JERSEY AUDIT OFFICE

Critical Infrastructure Resilience – Cyber Security

Audit Specification

Background

National Infrastructure are those facilities, systems, sites, information, people, networks and processes necessary for a jurisdiction to function and upon which daily life depends.

Not everything within a national infrastructure sector is judged to be 'critical'. Jersey's critical infrastructure can be described as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Jersey or affect Jersey's ability to ensure national security.

There are broadly twelve sectors that could be considered to be critical infrastructure for Jersey as shown in Exhibit 1.

Exhibit 1: Jersey's critical infrastructure sectors

• Chemicals	• Energy	• Space
• Communications	• Finance	• Transport
• Defence	• Food	• Waste
• Emergency Services	• Health	• Water

Critical infrastructure systems within these sectors are particularly vulnerable to being damaged or disrupted.

Ensuring the security and resilience of Jersey's critical infrastructure is a responsibility shared by the States, infrastructure owners and operators. Each have different responsibilities for critical infrastructure depending on the system and/or the nature of the threats to be mitigated. Responses to a threat can involve the asset owner and operator, the technical and operational lead for Government and emergency services or law enforcement. Co-ordination among entities is therefore required to prepare, rehearse and respond to critical infrastructure threats.

Cyber resilience is the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them. Critical infrastructure systems are prime targets for cyber-attacks due to their vital role in society. Potential cyber security threats do not just affect data and systems in government and business, but also critical infrastructure, including emergency services, energy, health, transport and water.

In October 2017, the Government published its Cyber Security Strategy. The Strategy is centred around the following five pillars:

1. Government: Continuously secure Government's information.
2. Critical national infrastructure: Strengthen the critical national infrastructure's cyber resilience.
3. Business: Work in partnership with the private sector to encourage and incentivise improved cyber security across the Island's businesses.
4. Legislation and international engagement: Ensure the appropriate legislation is in place on-Island and engage with the international community to enhance cooperation.
5. Citizens: Help ensure people in Jersey are secure online by raising awareness, building cyber skills, knowledge and capability.

To protect the Island, there is a need for Government to work with the private sector and the operators of critical national infrastructure. In addition, there is a need for Government to have robust cyber security arrangements over its own operations.

The Jersey Cyber Security Centre (JCSC) was established in 2021 to promote and improve the Island's cyber resilience. It operates on an arm's length basis from Government.

The Government of Jersey has invested and is investing in a cyber security programme focussed on Government of Jersey IT systems and related infrastructure to improve its own arrangements. Exhibit 2 summarises the actual and committed expenditure on the cyber security programme within Government.

Exhibit 2: Expenditure on Government's cyber security programme

	Actual expenditure 2020 to 2024 £000	Budgeted expenditure 2025 to 2028 £000	Total actual and committed expenditure £000
Cyber Security Programme	12,989	10,171	23,160

Source: States of Jersey Group Annual Report and Accounts 2020-2024 and Budget 2025-2028

In May 2022 I published a report on *Cyber Security Arrangements* which focussed on the Government's cyber security programme at that time.

The States are due to debate a new draft Cyber Security Law during 2025.

The Functions of the Comptroller and Auditor General (C&AG)

Article 11 of the Comptroller and Auditor General (Jersey) Law 2014 requires the C&AG to:

- provide the States with independent assurance that the public finances of Jersey are being regulated, controlled, supervised and accounted for in accordance with the Public Finances (Jersey) Law 2005
- consider and report to the States on:
    - the effectiveness of internal controls of the States, States funded bodies and funds
    - the economy, efficiency and effectiveness in the way the States, States funded bodies and funds use their resources; and
    - the general corporate governance arrangements of the States, States funded bodies and funds; and
- make recommendations to bring about improvement where improvement is needed.

Objectives of this review

The audit's overall objective is to assess whether the Government has an effective approach to cyber resilience.

Scope

The scope of the audit will include:

- the Government's cyber security programme

- emergency services and how they are integrated into cyber security governance arrangements
- how operators within the energy sector are integrated into cyber security governance arrangements
- how telecommunications operators are integrated into cyber security governance arrangements; and
- the arrangements in respect of the JCSC.

The audit will not consider arrangements in respect of private sector businesses on the Island.

Audit approach

This audit will use a combination of a problem-oriented and system-oriented approach.

The audit will commence with an initial documentation request. The findings of the document review will be followed up by interviews with key officers and with other stakeholders. Since this audit covers multiple departments and Chief Officers an initial kick-off workshop will be run to agree a practical plan to support efficient data collection and to help avoid overlap and duplication.

The audit will commence in June 2025 with fieldwork taking place across the summer and early autumn.

The detailed work will be undertaken by affiliates engaged by the C&AG.

Audit criteria

To assess if the Government's efforts to improve cyber security are providing value for money, the audit will consider whether:

- clear, risk-based cyber resilience outcomes have been set for the programmes and arrangements put in place within the States
- the right support, incentives and monitoring procedures have been established to provide assurance over cyber security arrangements relating to critical infrastructure operated by the States of Jersey Group and by asset owners in the telecommunications and energy sectors; and

- actions taken by the States and the JCSC have appropriately prioritised, and built the capability to deliver, the cyber security they need to operate effectively.

The audit criteria will include the following aspects of cyber security governance arrangements:

- Network Security: The adequacy of security of the network infrastructure, including firewalls, intrusion detection systems, and network segmentation within the States.
- Data Protection: How sensitive data is stored, transmitted, and accessed, ensuring encryption and other protective measures are in place within the States.
- Access Controls: User access controls operate to ensure that only authorised personnel have access to sensitive information and systems with the States.
- Incident Response Plan: A well-defined incident response plan is in place to address potential security breaches and minimise damage both within the States and Island-wide.
- Employee Training: Systems users within the States are trained in cyber security best practices and are aware of potential threats such as phishing attacks.
- Physical Security: Physical security measures in place within the States protect hardware and data from unauthorised access or theft.
- Compliance: There is compliance with relevant industry regulations and standards both within Government and in respect of Island-wide arrangements.
- Vulnerability Assessments: Regular vulnerability assessments and penetration testing are in place across States systems to identify and address potential weaknesses in systems.
- Security Policies: A comprehensive and up-to-date suite of policies is in place both within the States and in respect of Island-wide arrangements.
- Risk Management: A risk management framework is in place to identify, assess, and mitigate States and Island-wide cyber security risks.
- Business continuity: Effective plans are in place for critical services on the Island to respond in the event of a cyber attack.
- Horizon planning: Island-wide and States governance arrangements ensure that emerging threats, including the threats from improper or inadvertent use of Artificial Intelligence, are identified and integrated into the ongoing approach.

JERSEY AUDIT OFFICE

LYNN PAMMENT CBE
Comptroller and Auditor General

Jersey Audit Office, De Carteret House, 7 Castle Street, St Helier, Jersey JE2 3BT
T: +44 1534 716800 E: enquiries@jerseyauditoffice.je W: www.jerseyauditoffice.je