# F. Role capability checklist

In Chapter 4, we discussed the need for entities to undertake assessment of cyber capability. We have provided an example framework modelled after the people, processes, technology (PPT) framework and the key technical and non-technical capabilities required for cyber incident response and recovery. The framework is based on the work of Bruce Schneier, who is an academic and a world expert on cyber security.

The PPT framework helps build systems that effectively balance and coordinate how people, processes, and technology support each other. All 3 elements need to work for effective cyber incident response and recovery. If one aspect is weak or not aligned with the others, it can affect the overall efficiency and effectiveness of the cyber response.

The table below can be used by entities to map where they do or do not hold relevant capabilities across their people, processes or through technology. Entities should also understand whether these capabilities are internal or external, and when they were last tested. Definitions for each of the below capability areas are included in Figure F2.

**Figure F1**
**Role capability checklist using the people, processes, technology framework**

| Team | Capability area | Internal/ external | People | Process | Technology |
|---|---|---|---|---|---|
| Non-technical related teams | Communications | | | | |
| | Crisis management | | | | |
| | Executive leadership team and/or those charged with governance | | | | |
| | Human resources | | | | |
| | Incident response officer | | | | |
| | Legal | | | | |
| | Privacy and data governance | | | | |
| Information and communications technology teams | Applications | | | | |
| | Cloud | | | | |
| | Endpoints and infrastructure | | | | |
| | Identity access management | | | | |
| | Network | | | | |
| | Operating system | | | | |
| | Service desk | | | | |
| Specialised technical teams | Cyber threat intelligence | | | | |
| | Digital forensics | | | | |
| | Operational technology | | | | |
| | Penetration testing | | | | |
| | Physical security | | | | |
| | Security operations centre | | | | |

*Source: Queensland Audit Office based on Bruce Schneier's people-process-technology framework.*

## Figure F2
## Capability area definitions

| Term | Definition |
|---|---|
| Communications team | The communication team's role in incident response is to communicate information related to the cyber incident to the organisation's employees, customers, suppliers, media, and the public. It is responsible for having adequate, consistent communication means available and for being transparent with external and internal stakeholders. The communications team usually works closely with the human resources team and legal team to save and restore trust in the entity. |
| Crisis management team | The crisis management team (CMT) or cyber incident response team (CIRT) is a team of professionals that are adept in disaster management, situational analysis, coordination, and response planning for extreme cyber events.<br>In an extreme event, the CMT/CIRT becomes responsible for coordinating and managing an entity's responses. The composition of a CMT/CIRT varies based on an entity's size and available skills and resources (including third-party vendors that either manage ICT systems/applications or external incident response providers). |
| Executive leadership team and/or those charged with governance | Significant cyber incidents may require the formation of the executive leadership team (ELT) and/or those charged with governance (TCWG) to provide strategic oversight, direction, and support to the CMT, with a focus on:<br>• identifying and managing strategic issues<br>• engaging and communicating with stakeholders (including the board, councillors, and ministerial liaison, if applicable)<br>• managing resource and capability demand (including urgent logistics or finance requirements and human resources considerations during the response effort).<br>The composition and roles of the ELT or TCWG may vary depending on the incident impacts and size and structure of the organisation and the required experience for decision-making. |
| Human resources team | Human resources, in the context of incident response, assist in matters concerning insider threats (see 'insider privilege abuse' in Appendix G) or other human aspects of a cyber incident. This could include data exposure of employees, handling interviews with employees, and managing staff surge capacity and wellbeing in the prolonged event. |
| Incident response officer | A cyber security expert with the skills to rapidly address cyber security incidents within an organisation. In the role of a first responder, they use a host of tools to find the root cause of a cyber security incident, limit the damage, and significantly reduce the likelihood of it occurring again. |
| Legal team | Legal counsel or legal teams may be required in incident response scenarios to understand potential legal ramifications or compliance obligations, such as breaches in privacy legislation. Legal officers are also often involved with the administration of insurance for entities. |
| Privacy and data governance team | The team responsible for maintaining a digital asset (or data asset) inventory detailing where data is situated, what category of data is related to a specific location, and what the encryption level is. If an incident involves data, the privacy and data governance team is responsible for understanding any business risks and privacy risks related to this data, and for handling such risks. |
| Applications | An application is a software program or group of software programs designed for end users. Examples of an application include a word processor, a spreadsheet, an accounting application, a web browser, or an email client. This contrasts with system software, which is mainly involved with running the computer. |

| Term | Definition |
|---|---|
| Cloud | Cloud computing is a model for enabling, convenient, on-demand network access to a shared pool of computing resources (for example networks, servers, storage, applications, and services) that can be rapidly configured and released with minimal management. |
| Endpoints and infrastructure | A personal computer, personal digital assistant, smart phone, or removable storage media (for example a USB flash drive or external hard drive) that can store information. All these endpoints communicate through the network server – a computer that provides services to users or other systems, for example a file server, email server, or database server. |
| Identity and access management | The process used in businesses and organisations to grant or deny employees and others authorisation to secure systems. |
| Network | The infrastructure used to carry information between workstations and servers or other network devices. |
| Operating system | System software that manages hardware and software resources and provides common services for executing various applications on a computer. |
| Service desk | Service desk teams respond to minor or moderate incidents and maintain communication with users and stakeholders. They use their service management platform to assist in following adequate processes, triaging and documenting the incident, and maintaining contact with end users who are reporting incidents. |
| Cyber threat intelligence | Information that helps organisations better protect against cyber incidents by providing an understanding of current and emerging threats and vulnerabilities. It can incorporate recent threat actor behaviours, and successful remedial procedures, tools, and techniques. |
| Digital forensics | Capabilities that enable incident responders to investigate the source, entry point, and extent of a cyber incident or data breach. |
| Operational technology (OT) team | A team of specialists that understand data from operational technology (programmable systems or devices that interact with the physical environment) monitoring solutions, assist with reconfiguring or rerouting OT equipment, and understand software related to the OT environment. The OT team maintains an updated and precise inventory of asset specifications (for example IP addresses and data flow) and physical location. It is also tasked with backing up systems and maintaining disaster recovery versions. |
| Penetration testing | Simulated cyber attacks to evaluate the security of a system and identify its exploitation risks to gain access to systems and data. |
| Physical security | Physical security, in the context of incident response, physically secures information assets and systems by making them inaccessible. The information assets could include swipe card access for lockable doors, security cameras monitored by a security team, or lockable cabinets for paper records. |
| Security operations centre (SOC) | The focal point for security operations and computer network defence for an organisation. The SOC defends and monitors an organisation's systems and networks (that is, cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analysing, and responding to cyber security incidents in a timely manner. This may not be located within an organisation. |

*Sources: Queensland Audit Office from Australian Signals Directorate and the National Institute of Standards and Technology.*