

Configuration Management Policy

(ISO 27001:2022 Technological Controls - Clause 8.9)

Author	Greg Nott
Version	2.0
Date Created	06/05/2023
Last Update Date	14/05/2024
Document Control	Released
Document ID	230506-IMS-POL-ConfigurationManagement-V2
Security Classification	Public

Table of Contents

Configuration Management Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose	4
Exceptions	4
Roles and Responsibilities.....	4
Senior Management	4
IMS Team.....	4
System/Service Owners	5
IT Staff	5
Configuration Management Process.....	5
Configuration Identification	5
Configuration Control.....	5
Configuration Status Logging	5
Configuration Verification and Audit	5
Configuration Documentation	6
Compliance and Monitoring	6
Training and Awareness	6
Review.....	6
Appendix A – Glossary of Terms	7

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	07-Aug-23
Greg Nott	2.0	Paul Langan	14-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	03-Aug-23
Paul Langan	Review & Rebrand	2.0	14-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	06-May-23
Greg Nott	Review & Rebrand	2.0	14-May-24

Associated Documents

Document	Version
239619-IMS-POL-ITSNProcessGuide-V1	1.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Configuration Management Policy adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

This policy applies to all information assets, including but not limited to hardware, software, network devices, databases, and documentation, owned or controlled by ARO.

Purpose

The purpose of this policy is to establish the framework for effective configuration management practices within ARO to ensure the confidentiality, integrity, and availability of information assets. By establishing this framework, we aim to meet the following objectives:

- To establish a standardised approach for managing configuration items throughout their lifecycle.
- To ensure the accuracy, completeness, and consistency of configuration information.
- To minimise unauthorised changes and prevent unauthorised access to configuration items.
- To facilitate efficient incident response and problem resolution through accurate configuration information.
- To comply with legal, regulatory, and contractual requirements related to configuration management.

Exceptions

- Any exceptions to the application of this policy or where controls cannot be adhered to MUST be presented to the Head of Information Security or a member of the management team (or a member of the IMS Team).
- All exceptions to this policy MUST be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

Roles and Responsibilities

Senior Management

- The Senior Management Team is responsible for providing the necessary resources and support for the implementation of effective configuration management practices.
- The Senior Management Team (or a nominated team member) will review and approve the configuration management policy and any subsequent changes.

IMS Team

- The IMS Team is responsible for overseeing the implementation and operation of the configuration management process.

- The IMS Team will work with the System/Service Owners to ensure that configuration items are properly identified, documented, controlled, and maintained throughout their lifecycle.

System/Service Owners

- The System/Service owners are responsible for identifying and documenting the configuration items associated with their respective systems.
- The System/Service owners will ensure that changes to configuration items are properly authorised and implemented.

IT Staff

- IT staff members are responsible for following the configuration management process and complying with the established procedures.
- IT staff members will report any configuration management issues or non-compliance to the IMS Team.

Configuration Management Process

Configuration Identification

- All configuration items shall be identified and documented in the configuration management system. ARO currently use multiple systems including:
 - Microsoft SharePoint
 - Service Now (BOLT)
 - IT Glue
 - PassPortal
- Each configuration item shall be assigned a unique identifier and categorised based on its type and criticality.

Configuration Control

- Changes to configuration items shall be controlled through a formal change management process.
- Changes shall be assessed for their impact on security and approved by the appropriate authority before implementation.

Configuration Status Logging

- The status and attributes of configuration items shall be recorded and maintained in the configuration management system.
- Any changes to the configuration items shall be reflected in the configuration records.

Configuration Verification and Audit

- Regular verification and audit activities shall be conducted to ensure the accuracy and completeness of configuration information.
- Any discrepancies and inconsistencies identified should be reported and addressed.

Configuration Documentation

- Configuration items shall be documented, including their specifications, dependencies, and relationships.
- The documentation shall be maintained and updated as necessary to reflect the current state of the configuration items.

Compliance and Monitoring

- Compliance with this policy shall be periodically monitored through internal audits and assessments.
- Any non-compliance or deviations shall be reported to the Head of Information Security for appropriate action.

Training and Awareness

All personnel involved in the configuration management process shall receive appropriate training and awareness sessions.

Review

This policy shall be reviewed and updated as necessary to reflect changes in the organisation's business environment, legal and regulatory requirements, and best practices.

Appendix A – Glossary of Terms

Term	Meaning
Configuration Item (CI)	A configuration item is a hardware, software, or network component that is under configuration management control.
Configuration Management	Configuration management is the process of identifying, organising, and controlling configuration items throughout their lifecycle.
Change Management	Change management is the process of controlling changes to configuration items in a systematic and coordinated manner.