Information Management Manual

Contents

1 Introduction

The Sellafield Ltd Mission to 'deliver safe, secure site stewardship whilst demonstrating value for money and urgency in the reduction of risks and hazards posed by Sellafield's historic facilities and wastes' is underpinned by the Standard Nuclear Performance Model (SNPM). It recognises the contribution by Information Management (IM) as a key enabling processes.

As a knowledge intensive business, Sellafield Ltd understands the importance of its human and information assets to delivering its mission. Quite simply, 'Information sits at the heart of everything we do'. Effective management of information will enable the business to realise considerable benefits, avoid considerable costs and be of wider value to the business, not least in helping us perform our jobs.

Never before has information played such a vital role in an organisation's success. Information is the linchpin in every business decision. Sellafield Ltd relies on timely, accurate information to make major decisions and to communicate with all its stakeholders to enable collaboration both internally and externally.

Sellafield Ltd requires an Information Management vision that better fits within the Standard Nuclear Performance Model (SNPM) and an approach to managing information assets that is similar to managing any business assets using standard frameworks and that incorporates a risk based approach to optimise investment to both mitigate risks and realise the value of information assets.

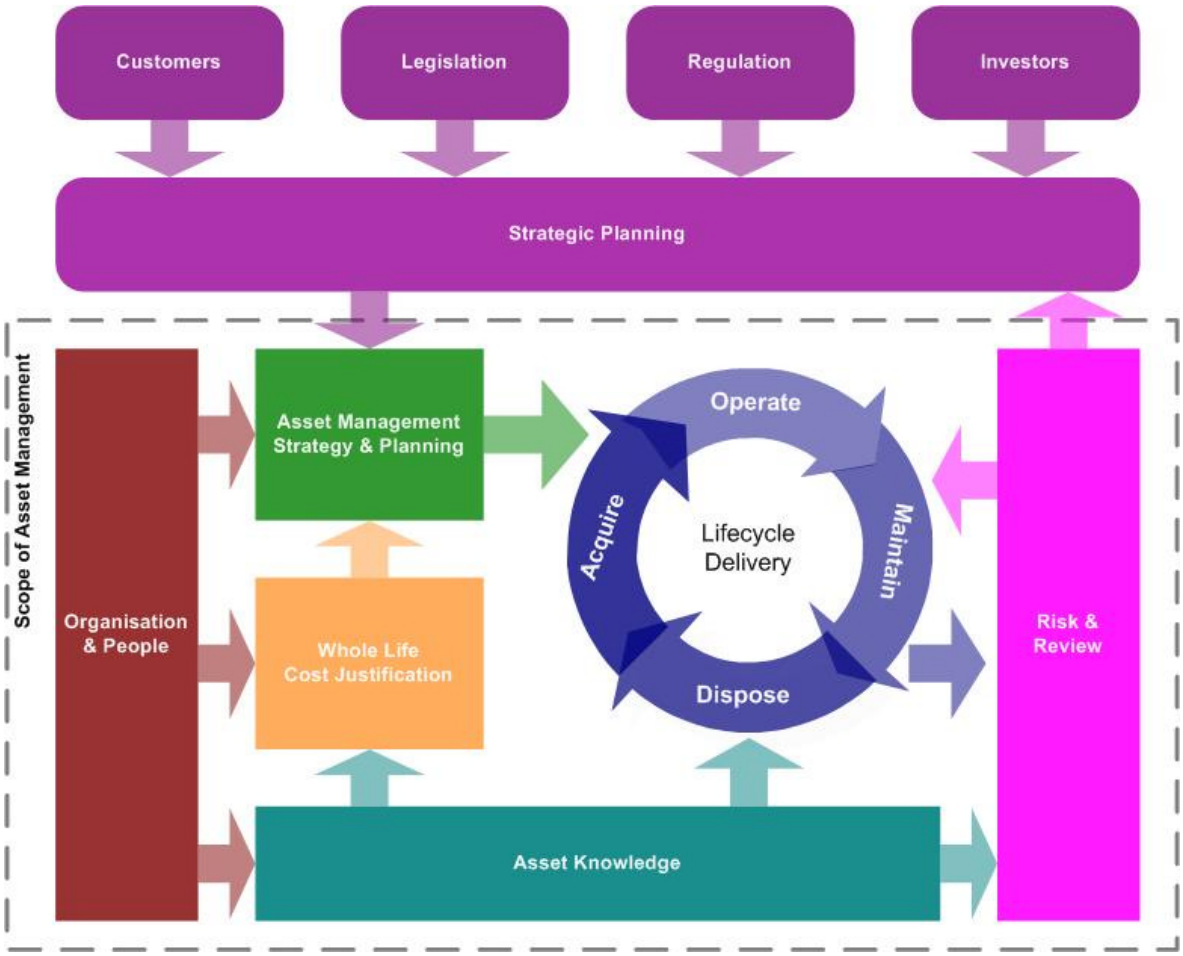

Figure 1: A standard asset management framework

Our aim is to achieve a future state whereby information management fully aligns to support the business strategic imperatives, termed Outcome Based Information Management. This approach works backwards from business goals and outcomes to inform the imperatives for information and supporting information technology.

The strategic vision for information management at Sellafield Ltd is presented in figure 2 below.

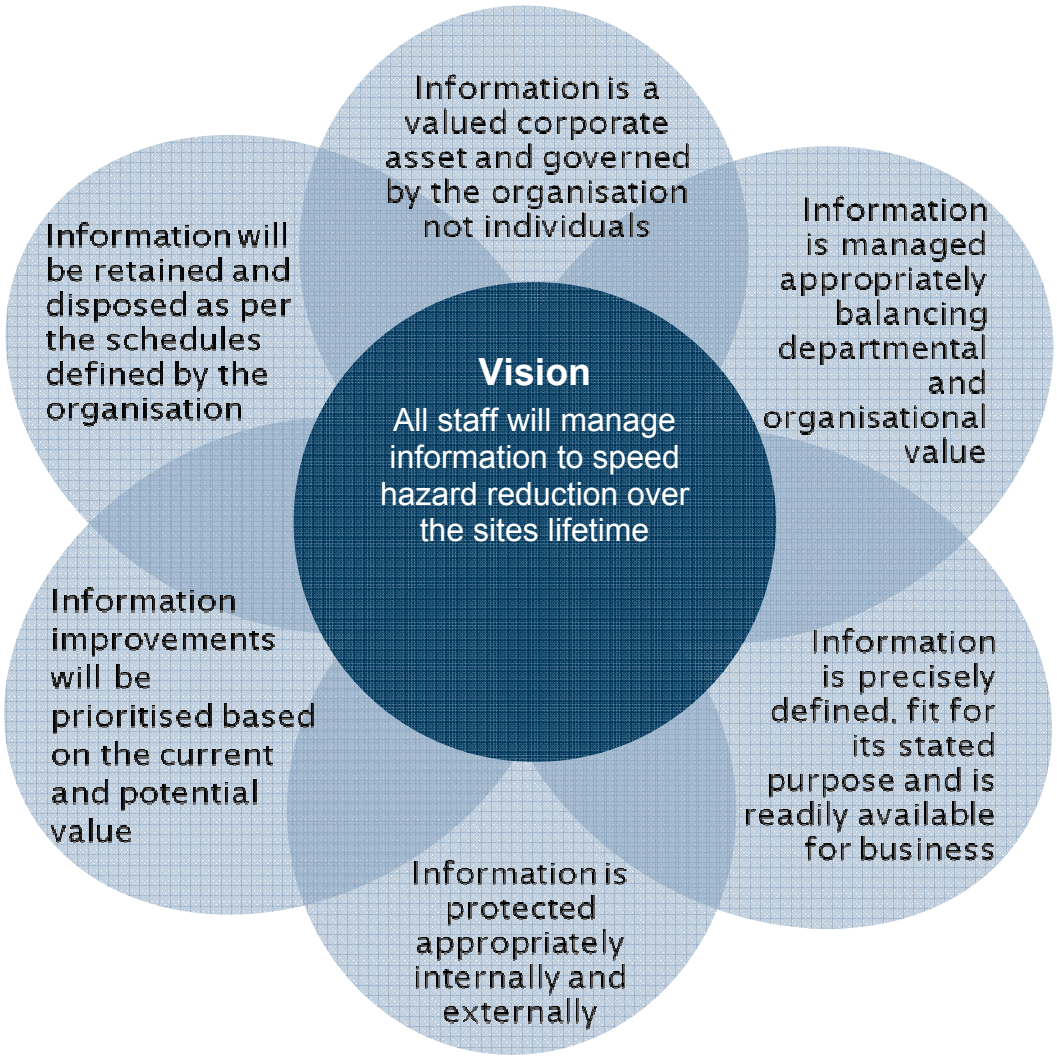

Figure 2: Sellafield Ltd strategic vision for information management

The Nuclear Decommissioning Authority (NDA) owns all the physical assets (e.g. buildings, plants, waste products, and nuclear materials) located on the Sellafield Ltd site and all the information assets (e.g. electronic and physical files) that are created and managed by Sellafield Ltd in the course of its business, including legacy information holdings from the past e.g. historic archives.

