards, has been approved at senior executive level and is reviewed at least annually.	A documented cyber security framework exists, is aligned to industry-recognised standards and has been approved at senior executive level. This is reviewed at set intervals, but not in the last 12 months.	A cyber security framework has been approved by an operational or technology lead and is reviewed on an ad-hoc/infrequent basis.	There is no formally documented cyber security framework to deliver the cyber security strategy.	
	3	Has a senior executive been appointed who is accountable for the delivery of the cyber security framework within the organisation?	A senior executive has been appointed who is accountable for delivery of the cyber security framework. This is either their dedicated role or a significant proportion of their role.	Someone (not a senior executive) within the organisation has been appointed and is accountable for delivery of the cyber security framework. There are plans to appoint a senior executive in the future.	Someone (not a senior executive) within the organisation has been appointed and is accountable for the delivery of the cyber security framework.	No-one has been appointed to be accountable for the delivery of the cyber security framework.	
	4	Are risks to cyber security managed effectively?	All risks to cyber security are translated into and managed within the enterprise risk framework. These are aligned to enterprise-level risk appetite statements and reassessed on an ongoing basis.	All risks to cyber security are translated into and managed within the enterprise risk framework. These are aligned to functional risk appetite statements and reassessed at set intervals.	Risks to cyber security are managed locally, with some visibility provided at an organisational level. These risks are reassessed on an ad-hoc/infrequent basis.	There is some awareness of risks to cyber security but no formal structure to manage them.	
	5	Has the effectiveness of cyber controls been independently assessed against the control objective?	The effectiveness of cyber security controls has been independently assessed by a party with the competent level of skill and forms part of an established annual process, including senior executive review.	The effectiveness of cyber security controls has been independently assessed by a party with the competent level of skill and signed-off in the last 18 months, but is not part of an ongoing process.	The effectiveness of cyber security controls has not yet been independently assessed by a party with the competent level of skill, but an assessment is scheduled within the next six months.	The effectiveness of cyber security controls has not been independently assessed by a party with the competent level of skill and there is no plan to do so.	
	6	What level of knowledge and skills exists at the senior executive level?	All senior executives have sufficient understanding to provide effective oversight of the firm's cyber security strategy and cyber risk management. At least one senior executive has specialist knowledge and skills which the other executives can draw on.	At least one senior executive has sufficient understanding to provide effective oversight of the firm's cyber security strategy and cyber risk management. Training is scheduled to develop other senior executives' capabilities in the next 12 months.	Senior executives are currently dependent on external knowledge and skills to provide effective oversight of the firm's cyber security strategy and cyber risk management. There is a plan to address this in the next 12 months.	No senior executives currently have the relevant knowledge and skills to provide effective oversight of the firm's cyber security strategy and cyber risk management. There are no plans in place to address this.	
	7	Are roles, accountabilities and responsibilities for delivering the cyber security strategy clearly defined, assigned and understood by senior executives?	All roles, accountabilities and responsibilities are clearly defined, documented and assigned. All senior executives are aware of these and their understanding is validated.	All roles, accountabilities and responsibilities are clearly defined, documented and assigned. Senior executives' awareness and understanding of these are assumed.	Some roles, accountabilities and responsibilities are defined and assigned. Senior executives' awareness and understanding of these are assumed.	Accountabilities and responsibilities are not defined or assigned to roles.	
	8	To what extent is management information (MI), including Key Risk Indicators (KRIs), used to inform decision makers on the performance of cyber security controls?	Senior executives regularly review MI on cyber security controls. This MI is used to support the discussion of cyber security and relevant decision making.	Second line staff, such as operational risk leads, regularly review MI on cyber security controls. This MI is used to support the discussion of cyber security and relevant decision making.	First line staff, such as technology or operational leads, regularly review MI on cyber security controls. This MI is used to support relevant decision making.	MI on cyber security controls is not regularly reviewed.	
