

# Cyber Risk Checklist - Detect

*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
<b>Anomalies and Events:</b> Anomalous activity is detected and the potential impact of events is understood.	A baseline of network operations and expected data flows for users and systems is established and managed						
	Detected events are analysed to understand attack targets and methods						
	Event data are collected and correlated from multiple sources and sensors						
	Impact of events is determined						
	Incident alert thresholds are established						

CATEGORY	SUBCATEGORY	LEVEL 0 INCOMPLETE	LEVEL 1 INITIAL	LEVEL 2 BASIC	LEVEL 3 DEFINED	LEVEL 4 MANAGED	LEVEL 5 OPTIMISING
<b>Security Continuous Monitoring:</b> The information systems and assets are monitored to identify cyber-security events and verify the effectiveness of protective measures.	Data-at-rest is protected						
	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						
	The development and testing environment(s) are separate from the production environment						
	Integrity checking mechanisms are used to verify hardware integrity						
<b>Detection Processes:</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Roles and responsibilities for detection are well defined to ensure accountability						
	Detection activities comply with all applicable requirements						
	Detection processes are tested						
	Event detection information is communicated						
	Detection processes are continuously improved						

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

© 2022 Ansvar Insurance Limited (ABN 21 007 216 506 AFSL No 237826) of Level 5, 1 Southbank Boulevard, Southbank VIC 3006 (Ansvar). Ansvar is a member of the Benefact Group in the UK (formally known as Ecclesiastical Group). All rights reserved, except as permitted by the Copyright Act 1968, no reproduction or communication of any of the content of this document may occur without the permission of Ansvar.

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.