As owner of the information contained in its Estate, the NDA is obliged by the various statutes, regulations and requirements of Regulators and Government (primarily Cabinet Office – Data Handling Review 2008) to manage its information, knowledge and records to the standard required of a responsible public body. The Information Governance Strategy issued by the NDA states that the NDA must:

- Create, manage, secure, retain and destroy all of its records in accordance with the Public Records Act (PRA), Security Policy Framework (SPF) and national and international Standards as obligated by relevant Acts and HMG policy;
- Maintain a Place of Deposit for its long-term records;
- Ensure that suitable systems are in place so that information can be located in the Estate to enable the NDA to perform its obligations under the Freedom of Information Act (FoIA), Environmental Information Regulations (EIR) and Data Protection Act (DPA). This includes a number of elements that promote openness and transparency through proactive publication; Information Asset Registers, Publication Schemes & effective Records Management policies and systems;
- Ensure that its sensitive nuclear and personal information is kept secure whilst, at the same time, making all information accessible to all stakeholders, including members of the public, where appropriate and prudent to do so;
- Put in place systems to enable information and knowledge capture and sharing;
- Promote collaborative practices wherever practical.

2 Information Management framework

2.1 Scope and context – what is information?

Information can take many different forms. Information at its most basic level is in the form of raw data. Information can come from a variety of sources and can exist in a wide range of formats, such as an employee's handwritten notes, databases through to emails, paper, video, flipcharts, photographs, drawings and 3D-models.

In the context of this manual information is defined as business information comprising any *printed or electronically generated document or structured data stored in databases.* This information may have its origins inside or outside the company and is used to facilitate or provide evidence of the business carried out by Sellafield Ltd.

For Sellafield Ltd information relating to activities carried out or in relation to nuclear sites or other nuclear premises needs to be protected in the interests of national security. Such information is known as Sensitive Nuclear Information (SNI).

2.2 Information management components

This manual provides a high level description of the Information Management processes and how Sellafield Ltd is organised in terms of its Information Management capability to deliver that process.

The structure under this manual is as follows:

- **4.09.100** – Information lifecycle and records management
- **4.09.200** – Information risk management
- **4.09.300** – Information security management (which also includes)
    - Data Sharing Manual
    - Use of CCTV Content
    - Personal Data Handling

- **4.09.400** – Information service delivery (which also includes)
    - Application portfolio management
    - Architecture management
- **4.09.500** – Sellafield maps
- **4.09.600** – Intellectual property management

SLPs and SLSPs which are underpinning these manuals are within the SLMS.

4.09.500 Sellafield Maps is not part of ISO but the documentation sits under Information Management, and is not part of this manual. (Sellafield Maps are writing there own SLMs, SLPs and SLSPs).

This manual gives an overview of Sellafield Ltd IM policy, objectives, structure, roles and responsibilities. There are documents underpinning this manual that explain how to conduct the principle components of Information Management in the context of Sellafield Ltd:

- Information lifecycle and records management

  This provides a description of the lifecycle management arrangements for information created by and for Sellafield Ltd, to ensure compliance with best practices for records management including ownership, identification, retention, availability, preservation and disposal (applicable to electronic and physical records); to provide assurance to stakeholders that key information is managed efficiently throughout its lifetime.

- Information risk management

  This provides a description of the Information Risk Management arrangements, for Sellafield Ltd and its supply chain, to ensure compliance and provide assurance to Stakeholders that any risks to Sellafield Ltd Information are managed efficiently and effectively in accordance with statutory regulations and the international standards for Information Security for the protection of Sellafield Ltd's information assets

- Information security management

  This provides a description of the information security arrangements, for Sellafield Ltd and its supply chain, to ensure compliance and provide assurance to stakeholders that Sellafield Ltd's information assets are protected in accordance with the statutory regulations and standards for information security and also includes data sharing, use of CCTV and handling personal data

- Information service delivery

This provides a description of how Sellafield Ltd manages its architecture structure which supports a mixture of Solution Architecture and Enterprise Architecture activities, its applications which sit on the network and the service delivery for IT management arrangements to ensure compliance with its legal and contractual obligations to other parties.