	9	Is there an exercising programme in place to validate your organisation's ability to respond to cyber security incidents, and inform your cyber security framework?	An ongoing strategic exercising programme is in place to validate the organisation's effectiveness in responding to cyber incidents across staff and processes, the results of which inform the development of the cyber security framework.	Exercises are conducted on an annual basis to validate the organisation's effectiveness in responding to cyber incidents across staff and processes, the results of which inform the development of the cyber security framework.	Exercising has been undertaken to validate the organisation's effectiveness in responding to cyber incidents, but this has not been conducted in the last 12 months.	The organisation does not undertake exercising to validate its effectiveness in responding to cyber incidents.	
Identify	10	Are business functions understood?	All business functions have been identified and prioritised in terms of their criticality and their underlying technology and processes. This is reviewed on an ongoing basis and updated in accordance with risk and change management processes.	All business functions have been identified and prioritised in terms of their criticality and their underlying technology and processes. This is reviewed annually.	Critical business functions have been identified and prioritised in terms of their criticality. This is reviewed on an infrequent or ad-hoc basis.	Critical business functions have not been formally identified and prioritised along with their underlying technology and processes.	
	11	Is a current inventory of information assets with supporting systems maintained?	Information assets and systems are identified, prioritised, and documented in a single inventory on an ongoing basis.	Information assets and systems are identified, prioritised, and documented in single/multiple inventories which are reviewed at set intervals.	Information assets and systems are identified, prioritised, and documented, and these are reviewed on an ad-hoc/infrequent basis.	Information assets and systems have not been formally identified, prioritised and documented.	
	12	Do you understand who your third party providers are and the services they provide?	An accurate register is maintained of all third party providers and the services they provide. Processes and procedures are in place to ensure that new third parties and/or changes in existing services are captured within the register.	A register is maintained of all critical third party providers and the services they provide. Processes and procedures are in place to ensure that new critical third parties and/or changes in existing services provided are captured within the register.	A list is held of critical third party providers and the services they provide.	There is no centrally held list of third party providers and services.	
	13	Are hardware and software vulnerabilities proactively identified and documented with their risk assessment?	There is an established vulnerability detection process to discover, document and risk assess vulnerabilities on a ongoing basis.	There is an established vulnerability detection process to discover, document and risk assess vulnerabilities on at least a monthly basis.	There is a vulnerability detection process to discover, document and risk assess vulnerabilities on an ad-hoc/infrequent basis.	There is no vulnerability detection process in place.	
	14	Are end of life hardware and software assets identified and effectively managed prior to expiration?	An asset inventory (or similar) is held which tracks the end-of-life for each asset. Assets out of support are recognised as potential vulnerabilities and managed accordingly through the risk management framework.	An asset inventory (or similar) is held which tracks the end-of-life for each asset. Decisions about when to replace these are risk-based.	End-of-life for groups of assets are tracked. Decisions about when to replace these groups are risk-based.	There is no process to identify end-of-life hardware or software.	
	15	To what extent have baseline patterns of network and communications activity been recorded and documented?	A baseline of network and communications activity has been identified and documented for the entire network including ingress/egress points. This is validated on a continuous basis.	A baseline for organisational network and communications activity has been identified and documented for some parts of the network including some ingress/egress points. This process is carried out at set intervals.	A baseline for organisational network and communications activity has been identified for egress/ingress points only. This process has been undertaken once and is planned to take place on an ad-hoc/infrequent basis.	A baseline of network and communications activity is not maintained.	
Protect	16	Does all remote access to the corporate network and business applications require strong authentication?	All remote access to the corporate network and business applications requires at least two-factor authentication.	Remote access to the majority of corporate network and business applications requires at least two-factor authentication.	Remote access for a limited number of corporate network and business applications requires at least two-factor authentication.	Remote access to the majority of corporate network and business applications requires only single-factor authentication.	
	17	How is user access to data via systems managed?	Requests for enabling or modifying user access to data requires permission from the data owner.	Requests for enabling or modifying user access to data is managed by line manager approval.	Requests for enabling or modifying user access to data requires permission from the system owner only.	Requests for enabling or modifying user access to data is not managed centrally.	
