Cyber Risk Checklist - Respond

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
Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Response plan is executed during or after an incident	○	○	○	○	○	○
Communications: Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Personnel know their roles and order of operations when a response is need						
	Incidents are reported consistent with established criteria	○	○	○	○	○	○
	Information is shared consistent with response plans						

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Communications: (Continued)	Coordination with stakeholders occurs consistent with response plans	○	○	○	○	○	○
	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness						
Analysis: Analysis is conducted to ensure effective response and support recovery activities.	Notifications from detection systems are investigated	○	○	○	○	○	○
	The impact of the incident is understood						
	Forensics are performed	○	○	○	○	○	○
	Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)						
Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents are contained	○	○	○	○	○	○
	Incidents are mitigated						
	Newly identified vulnerabilities are mitigated or document as accepted risks	○	○	○	○	○	○
Improvements: Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans incorporate lessons learned						
	Response strategies are updated	○	○	○	○	○	○

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