- Intellectual property management

  This provides a description of the Sellafield Ltd obligations with regard to Intellectual property arising from the M&O contract and the Parent body Agreement and also arrangements to ensure compliance with its legal and contractual obligations to other parties.

2.3 Legislation requirements

This information management manual aims to provide the frameworks for Sellafield Ltd to meet the requirements of the following legislations:

- The Public Records Act 1958 / 1967 (Ministry of Justice / The National Archives) - The legislation governing the selection and transfer of public records.

- The Freedom of Information Act 2000 (Ministry of Justice / Information Commissioner's Office) - UK government legislation defining what information public sector organizations are obliged to provide on request. To meet the obligations of the Act, public bodies must have effective information and records management processes in place; there is a code of practice on records management under section 46 of the Act.

- The Data Protection Act 1998 (Ministry of Justice / Information Commissioner's Office) - Provision for the regulation of the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.

- Environmental Information Regulations 2004 (Defra) - The Environmental Information Regulations (EIRs) give the general public certain rights of access to environmental information. The definition of environmental information in the EIRs is very wide and includes information that might not be considered environmental at first glance. EIRs only cover environmental information - Freedom of Information covers all information held by public authorities.

2.4 Customer and regulatory requirements

This information management manual aims to provide the frameworks for Sellafield Ltd to meet the requirements of the following key stakeholders:

Customer (NDA)

- M&O contract;
- Strategy & policy;
- Information Assurance Maturity Model (IAMM);

Regulator (ONR)

- Nuclear Industry Security Regulations 2003 (NISR 2003);
- Security Policy Framework (SPF);
- Civil Nuclear Information Security (Infosec) Standard and Civil Nuclear Personnel Security Standard (referred to in this document as Civil Nuclear Security (CNS) Standards);
- National objectives, requirements and model standards (NORMS), and
- Nuclear Site Licence requirements;

2.5 Standards and industry best practice requirements

The requirements for robust information management processes are also in support of recognised standards and industry best practices

Standards
- ISO 27000 Series Standards for Information Security;
- ISO 15489-1 Records Management;
- BS 10008 Evidential Weight and Legal Admissibility of Electronic Information;

Industry best practices
- WANO/INPO;
- IAEA;

2.6 Information Management Policy

In Summary, the Sellafield Ltd Information Management Policy (SLCP 4.09.02) states that:

'Sellafield Ltd. regards information and knowledge as valuable assets critical to delivering its mission. We shall provide robust information management arrangements, including all aspects of information risk and security, to ensure information (in all its forms; including records, data, documents or any media type) and all forms of knowledge is identified, valued, secured, preserved, easily retrieved and reused for the Company and its stakeholders.

We shall establish and maintain suitable means of storing information for re-use at the point of work whilst also protecting information and associated technology to ensure the Company meets its legal and proliferation-sensitive obligations. Any loss of information shall be reported and investigated accordingly.

2.7 Information Management Principles

The following principles underpin this policy and specify that Sellafield Ltd:

1. Has in place a risk based approach to the management of information throughout its lifecycle and in accordance with quality and value added to the Company.

2. Ensures information management arrangements give due attention to security, protection, usability, retrievability, preservation, environmental and cost issues in order to make the right information available through a knowledge sharing and learning culture.

3. Ensures compliance with all legal and regulatory requirements relating to the retention of information including long term preservation (physical and digital).

4. Maintains a business ownership model for all information assets, with clearly defined roles and accountabilities, to ensure critical information assets are effectively controlled, leveraged, and optimised for the benefit of the Company.

5. Promotes an effective information management culture, including information security, through the continued delivery of awareness and training.

6. Supports the move from systems and processes primarily underpinned by paper to a compliant electronic environment in accordance with BS 10008 (Evidential Weight and Legal Admissibility of Electronic Information).

7. Ensures that information management principles are incorporated in the design of new or upgraded processes and systems utilising appropriate automation of workflows to provide a timely and accurate single source of data.

8. Rationalises and optimises information systems to a strategic enterprise level blueprint based on an integrated set of best-in-class (functional capability) systems and sourced, where possible, from industry standard packaged solutions.