	18	How is user access to data via systems reviewed?	All user access and permissions to data is reviewed on an ongoing and requirements basis, e.g. as part of the joiners-movers-leavers process.	All user access and permissions to data is reviewed on at least an annual basis.	User access to data is reviewed on an ad-hoc basis and does not specify a review of permissions.	User access reviews are not required by policy.	
	19	Are privileged rights understood, documented and reviewed in terms of assignment to system and user accounts?	All privileged rights are centrally managed and documented. Access privileges are reviewed by the system/business owner on an ongoing basis and as part of any joiner-movers-leavers process.	All privileged rights are documented. Access privileges are reviewed by the system/business owner at set intervals and as part of any joiner-movers-leavers process.	Privileged rights are centrally understood and enforced as part of a joiners-movers-leavers process. Reviews are conducted on an ad-hoc/infrequent basis.	There is no centralised view of privileged rights or their assignment.	
	20	Are appropriate controls in place to classify information in terms of criticality and sensitivity?	All information assets and documents are classified and labelled in line with policy. Labelling is enforced for user generated content (e.g. emails and documents, etc.).	All information assets and documents should be classified and labelled in line with policy. Labelling is reliant on the user.	All documents should be classified and labelled in line with policy. Labelling is reliant on the user.	There is no consistently applied classifying and labelling of information.	
	21	Are appropriate tools and processes in place to detect and prevent sensitive data from leaving the corporate network?	Tools and processes are in place to prevent unauthorised sensitive data from leaving the corporate network at all egress/ingress points. All incidents are investigated and escalated where appropriate.	Tools and processes are in place to monitor for unauthorised sensitive data leaving the corporate network at all egress/ingress points. All incidents are investigated and escalated where appropriate.	Tools and processes are in place to monitor for unauthorised sensitive data leaving the corporate network at some egress/ingress points. Incidents are investigated on a best endeavours basis.	There are no formalised tools or processes in place to monitor or prevent unauthorised sensitive data leaving the corporate network.	
	22	Which option best describes your backup process?	All data and system configurations are backed up and encrypted in line with business requirements, including at least one format which does not require continuous access to the network.	All data is backed up and encrypted in line with business requirements, including at least one format which does not require continuous access to the network.	Critical data is backed up. Backups are typically protected and stored offsite, but this is not a formal requirement.	Data is not consistently backed up.	
	23	Do you have effective processes and procedures in place to assess the security capabilities and management of cyber risk by third party providers?	All third party providers are reviewed in line with the risks they present at set intervals. Findings are recorded and acted upon as required.	All critical third party providers are reviewed in line with the risks they present at set intervals. Findings are recorded and acted upon as required.	All critical third party providers are reviewed at the on-boarding stage in line with the risks they present. Findings have been recorded.	No assessment of third party providers is undertaken specifically in relation to risks they present.	
	24	Are proportionate measures in place to ensure that third parties with ongoing access to your network are appropriately managed?	Third party access to infrastructure and information is identified and documented, and proportionate controls implemented as a result e.g. periodic due diligence exercises, compliance audits, non-disclosure agreements, vetting/screening, contractual agreements.	Third party access to critical infrastructure and information is understood, and proportionate controls have been implemented e.g. periodic due diligence exercises, compliance audits, non-disclosure agreements, vetting/screening, contractual agreements.	Third party access to critical infrastructure and information is understood, and the organisation has measures in place to monitor (but not actively manage) this.	There are no measures currently in place to manage third party access to infrastructure or information.	
	25	Is cyber security incorporated in change management and design processes, as well as service and product development?	Cyber security is a fundamental part of all change processes and is considered within the business strategy.	Cyber security is a fundamental part of change processes relating to critical systems, services and products.	Cyber security is considered but not formally embedded as a part of change processes relating to critical systems, services and products.	Cyber security is not regularly considered in the context of change.	
