



The National Archives

The SIRO and the Cyber Information Challenge

What Should Keep You Awake at
Night?





Overview

- Background
- The SIRO's Role and Responsibilities
- Definitions of Cyber Security and Information
- An Overview of the SIRO's Relationships
- Case Studies



Activity

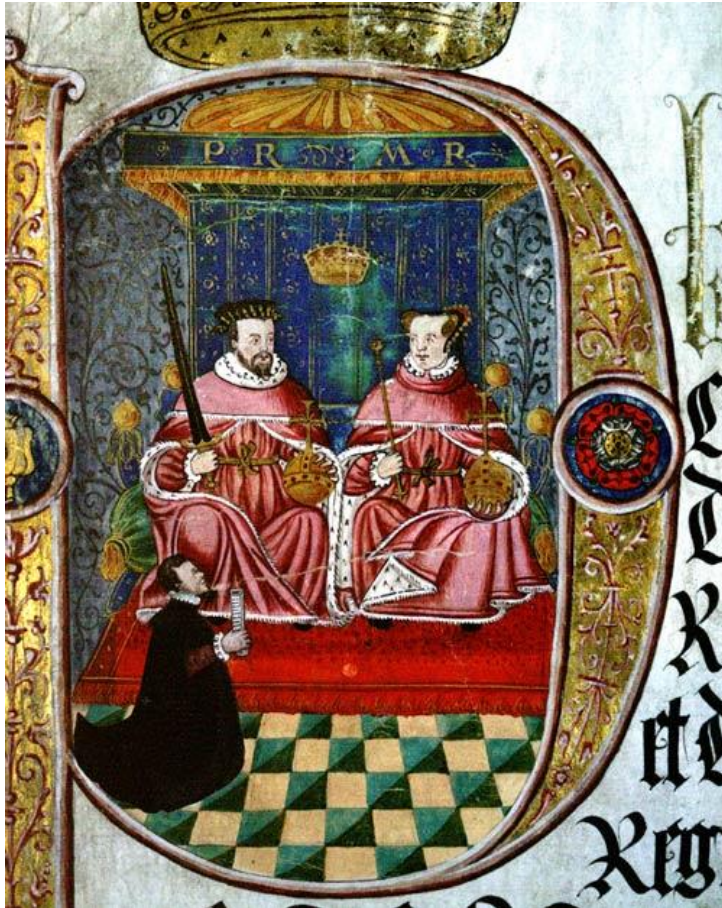
How long you've been in the SIRO role?

What is the **best** thing about your organisation's approach to information risk?

Any concerns you have in your SIRO role?



Senior Information Risk Owner



- Your role was created to provide board-level accountability and greater assurance that information risks are addressed
- You ensure that information risks are treated as a priority for the business
- You play a vital role in getting your organisation to recognise the value of its information
- By treating information as a business priority not an ICT issue you ensure that risks are addressed, managed and capitalised upon



Information assets... a definition

- a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively
- has recognisable and manageable value, risk, content and lifecycles

Key points for the SIRO

- Understand the kind of information that is held by your organisation
- Gain an overview of what enters and leaves your organisation's information assets
- Understand why anything might be entering or leaving your organisation's assets





What is Cyber Security?

Definition:

Cyber security involves the security of any integrated or networked system

This could be connected through the internet, connected virtually over private networks or through integrated mechanical systems (e.g. building controls, automated systems etc.)

Access to Information

- Having access to information is necessary for all employees
- However access must be for a clear business purpose
- Unmonitored access leaves an organisation's information assets open to exploitation





