Cyber Risk Checklist - Protect

This Risk Maturity Self-Assessment has been developed by Interactive and Ansvar Insurance. It is founded on the 2018 NIST Cybersecurity Framework (CSF) with the addition of maturity levels and is intended to provide general information to assist your organisation in managing cyber-risks. This is not an exhaustive list.

The goal of the Maturity Level descriptions is to provide some guidance around what good practices look like. If, for example, you believe that a 5% policy exception rate is too high for a Level 3 maturity, feel free to change it to better suit your needs.

A 'Blank' response to any question indicates that further planning and investigation is required to effectively manage risk.

PLEASE TICK THE BOX THAT BEST REFLECTS YOUR ORGANISATIONS CYBER RISK MATURITY LEVEL

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	○	○	○	○	○	○
	Physical access to assets is managed and protected						
	Remote access is managed	○	○	○	○	○	○
	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties						
	Network integrity is protected (e.g., network segregation, network segmentation)	○	○	○	○	○	○

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Authentication and Access Control (continued)	Identities are proofed and bound to credentials and asserted in interactions						
	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)						
Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	All users are informed and trained						
	Privileged users understand their roles and responsibilities						
	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities						
	Senior executives understand their roles and responsibilities						
	Physical and cybersecurity personnel understand their roles and responsibilities						
Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data-in-transit is protected						
	Assets are formally managed throughout removal, transfers, and disposition						
	Adequate capacity to ensure availability is maintained						
	Protections against data leaks are implemented						
	Integrity checking mechanisms are used to verify software, firmware, and information integrity						

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Data Security (continued)	The development and testing environment(s) are separate from the production environment	○	○	○	○	○	○
	Integrity checking mechanisms are used to verify hardware integrity						
Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	A baseline configuration of information technology/ industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	○	○	○	○	○	○
	A System Development Life Cycle to manage systems is implemented						
	Configuration change control processes are in place	○	○	○	○	○	○
	Backups of information are conducted, maintained, and tested						
	Policy and regulations regarding the physical operating environment for organisational assets are met	○	○	○	○	○	○
	Data is destroyed according to policy						
	Protection processes are improved	○	○	○	○	○	○
	Effectiveness of protection technologies is shared						
	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	○	○	○	○	○	○

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Information Protection Processes and Procedures: (continued)	Response and recovery plans are tested	○	○	○	○	○	○
	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)						
	A vulnerability management plan is developed and implemented	○	○	○	○	○	○
Maintenance: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools						
	Remote maintenance of organizational assets is a pproved, logged, and performed in a manner that prevents unauthorized access	○	○	○	○	○	○
Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy						
	Removable media is protected and its use restricted according to policy	○	○	○	○	○	○
	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities						
	Communications and control networks are protected	○	○	○	○	○	○
	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations						

MATURITY LEVEL	Definition - (adapted from COBIT 2019 / CMMI capability levels)
Level 1 - Initial	Incomplete set of activities that are initial, intuitive, ad-hoc, in silos and/or not very organised. The full intent is not always achieved.
Level 2 - Basic	Basic yet complete set of activities that are not yet standardised and/or well documented.
Level 3 - Defined	Activities are documented and achieve their purpose in an organised, standardised way. Evidence can be provided for most activities but output is not always measured or tested.
Level 4 - Managed	Formal process exists and are well documented. Evidence can be provided for all activities, outputs are tested and performance is measured.
Level 5 - Optimising	Formal process exists and are well documented. Evidence can be provided for all activities and performance is measured to pursue continuous improvement.

ansvar
INSURANCE & RISK SPECIALISTS