	26	Are baseline system security configuration standards and hardening procedures in place to facilitate consistent application of security requirements to operating systems, databases, applications, devices, etc.?	Baseline security standards are documented and applied. Assets are monitored on an continuous basis for compliance against these standards.	Baseline security standards are documented and applied. Assets are checked at set intervals for compliance against these standards.	Baseline security standards are documented and applied. Assets either have not been checked for compliance against these standards, or are checked on an ad-hoc/infrequent basis.	Baseline security standards are not maintained.	
	27	Do you use monitoring and/or filtering solutions to restrict network traffic to or from ingress/egress points which might present a risk to the organisation?	The organisation proactively restricts or blocks access to all ingress/egress points. Filters are reviewed and regularly updated.	The organisation proactively restricts or blocks access to sensitive ingress/egress points. Filters are regularly updated.	The organisation proactively monitors access to ingress/egress points. Filters are regularly updated.	Monitoring or filtering solutions are not widely used.	
	28	Do you employ multiple layers of security to ensure that the corporate network is segregated effectively and protected from externally facing systems (e.g. firewalls and multiple AV vendors)?	A defence-in-depth strategy is employed creating multiple layers of security, including network segregation and application white listing. The organisation does not rely on a single solution for any of its cyber defences.	A defence-in-depth strategy is employed creating multiple layers of security. In most instances the organisation does not rely on a single solution for its cyber defences.	There are a few points where security is a single layer, but these do not relate to any critical systems.	The organisation typically relies on single vendors and solutions to protect the business.	
	29	Are staff provided with cyber security training?	All staff are provided with mandatory cyber security training as part of an ongoing programme. Levels of understanding are measured and gaps in knowledge are identified and used to adapt or prompt additional training.	All staff are provided with mandatory cyber security training at set intervals. Levels of understanding are measured and are used to prompt additional training.	Staff have access to cyber security training but it is not mandatory.	There is no training provided on cyber security.	
	30	Do you take a risk based approach to identifying your high risk staff and is additional cyber security training provided as needed to these members of staff?	High risk staff are identified and reviewed on a ongoing basis. Additional bespoke training is provided.	High risk staff are identified and additional training is provided at set intervals.	High risk staff are identified but no additional training is provided.	High risk staff are not identified.	
	31	Is appropriate screening and/or background checks conducted on new appointments and when employees change roles?	Staff screening is conducted upon employment and when employees change roles. Similar checks, following a recognised standard, are conducted on all staff at regular intervals throughout their employment, including those with access to critical systems.	Staff screening is conducted upon employment, and some further screening is conducted when senior or privileged roles are filled.	Staff screening is conducted upon employment.	References are checked upon employment.	
	32	Are physical access controls implemented, maintained and tested regularly across your organisation's facilities?	Physical access controls are implemented and maintained for all facilities. Access reviews are completed on an ongoing basis.	Physical access controls are implemented and maintained for all facilities. Access reviews are completed at set intervals.	Physical access controls are implemented and maintained for some facilities. Access reviews are completed on an ad-hoc/infrequent basis.	Physical access controls are implemented and maintained for some facilities. Access reviews are not conducted.	
Detect	33	Do you have the ability to monitor for and detect anomalous activities and/or events?	Event information is collected in real time, or near real time which is then collated, aggregated and analysed. Any alerts, anomalies or suspicious activities are investigated as they are detected. The integrity of this information is protected.	Event information from critical systems is collected in real time, or near real time which is then collated, aggregated and analysed. Any alerts, anomalies or suspicious activities are investigated as they are detected. The integrity of this information is protected.	Event information from some systems is collected in real time, or near real time which is then collated, aggregated and analysed. Any alerts, anomalies or suspicious activities are investigated as they are detected.	No capabilities have been established to monitor and detect anomalous activities and/or events on an ongoing basis.	