9. Treats personal information lawfully and correctly, in particular adhering to the Eight Principles of Data Protection, contained in the Data Protection Act 1998.

10. Ensures arrangements are in place to monitor and protect the confidentiality, integrity and availability of the Company's information assets from all known threats, whether internal or external, deliberate or accidental in accordance with NISR (2003 as amended), the Security Policy Framework (SPF) and CNS Standards.

11. Has in place suitable arrangements for the monitoring of activity on Company information systems to prevent or detect actual or potential security breaches and take appropriate action in response.

12. Ensures that Intellectual Property (IP) is managed in a manner that meets all legal and contractual obligations and requirements.

This policy and principles will result in the introduction of a risk based approach to managing information assets.

2.8 Organisation and responsibilities for information management

The overall delivery model for information management across Sellafield Ltd is a distributed model with central authority / governance roles and business delivery / implementation roles.

The objective is to establish information governance that involves information governance role holders, senior business representatives plus ISO and other specialist technicians to ensure informed decision making and provide an opportunity to transition to effective information process governance.

Delivery of information management transformation requires a capacity to change. The cost reimbersable Government Owned Contractor Operated (GOCO) model, the inclusion of information governance within the Sellafield Ltd Excellence Plan and the organisational changes to support this should ensure suitable capacity is made available to deliver the changes sought.

High level information governance shown in figure 3 is provded by an Information Goverance Steering Group led by the CIO, on which a senior business sponsor serves and which has a direct reporting line to SIRO, a Board level position.

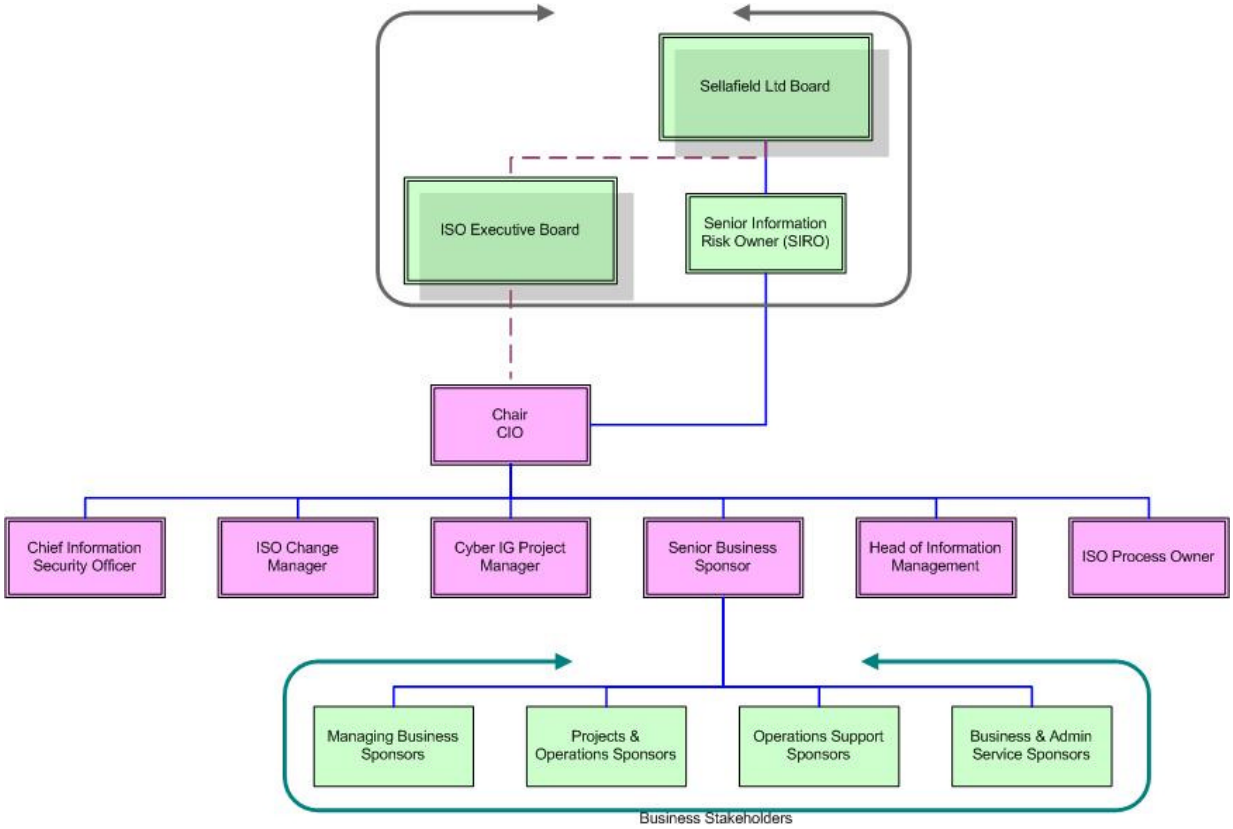

Figure 3: Information governance organisation

Key roles and responsibilities

Sellafield Ltd Executive Committee, responsible for:

