The Institute of Internal Auditors Australia

The 20 Critical Questions Series

What Directors should ask about Information Management

Updated 2022

Information Management Foundations

1. Does the organisation have an approved framework for information management? Does this include a consistent document hierarchy and suite of documents that is mandated across the organisation?
2. Does the organisation know what information they have and is this documented in an information inventory?
3. Has the organisation formally assessed information management risk and remediated identified exposures? Is information linked to threats?
4. Does the organisation have a specific senior person responsible for information management? Does the organisation have a senior level information management committee or is this topic actively considered as part of another senior level committee?
5. Does the organisation have an approved information management plan? Is there an adequate budget to effectively manage the organisation's information and to remediate risks?
6. Is it clear what technical infrastructure the organisation's information resides on? Is it clear what is stored in-house and what is not?

Information Management Controls

7. Does the organisation comply with its legal and regulatory information management and protection obligations? Where required, is data only stored in Australia and not overseas? How does the board and audit committee know there is compliance?
8. Is there an approved information classification system that is consistently applied for security and also privacy obligations?
9. Is there approved information management policy and procedures in place that have been disseminated to employees and contractors? Are there limitations on what information employees and contractors can access according to an approved access privileges matrix? Are information management requirements built-in to employee job descriptions and contractor contracts?
10. Are inappropriate accesses outside predetermined parameters monitored through consistent Line 2 control arrangements or as part of Line 3 internal audit coverage? Are sanctions imposed on employees and contractors who access information outside their authorised access limitations?

Information Management Continuity

11. Is unforeseen release or loss of information covered in the ICT disaster recovery plan or business continuity plan? Is there a media plan to deal with the media following an unforeseen release or loss of information?

ICT Intrusion Attempts, Data Breaches and Data Spills

12. Are there effective and tested processes in place to detect ICT intrusion attempts, data breaches and data spills? Is an up-to-date record of these kept and is there regular follow-up to ensure appropriate action is taken in a timely way?
13. Are there formal processes in place for timely response to intrusion attempts, data breaches and data spills, and is this swiftly reported to senior management and the audit committee?
14. Are there competent investigation resources readily available to investigate intrusion attempts, data breaches and data spills and to rapidly remediate exposures and risks?

Information Management Review and Audit

15. Is there an integrated 3 Lines approach to assurance activities over information management including unauthorised access?

What Directors should ask about Information Management

16. Has organisation compliance with good practice information management principles been formally assessed or audited and does this include cybersecurity and adherence to privacy principles.
17. Are regular reviews and audits of information management arrangements performed and reported to senior management and the audit committee? Does this include regular penetration testing?

Information Management Reporting

18. Are information breaches and attempts formally reported and investigated, and are these reported to senior management and the audit committee in a timely way?
19. Are there processes in place for information to be effectively used for business improvement and business intelligence purposes?
20. Are there performance measures in place to provide assurance of effective information management, and are results reported to senior management and the audit committee in a timely way?

The Big Question

How does the organisation know it can be confident its information is effectively managed and protected and there is compliance with legal and regulatory obligations?

Definitions

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

Data Breach – Unauthorised access to data from outside the organisation.

Data Spill – Accidental or deliberate exposure of information into an uncontrolled or unauthorised environment or to people without a need-to-know – also called 'information disclosure' or 'data leak'.

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 Management – Acquisition, custodianship, distribution, use and archiving or deletion of information in electronic or hard copy format.

Information Privacy – Collection, use and disclosure of personal information, and the rights of individuals to access their personal information.