Interactive®

ansvar
INSURANCE & RISK
SPECIALISTS

Cyber Risk Checklist - Identify

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 / IDENTIFY	MAYBE A BETTER WORD HERE SUBCATEGORY NOT VERY DESCRIPTIVE?	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Asset Management: The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy.	Physical devices and systems within the organisation are inventoried	○	○	○	○	○	○
	Software platforms and applications within the organisation are inventoried						
	Organisational communication and data flows are mapped	○	○	○	○	○	○
	External information systems are catalogued						
	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	○	○	○	○	○	○
	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established						

CATEGORY / IDENTIFY	MAYBE A BETTER WORD HERE SUBCATEGORY NOT VERY DESCRIPTIVE?	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Business Environment: The organisation's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The organisation's role in the supply chain is identified and communicated	○	○	○	○	○	○
	The organisation's place in critical infrastructure and its industry sector is identified and communicated						
	Priorities for organisational mission, objectives, and activities are established and communicated	○	○	○	○	○	○
	Dependencies and critical functions for delivery of critical services are established						
	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	○	○	○	○	○	○
Governance: The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Organisational cybersecurity policy is established and communicated						
	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	○	○	○	○	○	○
	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed						
	Governance and risk management processes address cybersecurity risks	○	○	○	○	○	○
Risk Assessment: The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals.	Asset vulnerabilities are identified and documented						
	Cyber threat intelligence is received from information sharing forums and sources	○	○	○	○	○	○
	Threats, both internal and external, are identified and documented						
	Potential business impacts and likelihoods are identified	○	○	○	○	○	○

CATEGORY / IDENTIFY	MAYBE A BETTER WORD HERE SUBCATEGORY NOT VERY DESCRIPTIVE?	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Risk Assessment (continued)	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk						
	Risk responses are identified and prioritized	○	○	○	○	○	○
Risk Management Strategy: The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by organisational stakeholders						
	Organisational risk tolerance is determined and clearly expressed	○	○	○	○	○	○
	The organisation's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis						
Supply Chain Risk Management: The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has established and implemented the processes to identify, assess and manage supply chain risks.	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders	○	○	○	○	○	○
	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber-supply chain risk assessment process						
	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation's cybersecurity program and Cyber Supply Chain Risk Management Plan.	○	○	○	○	○	○
	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.						
	Response and recovery planning and testing are conducted with suppliers and third-party providers	○	○	○	○	○	○

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.

The content contained this document is of general nature and does not constitute legal, financial or personal advice. Before using this information, you should consider the appropriateness of it having regard to your own business objectives, needs and individual circumstances. To the extent permitted by applicable law Ansvar expressly disclaims all liability howsoever arising from this publication whether in contract, tort or otherwise (including, but not limited to, liability for any negligent act or omission) to any person in respect of any claims or losses of any nature including direct, indirect, incidental or consequential loss, punitive damages, penalties or costs.