- setting challenging but achievable enterprise goals and objectives
- prioritising resources and funding to deliver those objectives, always ensuring that nuclear safety remains our overriding priority

Senior Information Risk Officer (SIRO), responsible for:

- Owning the overall information risk policy and procedures and advising the Accounting Officer on information risk
- Leading the company/organisation management of information risk at Board level and Ensuring the Board are kept up to date, and adequately briefed, on information risk issues
- Understanding the information risks to the organisation (including the risks to SNI)
- Accepting information risks that are above the set risk appetite and risk tolerance
- Understanding the information risks through the organisation's delivery chain and ensures they are addressed and they inform investment decisions
- Developing and a strategy for implementing the risk policy within an overall Information Governance Framework
- Ensures the approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Ensuring records are kept relating to material discussions and decisions affecting Information Risk Policy

- Ensuring the recording and reporting of information risk incidents
- Attendance at regular Cabinet Office SIRO seminars
- Ensuring compliance with mandatory data handling requirements

Chief Information Officer (CIO), responsible for:

- Linking business and information strategies and plans
- Optimising the cost of IT and delivering value for money
- Rationalisation of IT systems and operations
- Expanding the use of information assets
- Building business skills in the ISO organisation, via knowledge transfer and incorporation of business resources into the ISO
- Leading enterprise change initiatives
- Managing information risk and exposure
- Improving the business and ISO relationship
- Manage external stakeholders i.e. NDA and regulators

Chief Information Security Officer (CISO), responsible for:

- Develop, implement and monitor a strategic, comprehensive enterprise information security and risk management programme to ensure the integrity, confidentiality and availability of information owned, controlled or processed by the business
- Facilitate appropriate resource allocation, and increase the maturity of the information security capability across the business
- Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations
- Develop and manage a capability to respond to and recover from disruptive and destructive information security events
- Create and manage information security and risk management awareness training programmes for all employees, contractors and approved information system users
- Develop and oversee effective disaster recovery policies and standards to align with business continuity goals. Coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of an information security event
- Work directly with the business to facilitate information risk assessment and risk management processes, and work with stakeholders throughout the business on identifying acceptable levels of residual risk
- Create, communicate and implement a risk-based process for vendor information risk management, including assessment and treatment for risks that may result from partners and other service providers
- Provide strategic risk guidance for information related projects, including the evaluation and recommendation of information controls
- Ensuring HR policies for information security management exist and are enforced. Where good behaviour is identified this is rewarded
- Ensuring the measuring and reporting of mandatory data handling compliance

- Ensuring the recording and reporting of information risk incidents

Information Asset Owner (IAO), responsible for:

- Leading a culture that values, protects and uses information in line with business and stakeholder requirements
- Ensuring that information assets are identified and recorded
- Ensuring that information assets are handled and managed appropriately. This means that their value to the organisation is fully exploited and business benefits maximised
- Ensuring that information assets are protected appropriately and where the information is shared that the proper confidentiality, integrity and availability safeguards apply.
- Knowing what information the asset holds, and what is transferred in or out of it.
- Knowing who has access and why, and ensure that their use of the asset is monitored.
- Understanding and addressing risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are appropriately managed
- Assisting in the enforcement of HR information security processes and escalate incidents to relevant individuals or teams
- Ensuring Personal Information is appropriately protected in accordance with the DPA.
- Participating in information risk assessments and reviews; identifying business participants in information risk assessments
- Informing the Information Risk Manager of any significant changes to their information asset that could affect the identified information risks