	34	Are remote access attempts recorded and alerts exist for potential malicious activity?	All access attempts are recorded and alerts exist for potentially malicious activity for all corporate network and business applications that are remotely accessible.	All access attempts are recorded and alerts exist for potentially malicious activity for critical corporate network and business applications that are remotely accessible.	Successful access attempts are recorded and alerts exist for potentially malicious activity for a limited number of corporate network and business applications that are remotely accessible.	There is no visibility of remote access attempts.	
	35	Do detective systems extend to monitoring personnel operating on the corporate network, including unauthorised connections or devices?	Expected activity for roles performed are profiled. Active monitoring takes place to identify deviation from expected patterns. Unauthorised connections are blocked.	Staff behaviour is monitored generally but specific individuals are not identified. Unauthorised connections are blocked.	Data loss prevention software to monitor outgoing communications from staff is employed, but no other monitoring is carried out.	Staff activity is not monitored.	
	36	How are known and documented vulnerabilities remediated in line with risk?	Vulnerabilities are remediated in line with the risks they present via the enterprise risk framework. Remediation is validated and assured as part of this process. There is an effective management process in place for accepted vulnerabilities.	Vulnerabilities are remediated in line with the risks they present. Remediation is validated and assured as part of this process. There is an effective management process in place for accepted vulnerabilities.	Vulnerabilities are remediated in line with the risks they present.	There is no consistent process for remediating vulnerabilities.	
	37	Do you carry out penetration tests to identify vulnerabilities that may affect your systems, networks, people or processes?	The organisation operates a strategic programme of threat intelligence-led end-to-end penetration tests, including against an industry recognised testing framework (e.g. CBEST or STAR) and aligned to long term business objectives.	The organisation undertakes threat intelligence-led end-to-end penetration tests against an industry recognised testing framework (e.g. CBEST or STAR).	The organisation undertakes testing against the wider enterprise or single applications, but these tend to be targeted in scope and/or are not threat intelligence-led.	The organisation does not regularly carry out penetration testing.	
	38	Are detection systems integrated within the organisation's incident response process?	Detection systems are linked directly to the incident response process, and automated alerting exists to trigger response actions if required. This is in place 24/7.	Detection systems are included within the incident response process. If the systems trigger an alert, the incident process is invoked manually. This is in place 24/7.	Detection systems are included within the incident response process. If the systems trigger an alert, the incident process is invoked manually. This is only available during business hours.	Detection systems have not been integrated into the incident response process.	
	39	Is there a process for gathering, analysing and sharing information on cyber threats?	There is a formalised process in place for analysing cyber threat intelligence. This encompasses information gathering from a diverse range of sources, collation and analysis, and defined links to business decision making. The process also articulates how intelligence should be shared with peers and other relevant parties.	There is a formalised process in place for analysing cyber threat intelligence. This encompasses information gathering from multiple sources, collation, analysis and dissemination to internal and external stakeholders.	There is an informal or nascent process in place for analysing cyber threat intelligence. This encompasses information gathering, analysis and dissemination.	There is no process in place for the utilisation of cyber threat intelligence.	
	40	Is cyber threat intelligence used to inform your cyber security strategy and framework?	Cyber threat intelligence is actionable, timely, targeted to specific audiences and used to support decision-making at all levels of the business (strategic through to tactical).	Cyber threat intelligence is actionable, timely and used to support a specific group (or groups) of business stakeholders.	Cyber threat intelligence is used to inform situational awareness and contextual understanding.	Cyber threat intelligence is not regularly used to inform decision making.	
Respond	41	Do your response plans include proactive communications with customers, third parties, authorities, media, etc.?	A communications plan and stakeholder map exists that has been developed and tested for use in a cyber incident.	A communications plan and stakeholder map exists that has been developed for use in a cyber incident.	A communications plan exists which is designed to be used for all incidents.	There is no formal communications plan for incidents.	
	42	Do incident response procedures/policies include how and when regulators and/or stakeholders should be informed of incidents?	The obligation to notify regulators and key stakeholders of incidents is included within incident response procedures along with set thresholds or triggers.	The obligation to notify regulators and key stakeholders of incidents is included within incident response procedures.	There is awareness of how and when regulators and key stakeholders should be notified of incidents, however this is not formally documented.	Obligations to report incidents to regulators and other key stakeholders are not widely understood across the organisation.	