Risks to Information

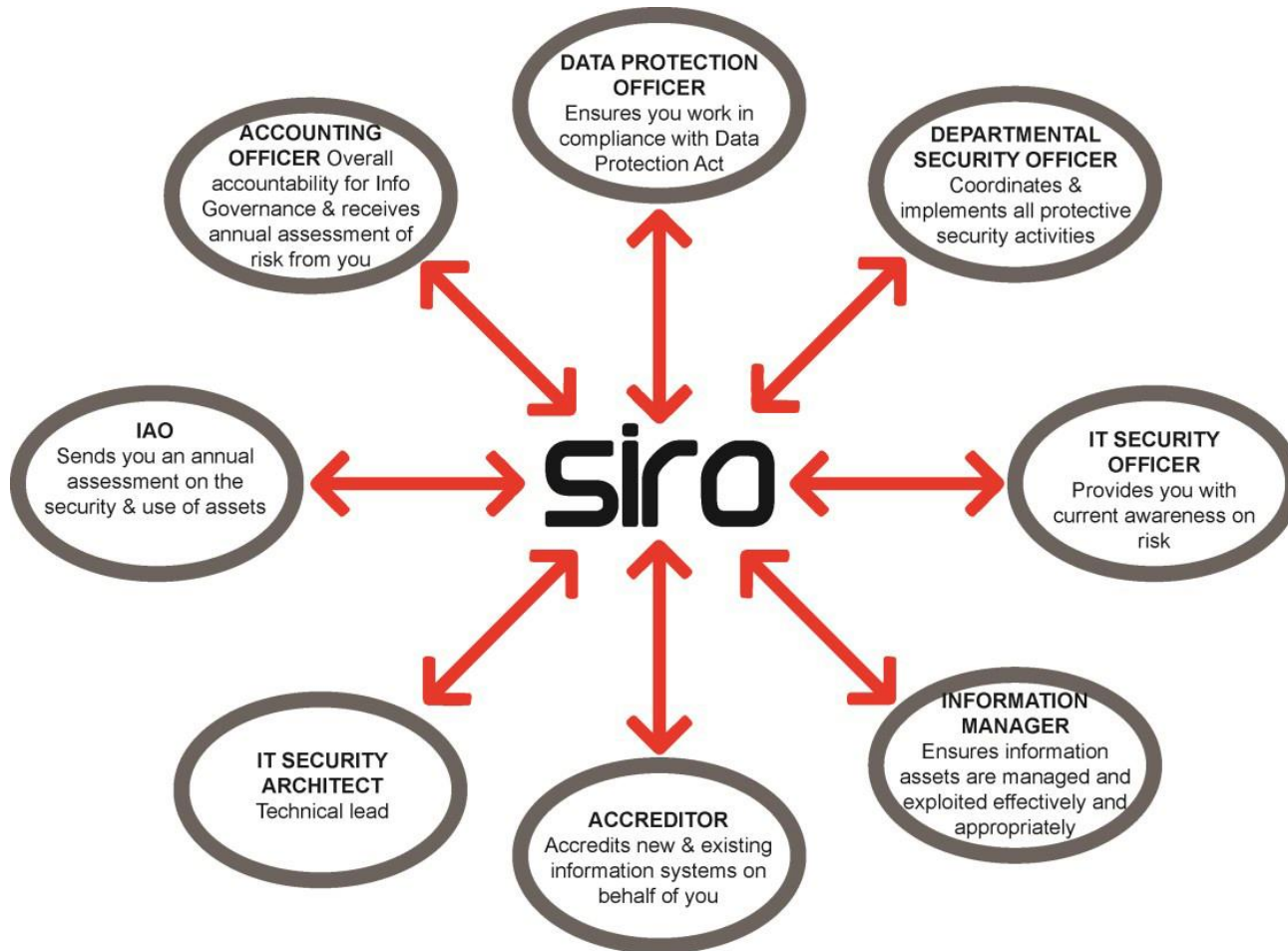
Confidentiality – ensuring only properly authorised persons can access information and proper controls in place to prevent unauthorised access

Integrity – assuring the authenticity, accuracy and completeness of data throughout its entire life-cycle

Availability – assuring that authorised people can access it when they need to, at the right times in the right ways



SIRO Key Relationships



Working with your Executive teams

- Establish an information risk strategy
- Identify business-critical information assets
- Establish and maintain an appropriate risk appetite