Chief Technology Officer (CTO), responsible for

- Delivering technologies and systems that meet the needs of the Sellafield Ltd business, users and staff
- Providing strong leadership and senior-level advocacy for the delivery of technology solutions that support Sellafield Ltd current and future business programmes
- Defining the strategic direction and business priorities for the development of the technology, ensuring that solutions and services are fully supported by the right architectures and systems, and that dependence on existing legacy systems is dramatically reduced
- Embedding the delivery of a sustainable, high quality technology capability across Sellafield Ltd, and a complementary commercial strategy
- Bringing a deep knowledge of the technology landscape and marketplace to Sellafield Ltd, and ensure that it makes effective use of modern standards and solutions
- Working with the NDA, Regulators and other estate SLCs as the Sellafield Ltd Technology Leader to exchange best practice, develop cross-estate strategic direction and deploy commodity shared services where appropriate

Data Protection Officer (DPO), responsible for:

- Implement the Data Protection
- Maintain the Data Protection Policy and procedures and disseminate new rules or regulations on Data Protection Act to staff

- Monitor, annually review and amend immediately where necessary the registrable particulars of the organisation's Data Processing registration with The Information Commissioner's Office
- Ensure that the Data Protection aspects are properly covered in the governance documents of all systems processing personal data
- Carry out Privacy Impact Assessments or Compliance Check List's on all systems processing personal data, on a prioritised basis
- Monitor the implementation of Data Protection standards, policies and procedures within the organisation and conduct frequent audits of data for compliance
- Ensure appropriate Awareness training is carried to all necessary staff
- Respond to all internal and external Data Protection issues and queries, seeking legal advice where necessary
- Liaise and advise the Human Resources department on Subject Access Requests and the appropriateness of disclosure

Intellectual Property Manager, responsible for:

- Developing Sellafield Ltd intellectual property capabilities in line with strategic business objectives and NDA priorities
- Supporting strategic business objectives by challenging site wide norms and behaviours where these relate to the use and management of Intellectual Property and leading and delivering step changes that enable Sellafield strategic intent
- Provision of intellectual property advice service to Sellafield Ltd, particularly with regard to contractual terms to be applied to contracts with sub-contractors
- Representing Sellafield Ltd intellectual property position to NDA and other stakeholders
- Ensuring that appropriate external best practice is used
- Facilitating changes to supply chain contracts following contract clarification process

Departmental Records Officer (DRO), responsible for:

- Creating a records management strategy based upon the business objectives
- Overseeing the development and implementation of a records programme and supporting infrastructure
- Maintaining the policies and procedures intended to:
    - Ensure compliance with the Public Records Act, Data Protection Act, Freedom of Information Act and Human Rights Act;
    - Ensure that the records of Sellafield Ltd are effectively managed and available as a corporate resource;
    - Ensure the destruction of records that are no longer required;
- Making arrangements to identify records worthy of permanent preservation and for their safekeeping
- Ensuring that the records selected for permanent preservation are prepared for transfer and then transferred to the National Nuclear Archive (NNA)
- Identifying those records that cannot be transferred to the NNA and retain these for such a period as stipulated in the relevant retention schedules

2.9 Performance management

Core to Sellafield Ltd business is the effective management of its information assets to maintain their Confidentiality, Integrity and Availability (CIA). To ensure effective governance of these assets throughout their life a number of processes, procedures and roles have been defined. These are subject to audit annually by the way of an Information Assurance Maturity Model (IAMM) assessment. This assessment is a requirement of the NDA and ONR and utilised a defined HMG Cabinet Office approach.

3 Definitions and Abbreviations

3.1 Definitions

None

3.2 Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNS	Civil Nuclear Security
HMG	Her Majesty's Government
IA	Information Assurance
IAEA	International Atomic Energy Agency
IAMM	Information Assurance Maturity Model
IAO	Information Asset Owner
INPO	Institute of Nuclear Power Operations
IP	Intellectual Property
ISO	Information Services Organisation (Sellafield Ltd Department)
ISO	International Standards Organisation (i.e. ISO 27000 Series)
IT	Information Technology
NDA	Nuclear Decommissioning Authority
NISR 2003	Nuclear Industries Security Regulations, 2003
ONR	Office for Nuclear Regulation
SIRO	Senior Information Risk Owner
SLM	Sellafield LtdManual
SLP	Sellafield LtdPractices
SLSP	Sellafield LtdSupporting Practices
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
WANO	World Association of Nuclear Operators

4 References

Refer to section 2.3

5 Amendment Record

Issue 3 to Issue 4

Date of amendment	Section or paragraph amended	Details of amendment
April 2015	2.2 only	Minor changes to align the structure of the topic area 4.09 manuals