	43	Does your incident response plan require you to share information on incidents and near-misses with industry peers (e.g. through CiSP)?	The incident response plan defines a specific requirement for information to be shared proactively through trusted channels, along with a named individual or team responsible for delivering this requirement. Information is shared as soon as is practically possible during or after an incident.	The incident response plan defines a specific requirement for information to be shared proactively through trusted channels. Information is typically shared after the conclusion of an incident.	The incident response plan does not specifically define proactive information sharing as a requirement; however this is done on an ad-hoc basis depending on the nature of the incident.	Information relating to incidents is not typically shared outside of the organisation.	
	44	Do you have thresholds that are aligned to impacts which determine the response when cyber security events or incidents occur?	Defined thresholds exist, aligned to impacts, which determine the response to an incident. These have been approved by business and supporting functions, and are formally documented as part of operational procedures. Thresholds are reviewed on a regular basis or after an event/incident.	Defined thresholds exist, aligned to impacts, which determine the response to an incident. These have been approved by the business and supporting IT functions and are formally documented as part of operational procedures.	Defined thresholds exist to help determine the response to an incident, but these are not formally documented or aligned to impacts.	There are no defined thresholds. Responses to incidents are determined on an ad-hoc basis.	
	45	Do you undertake in-depth investigations following a cyber security event or incident?	Processes are in place to carry out investigations and forensic analysis following an incident where required. Protective and detective controls are specifically engineered to facilitate the investigative process.	Processes are in place to carry out investigations and forensic analysis following an incident where required.	Processes are in place to carry out investigations following an incident where required. There is no forensic capability.	There are no processes in place to carry out investigation following an incident.	
Recover	46	Do you have a process in place to recover systems and data from an incident?	Processes are in place to recover systems and data in-line with business requirements. These processes are tested regularly against possible scenarios, findings are risk assessed with appropriate actions taken. The confidentiality, integrity and availability of these systems and data is maintained throughout the process.	Processes are in place to recover systems and data in-line with business requirements. These processes are tested regularly, findings are risk assessed with appropriate actions taken. The confidentiality, integrity and availability of these systems and data is maintained throughout the process.	Processes are in place to recover systems and data, however they are not all aligned to business requirements. These processes are not regularly or comprehensively tested.	There are no established policies and procedures in place for the recovery of data or systems.	
	47	Do you have a process in place that incorporates lessons learned from cyber security events and incidents?	Incident response and risk management processes incorporate lessons learned from incidents, near-misses and external events. These are used to inform improvements at all levels of the organisation (e.g. cyber security strategy through to incident response procedures).	Incident response and risk management processes incorporate lessons learned from incidents. These are used to inform improvements at operational levels of the organisation.	Incident response and risk management processes incorporate lessons learned from incidents. These may be used to inform improvements at operational levels of the organisation but not on a consistent basis.	Processes do not consistently incorporate lessons learned.	
	48	Have you engaged with critical third parties to understand the risks that exist between both parties, and taken steps to ensure that recovery activities are clearly understood by both parties?	Proactive relationships exist with critical third parties. There is assurance that response and recovery plans for all parties are understood, appropriate and tested.	Critical third parties have been engaged to discuss cyber risk. The organisation does not proactively share details of its recovery planning with third parties or involve them in testing.	There has been some limited engagement with third parties to map potential cyber risks.	There is no active engagement with third parties on cyber risk.	