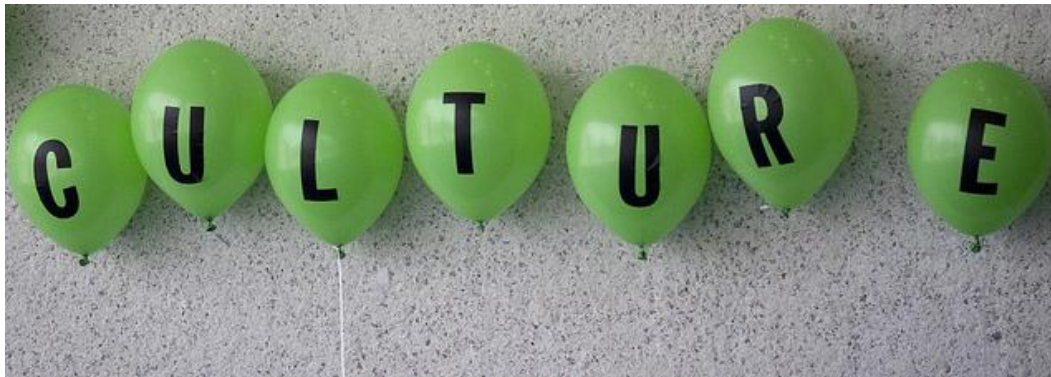
Working with colleagues

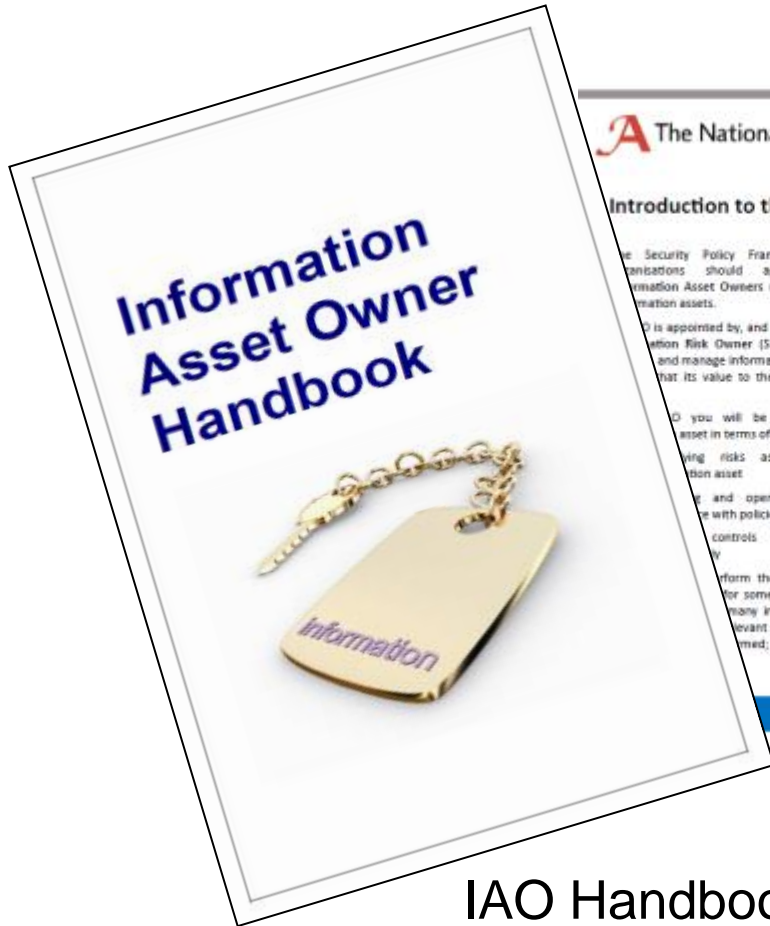
- Set up an information governance framework
- Act as an exemplar for information risk
- Ensure compliance with legislation
- Establish a reporting and learning culture

Business Culture

How can you foster a culture that values, protects and uses information for the success of the organisation and the benefit of the public?

What are the challenges for your organisation?





IAO Handbook



SIRO Handbook

For copies of literature, please contact the team at:
IATraining@nationalarchives.gsi.gov.uk or via Twitter @IACSEP