Comptroller and Auditor General

Information Security: Summary Report

18 June 2015

JERSEY AUDIT OFFICE

Information Security: Summary Report

Background

1.1 Information is at the heart of the operation of any organisation – including the States of Jersey. But the information has to be held securely because:

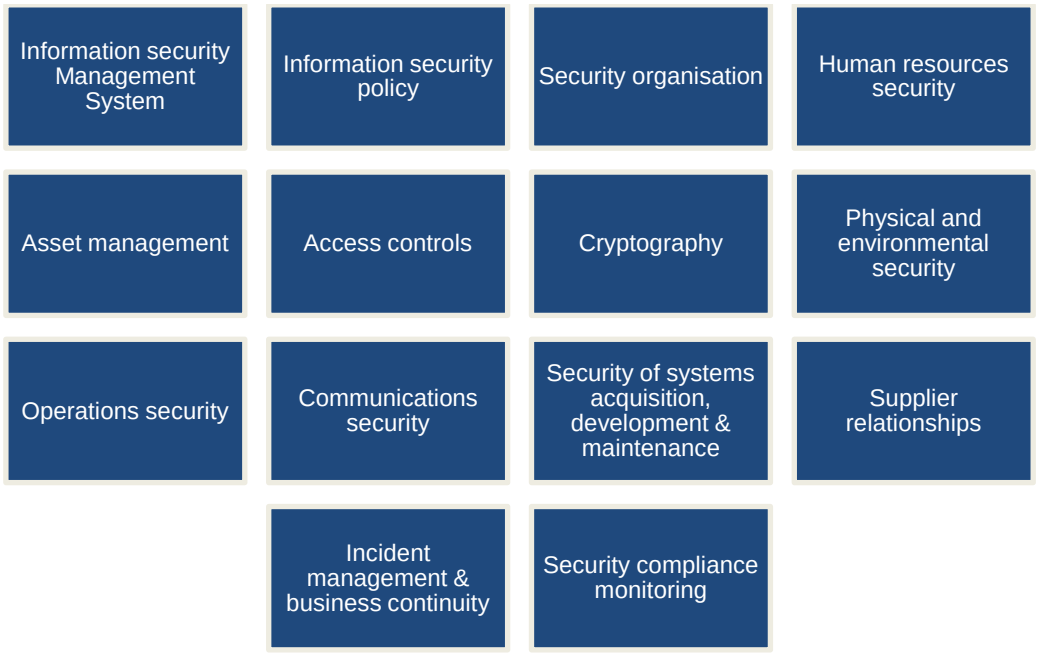
- it is important for the effective management of the States;
- much of it is sensitive, such as personal information;
- some of it is commercially confidential;
- some of it is legally privileged;
- the States have a legal obligation to disclose some information; and
- the States have a legal duty not to disclose other information.

1.2 The growing use of the internet has given rise to increased and new threats to information security, including:

- serious organised crime using the internet to steal personal or financial data to commit fraud, steal corporate intellectual property, or launder money;
- political activists hacking and using the internet to steal information or damage computer systems to serve political agendas; and
- state supported espionage and attacks on critical government infrastructure.

1.3 There are recognised international standards for data security covering both information security management systems and security techniques (see Exhibit 1).

Exhibit 1: Scope of ISO27001 Information Security Management Systems and ISO27002 Security Techniques



Scope and objectives of this review

2.1 The review focussed on identifying and evaluating the corporate approach to information security across the States and within a sample of Departments.

2.1 The United Kingdom National Audit Office (NAO) provided technical support for this review.

2.3 Detailed findings and recommendations in these areas have been reported to and accepted by management. I will follow up recommendations from this report and the more detailed report in 2016.

Key findings

3.1 The approach to information security within the States of Jersey is not fully formed. Departments see information security as primarily a technical issue: one department did not see it as a concern for it at all. Even those departments that recognise they have a responsibility for information are approaching it principally from a Freedom of Information approach as opposed to a robust information security approach.

3.2 The information security policies developed by the Information Services Department (ISD) are IT-centric and do not cover the full range of information security-related activities. Coupled with a lack of specific awareness training, the policies have reinforced the view that information security is the responsibility of ISD.

3.3 Across both ISD and the departments there is very little documented understanding of information security threats, vulnerabilities and mitigating actions. Even where departments are dealing with third parties and possibly exchanging large amounts of potentially sensitive information little consideration of information security threats is evident.

Conclusion

4.1 The States of Jersey are embarking on an ambitious reform programme, re-engineering the way services are delivered, and an ambitious e-government programme. Changes to ways of working, changes to information systems, outsourcing and increased use of the internet increase the risks of information security breaches. Against this background the States need to be confident that:

- a new, inclusive and corporate approach to information security is adopted so that information security is embedded in ways of working throughout the States; and
- sufficient appropriate skills and resources are in place to manage the threats and vulnerabilities.

Key recommendations

R1 Establish clear responsibilities for information security both corporately and in individual departments, supported by appropriate job descriptions, objectives and training.

R2 With the support of suitable expertise, complete detailed corporate and departmental information security risk assessments covering the topics in relevant international standards, identifying threats, vulnerabilities and the quality of countermeasures.

R3 Ensure adequate qualified security resources are available to assess and address security risks including those arising from the e-Government programme.

KAREN McCONNELL
COMPTROLLER AND AUDITOR GENERAL

JERSEY AUDIT OFFICE, LINCOLN CHAMBERS (1ST FLOOR), 31 BROAD STREET, ST HELIER, JE2 3RR
T: 00 44 1534 716800 E: enquiries@jerseyauditoffice.je W: www.jerseyauditoffice.je