Glossary

Letter	Term	Definition
A	Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions
A	Access Control	Means to ensure that access to assets is authorised and restricted based on business and security requirements. Source: ISO/IEC 27000:2018
A	Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity. Source: ISO/IEC 2382:2015
A	Accuracy	The closeness between an estimated result and the (unknown) true value
A	Advanced Persistent Threat (APT)	A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives. Source: Adapted from NIST
A	Alerting	The action of warning that a certain type of event has been encountered
A	Application	Computer program or set of programs that performs the processing of records for a specific function
A	Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals
A	Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met; an audit may be carried out by internal or external groups
A	Authenticity	Property that an entity is what it claims to be. Source: ISO/IEC 27000:2018
A	Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018
B	Business Function	A process or operation that is performed routinely to carry out a part of the mission of an organization.
C	Compliance	Ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed
C	Compromise	Violation of the security of an information system. Source: Adapted from ISO 21188:2018
C	Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. Source: Adapted from ISO/IEC 27000:2018
C	Continuously	An action or process that is carried out on all the time, without interruption
C	Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Source: Adapted from CPMI-IOSCO (citing NICCS)
C	Cyber Incident	A cyber event that: i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: Adapted from NIST (definition of "Incident")
C	Cyber Risk	The combination of the probability of cyber incidents occurring and their impact. Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")
C	Cyber Security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. Source: Adapted from ISO/IEC 27032:2012
C	Cyber Threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security. Source: Adapted from CPMI-IOSCO
D	Defence-in-Depth	Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation. Source: Adapted from NIST and FFIEC
D	Detect (Function)	Develop and implement the appropriate activities to identify the occurrence of a cyber event. Source: Adapted from NIST Framework
E	Effective or Effectiveness	High level of assurance that the proposed change(s) or action that will be implemented or has been undertaken will bring or has brought about the desired or intended result. Source: PRA/FCA
E	Egress Point	The point within a network where data leaves the organisation.
F	First line Staff	Technology or operational leads
F	Framework	A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of cyber security controls.
I	Identify (function)	Develop the organisational understanding to manage cyber risk to assets and capabilities. Source: Adapted from NIST Framework
I	Incident Management	Processes to detect and analyse incidents and determine an appropriate organisational response
I	Incident Response Team (IRT) [also known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: ISO/IEC 27035-1:2016
I	Incident	Cyber or operational, an instance of something happenning; an event or occurance.
I	Indicator	An occurrence or sign which reveals that an incident may have occurred or be in progress (IOSCO definition: http://bit.ly/1YDIyie).
I	Indicators of Compromise (IoCs)	Identifying signs that a cyber incident may have occurred or may be currently occurring. Source: Adapted from NIST (definition of "Indicator")
I	Information Asset	Any piece of data, device or other component of the environment that supports information-related activities, including data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services (IOSCO definition: http://bit.ly/1YDIyie).
I	Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: Adapted from NICCS
I	Ingress Point	The point within a network where data enters the organisation
I	Integrity	Property of accuracy and completeness. Source: ISO/IEC 27000:2018
L	Layered Protection	As any single defence against a cyber threat may be flawed, Firms can use a series of different defences to cover the gaps in the others' protective capabilities. For example, the use of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures and local storage encryption tools can each serve to protect information technology resources in ways the others cannot (IOSCO definition: http://bit.ly/1YDIyie).
L	Leading Standards, Guidelines and Practices	Standards, guidelines and practices which reflect industry best approaches to managing cyber threats, and which incorporate what are generally regarded as the most effective cyber security solutions (IOSCO definition: http://bit.ly/1YDIyie).
M	Malicious Software (Malware)	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. Source: Adapted from ISO/IEC 27032:2012
M	Monitoring	To determine the status of an activity, process, or system
M	Multi-Factor Authentication	The use of two or more of the following factors to verify a user's identity: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; -- biometric factor, "something that is a biological and behavioural characteristic of an individual". Source: Adapted from ISO/IEC 27040:2015 and ISO/IEC 2832-37:2017 (definition of "biometric characteristic")
N	Non-Disclosure Agreement (NDA)	A legal contract between at least two parties that outlines confidential material, knowledge or information on any restrictions on, or requirements for, its use.
N	Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. Source: ISO 27000:2018
O	Ongoing	An action or process that is recurring, that happens again and again, on a frequent basis
O	Operational Resilience	The ability of a Firm to: (i) maintain essential operational capabilities (resumption) under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of [sic] services (recovery). (IOSCO definition: http://bit.ly/1YDIyie).
