Connect › Support › Advance

The Institute of Internal Auditors Australia

The 20 Critical Questions Series

What Directors should ask about Information and Cyber Security

Updated 2022

Information and Cyber Security Foundations

1. Is the organisation 'cyber ready' at all times OR is there increased board, audit committee and management scrutiny on information and cyber security every time there is a publicised ICT security incident?
2. Does the organisation have a specific suitably qualified senior person responsible for information and cyber security? Does the organisation have a senior level ICT committee?
3. Is there an integrated 3 Lines Model approach to assurance activities over information and cyber security? Are there up-to-date policy and procedures in place that provide an effective framework for information and cyber security? Is there an approved information classification system that is consistently applied for security and also privacy obligations?
4. Is inappropriate or illegal use of ICT assets featured in the organisation code of conduct as a violation that attracts sanctions? Does the organisation have a 'hotline' to report ICT and cyber security incidents?
5. Is there a defined and controlled policy for ICT procurement? Does the organisation dispose of old and obsolete ICT assets in a secure and timely manner?

Risk and Threat Assessment

6. Does the organisation's enterprise risk management include cyber threats and monitoring procedures?
7. Does the organisation have a clear understanding of what the big ICT risks are? Is there a list of vulnerable ICT assets? Does this consider such things as supervisory control and data acquisition (SCADA) systems and the Internet of Things?
8. Has the organisation applied a risk-based approach to identify its most important ICT assets and what it needs to protect? Does this include (a) infrastructure (b) hardware (c) network (d) software (e) specific data?
9. Has an ICT threat risk assessment been performed? Have improvements been identified and a risk-based triage approach taken to implementation? Are responsibilities for implementation assigned, actively tracked and reported upward to the top level of the organisation including the audit committee and board?

ICT Infrastructure

10. Is it clear what technical infrastructure the organisation information resides on? Is it clear what is stored in-house and what is not? Where required, is data only stored in Australia and not overseas? How does the audit committee and board get assurance of this?
11. Is there a standard operating environment with rules around who can approve non-standard infrastructure, hardware and software? Is there an up-to-date register of all infrastructure, hardware and software? Are there regular audits to identify any non-standard items installed in contravention of the standard operating environment policy? Is there a standard security configuration?

ICT Access

12. Is there an ICT user privileges matrix built around specific job roles? Is this regularly reviewed to provide assurance the privileges that people have remain what they need to do their job? Does this happen promptly when people change jobs or leave the organisation? Is there a process to immediately revoke out-of-date privileges?
13. Is there layered security measures and effective controls over employee remote access to the organisation ICT environment? Is access limited to use of organisation ICT assets and not permitted on personal and home computing for work purposes?
14. Have information and cyber security policy and procedures been effectively disseminated and people trained in their use? Does this include board members, management, employees, contractors, consultants and suppliers? Does this include initial training and regular refresher training?

Disaster Recovery

15. Is information and cyber security covered in an ICT disaster recovery plan? Is there a response team available to rapidly respond to incidents? Is there an escalation process for incident response to keep management, employees and stakeholders informed when an incident gets progressively worse or takes a long time to fix?
16. Does the organisation have a priority list for restoration of ICT services following an incident? Is there regular testing to provide assurance recovery can be achieved within (a) acceptable timeframes (b) acceptable loss of data?

What Directors should ask about Information and Cyber Security

Monitoring and Reporting

17. Is there robust layered monitoring of the ICT environment to detect (a) internal improper or illegal activity (b) external penetration attempts (c) denial of service attacks? Are cyber security attempts and breaches formally reported and investigated? Is there independent review? Are these reported to senior management, audit committee and the board in a timely way?
18. Is inappropriate access outside predetermined parameters monitored through consistent Line 2 assurance arrangements and also periodic Line 3 internal audit coverage? Are sanctions imposed on employees and contractors who access information inappropriately or illegally outside their authorised access privilege limitations? Is there a defined process to deal with ICT security violations?
19. Are regular reviews and audits of information and cyber security arrangements performed and reported to senior management and the audit committee? Does this include regular penetration testing?
20. Has organisation compliance with standards and good practice information and cyber security principles been formally assessed or audited? Have results been reported to senior management and the audit committee?

The Big Question

How does the organisation know it can be confident it has an effective ICT control environment that will not be compromised?

The answer to this is:

- Good governance
- Complete inventory of ICT assets – infrastructure, hardware, network, software, data
- Routine risk identification, analysis and evaluation
- Standard security configurations
- Robust access management
- Prompt response and remediation
- Ongoing monitoring
- Breach reporting
- Manage resolution and close-out incidents

Definitions

Cyber Security – Protection of internet-connected systems and data from cyber threats to protect against unauthorised access.

ICT – A term used to holistically include information, communication and technology (ICT) related matters within an organisation – used interchangeably with the simpler abbreviation IT (information technology).

Information Security – Is concerned with protecting information and ICT systems from unauthorised access, use, disclosure, disruption, modification, or destruction.