









E. Cyber response and recovery governance checklist

Those charged with governance (such as executive management, boards, and councillors) of public sector entities, including local governments, have an important role to play in cyber response and recovery effectiveness. This includes, but is not limited to:














- confirming entities are well prepared prior to incidents occurring
- seeking updates and supporting management during an event
- contributing to key decisions such as when to seek external assistance, when to shut down and contain systems, when to then restore, and how to handle ransom demands if they are made
- endorsing escalation points and internal and external communications
- endorsing reporting to relevant authorities (for example, to CSU and/or the Australian Cyber Security Centre), depending on the incident and the requirements.

We have created a checklist of key questions for those charged with governance of public sector entities to consider with respect to cyber security incident response and recovery.

Figure E1
Cyber response and recovery governance checklist

Area	Detailed question	Have we considered?
Clarify compliance requirements	Are we required to comply with the Queensland Government’s IS18:2018 information security policy? If not, should we voluntarily adopt it?	
	Should we be ISO 27001-certified for all our key systems that have significant cyber risk? What do we need to improve to be certified?	
Determine adequacy of strategies and plans	When did we last test our entity’s incident response policies, plans, and procedures against best practice frameworks? Who was involved, what did we learn, and did we implement all the lessons learnt?	
	Have we identified all of the critical systems and information assets our entity holds that are susceptible to the risk of being exploited? Are they captured within our plans?	
	What scenarios has management tested incident response policies, plans, and procedures against? Are there other scenarios that we need to consider?	
	Have we integrated our cyber risk management, disaster recovery, business continuity, and information asset management processes, at both the organisational and whole-of-government levels (if applicable)?	
Clarify communication plans and reporting obligations	Does management have communication plans with prepared, consistent, and endorsed templates for a range of cyber scenarios that cater for internal and external stakeholders?	
	Are we clear on our escalation points within our incident response plans and on our reporting obligations during an event?	



Area	Detailed question	Have we considered?
	Do we have an alternative communications channel in the event email and telephone services are not available during the incident?	
Build or access capabilities needed to respond and recover	Have we done an assessment of the capabilities and toolsets our entity needs to respond to and recover from cyber incidents?	
	Based on that assessment, how well placed is our information technology team to respond to and recover from cyber incidents? Does management have a workforce plan to acquire or have access to the required skillsets and capabilities for cyber incident response and recovery?	
	What percentage of the required capabilities is internal versus external? Have we tested the external capabilities?	
Obtain assurance over third-party arrangements	How have we gained assurance that cyber security controls within outsourced management information systems and assets are operating effectively?	
	Have we tested our third-party arrangements for external capabilities to ensure that they will be available, familiar with our information system environments, and have the capabilities we require in a time of need?	
Develop a cyber-resilient culture	What mandatory training, penetration testing (simulated cyber attacks), phishing email testing, and other cyber resilience activities is management performing to raise awareness?	
	Are we contributing to and taking advantage of shared cyber threat intelligence and cyber incident learnings within the sector?	
Use existing public sector cyber expertise	How are we taking advantage of existing public sector cyber expertise (such as the Australian Cyber Security Centre and the Queensland Government Cyber Security Unit) and other entities within the sector to contribute to, promote, and share cyber threat intelligence?	
	Can our entity benefit from partnering with other public sector entities for collective research, investments, and buying power for cyber incident response technology, capabilities, and cyber insurance?	
Clarify cyber insurance details	Do we have cyber insurance and what is included? Are ransoms or extortion threats included or excluded from the policy?	
	At what stage in an incident response do we have to notify the insurer? Do we have to use the insurer's panel of nominated cyber consultants?	
	If the insurance policy specifies that we must use its panel of cyber consultants, have we tested working with them? Are they familiar with our information technology environment?	

Source: Queensland Audit Office.