P	Penetration Testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. Source: NIST
P	Physical Access	Physical access refers to the ability of individuals to physically gain access to a computer system
P	Policy	Formally documented management expectations and intentions
P	Privileged User	A user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform (NIST definition: http://bit.ly/1dIqXf5).
P	Protect (Function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents. Source: Adapted from NIST Framework
R	Recover (Function)	Develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired due to a cyber incident. Source: Adapted from NIST Framework
R	Recovery Point Objective (RPO)	The maximum target set for the period in which data might be lost which is usually informed by a business impact assessment
R	Reliability	Property of consistent intended behaviour and results. Source: ISO/IEC 27000:2018
R	Remediation	Process of correcting a fault or deficiency
R	Resilience	To identify, document, analyse and manage the resilience needs placed upon business services, and to ensure the delivery of these services meets those needs
R	Respond (Function)	Develop and implement the appropriate activities to take action regarding a detected cyber event. Source: Adapted from NIST Framework
R	Reviewed	An evaluation of a change, problem, process, project to ensure that all deliverables have been provided, and to identify opportunities for improvement
R	Risk	Combination of the probability of an event and its consequence.
R	Risk Assessment	Analysing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats
S	Second line Staff	Operational risk leads
S	Segregation (network)	Network segregation (also known as segmentation) is the act of splitting computer networks in to a number of smaller network segments with the intention to boost performance, minimise unneccessary traffic and improve security by creating barriers to restrict lateral movement
S	Senior Executives	NEDs, Board, senior management. Someone in a senior position in a business, who makes decisions and puts them into action.
S	Simulated Target Attack and Response (STAR)	Working alongside the Bank of England (BoE), Government and industry, CREST developed a framework to deliver controlled, bespoke, intelligence-led cyber security tests. STAR incorporates Penetration Testing and Threat Intelligence services to accurately replicate threats to critical assets. The STAR scheme is a prerequisite for membership of the BoE CBEST scheme, used to provide assurance to the most critical parts of the UK's financial services.
S	Situational Awareness	The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: CPMI-IOSCO
S	Social Engineering	A general term for trying to deceive people into revealing information or performing certain actions. Source: Adapted from FFIEC
S	Software	All or part of the programs, procedures, rules, and associated documentation of an information processing system
S	Staff	Includes all staff (temp, contractors, etc.)
S	Stakeholder Map	A document which determines the stakeholders in a particular task or activity and outlines their respective authority, relevance and importance
S	Systems	Servers, applications, network devices
T	Tactics, Techniques and Procedures (TTPs)	The behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. Source: Adapted from NIST 800-150
T	Third Party	A supplier of goods or support for a product or service, who is neither the primary vendor nor the purchaser
T	Third Party Provider(s)	A person, organisation or other entity that is not part of the service provider's own organisation and is not a customer – for example, a software supplier or a hardware maintenance company
T	Threat	Any possible intentional action or series of actions with a damaging potential to business services, including but not limited to; operations, the supply chain, society, economy or business continuity and integrity. (IOSCO definition: http://bit.ly/1YDIyie)
T	Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: NIST 800-150
T	Threat-Led Penetration Testing (TLPT) [also known as Red Team Testing]	A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. Source: G-7 Fundamental Elements
T	Traffic Light Protocol (TLP)	A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established colour code to indicate expected sharing boundaries to be applied by the recipient. Source: Adapted from FIRST
T	Training and Awareness	To raise awareness of desirable behaviours and develop the skills and knowledge of people in support of their roles in delivering business resilient services
T	Two Factor Authentication (2FA)	Two-factor authentication is a security process in which the user provides two means of identification when authenticating to an information system; one is typically a password and the other is typically a physical or electronic token
V	Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. Source: Adapted from CPMI-IOSCO and ISO/IEC 27000:2018
	Set intervals	