Connect › Support › Advance

The Institute of Internal Auditors Australia

Session 6
Auditing Information Security

Presented by

Shannon Jurkovic
Chief Information Security Officer
Bendigo and Adelaide Bank

Nick Kazimierczak
Head of Group Assurance
Bendigo and Adelaide Bank

Info Security Fundamentals

The Institute of Internal Auditors Australia

1st important framework… the C-I-A triad

- Confidentiality
- Integrity
- Availability

Info Security Fundamentals

The Institute of Internal Auditors Australia

2nd important framework… the Holistic Approach

- People
- Process
- Technology
- Governance
- Culture

Risks: Appetite and Tolerance

The Institute of Internal Auditors Australia

The risk landscape

- External threats and internal risks
- Consider the top 3-5 risks that keep you awake! Those that when they go take hold will have terrifying consequences…
- Describe them at a high / strategic level

Risks: Appetite and Tolerance

The Institute of Internal Auditors Australia

The risk landscape: potential key IS risks

1. Loss or compromise of critical technology assets and / or sensitive, confidential and / or business critical information within the IT environment
2. Loss or compromise of sensitive, confidential and/or business critical information through a third party or third-party service
3. Failure to detect and respond to cyber security incidents in a timely manner resulting in compromise of system(s) and/or data
4. Staff lack awareness and understanding of their role and responsibilities in protecting critical and sensitive data and information
5. Leadership fails to fulfil their obligation for overall accountability of information security, through inadequate visibility of threats and risks to technology assets

Risks: Appetite and Tolerance

The Institute of Internal Auditors Australia

Risk appetite and risk tolerance

- Appetite: per ISO 31000 “the amount and type of risk that an organisation is prepared to pursue, retain or take.”
- Risk tolerance: reflects the acceptable level of variation around a particular set of risk-based objectives.

Risks: Appetite and Tolerance

The Institute of Internal Auditors Australia

Risk appetite and risk tolerance

- Both Appetite and Tolerance should be captured in the Risk Appetite Statement (RAS) - defines Key Risk Indicators (KRIs) mapped to risks
- Critical that the above has a direct link to the organisation's strategy…. If this link fails…

Info Security Scenarios

The Institute of Internal Auditors Australia

Scenario # 1: Ransomware

- Access to IT assets is compromised where malicious software encrypts files and the attacker demands a ransom for access to be reinstated (often via bitcoin)
- Important to be prepared for these types of attacks and know how to respond and recover

Info Security Scenarios

The Institute of Internal Auditors Australia

Scenario # 2: Phishing

- Malicious email / text messages sent to a target with the goal for the target to share personal information or important security information (user IDs, passwords) to be used for cyber attacks
- These emails are designed to look real and be very deceptive… *They can be hard to spot!*

Info Security Scenarios

The Institute of Internal Auditors Australia

Scenario # 2: Phishing

- Need to prevent them breaching the organisation's defences (inbound email security) and…
- Ensure that staff are repeatedly trained to spot and **report** phishing attacks

Info Security Scenarios

The Institute of Internal Auditors Australia

Scenario # 3: 3rd party providers

- 3rd parties can be the ‘weakest link’ in the IS chain. Cyber criminals know this and **will** exploit this
- Make your expectations to 3rd parties clear and ensure captured in contractual agreements
- Undertake regular 3rd party IS maturity and capability assessments

Reporting and Monitoring

The Institute of Internal Auditors Australia

Reporting to stakeholders

- Transparency and trend analysis key
- Must reference risk appetite, tolerance and KRIs
- KRIs should ideally have Green, Amber and Red ranges (Amber = approaching limit, Red = breached limit)

Info Security Frameworks

The Institute of Internal Auditors Australia

Common industry frameworks

- NIST Cybersecurity
- ISO 27001 (Information Security) and ISO 27002 (Information Technology)
- SOC 2 Audit Framework

Info Security Frameworks

The Institute of Internal Auditors Australia

Common regulatory frameworks

- APRA's CPS 234 Information Security
- ACCC's Consumer Data Right regime (CDR)
- Payment Card Industry Data Security Standard (PCI DSS – anyone that processes credit cards)
- Changes to Critical Infrastructure Act

From IS Risk Owner to IA

The Institute of Internal Auditors Australia

Value of Internal Audit (to the Risk Owner!)

- Regular and independent execution of…
- **Control** design and operating effectiveness testing over…
- The full population of risks, that yields…
- Reporting with robust action follow-up.

Info Security IA controls testing

The Institute of Internal Auditors Australia

Key controls to focus upon

- Accuracy and completeness of information asset classification process
- Identity and logical access management
- Privileged account logical access management
- Physical access management

Info Security IA controls testing

The Institute of Internal Auditors Australia

Key controls to focus upon

- Use of separate environments for test and production systems
- Logical access controls over promotion of data from test to production
- Data protection and recovery testing

Info Security IA controls testing

The Institute of Internal Auditors Australia

Key controls to focus upon

- Inbound email security (phishing protection)
- Culture of security awareness
- Regular scans performed by IS risk owners to refresh vulnerability assessments
- Formal 3rd party IS monitoring / assessments

Info Security IA controls testing

The Institute of Internal Auditors Australia

Key controls to focus upon

- Restrictions over use of personal cloud based services and USB / external storage on IT assets
- Segregation of duties to ensure no conflict (real *or* perceived)
- Encryption (policies, procedures and practices)

Info Security IA controls testing

The Institute of Internal Auditors Australia

And finally….

- Monitoring and reporting over all these controls

Info Security IA controls testing

The Institute of Internal Auditors Australia

Info security internal audit techniques

- Traditional sample based approach to test controls, but also, develop with an eye to build….
- ….*continuous* controls monitoring on *full data population* using thresholds that derive *exceptions* for investigation (which *link* back to the *KRIs* based on the *RAS*)

Info Security IA controls testing

The Institute of Internal Auditors Australia

Info security internal audit techniques

- Penetration testing
- Behavioural audits
- Data lineage testing (using data analytics)
- Logical access testing at both network level and application level

Building Info Security into IA

The Institute of Internal Auditors Australia

Testing skills to recruit / develop in your teams

- IT general controls (don't forget the basics!)
- IT application controls
- Identity access controls
- Vulnerability and patch management

Building Info Security into IA

The Institute of Internal Auditors Australia

Testing skills to recruit / develop in your teams

- Awareness of control environments / capabilities / weaknesses of various operating systems and Cloud environments
- Data extraction and analysis (SQL, Alteryx)
- Visualisation tools (PowerBI, Tableau, Qliksense)
- Project Management

Building Info Security into IA

The Institute of Internal Auditors Australia

Prioritising info security on the IA plan

- Regular interaction with owners of IS risks
- Build a dedicated IS plan within your IA plan – and ensure coverage over key risks in a given time period (3 years) via a rotation plan
- Have owners of IS risks with you when presenting IS IA reports to your Audit Committee

Auditing Information Security

The Institute of Internal Auditors Australia

In conclusion

- Ensure your risk landscape is documented by risk owners, with a RAS and tolerances clearly defined + KRIs + reporting
- Audit the control environment surrounding the monitoring of the above
- Connect IS risk owners with the Audit Committee!