Cyber Risk Checklist - Recover

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.	Recovery plans are executed during or after a cyber-security incident	○	○	○	○	○	○
Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans are incorporated lessons learned						
	Recovery strategies are updated	○	○	○	○	○	○

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Public relations are managed						
	Reputation is repaired after an incident						
	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams						

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