RESILIENCE

Grant Agreement 101079792, RESILIENCE PPP

Operations Management Policy (OMP)

Title of Deliverable:	Operations Management Policy (OMP)		
Deliverable Number:	D2.10		
Type of Data:	Deliverable		
Lead Beneficiary:	FSCIRE		
Publishing Status	Public		
Last Revision Date:	15/04/2025	**by:**	FSCIRE (R. DEMO)
Verification Date:	31/05/2025	**by:**	KU Leuven (R. WYNS, M. De Leeuw)
Approval Date:	[DD/MM/YYYY]	**by:**	FSCIRE (F. Cadeddu)
Document Name:	RESILIENCE_WP2_D2.10_OMP_01.00_FINAL		

Funded by
the European Union

Change History

Version Number	Date	Status	Name	Summary of Main Changes
00.01	15/04/2025	DRAFT	Initial Draft	
00.02	28/04/2025	2nd DRAFT	Revised Text	Revisions from KULeuven and CAF
00.03	01/06/2025	3rd DRAFT	Version sent to BoD	Revisions are addressed and closed
01.00	03/06/2025	FINAL	Final Version	

Author(s)

Name	Beneficiary	Role
Rudy DEMO	FSCIRE	Author

Distribution List

Name	Beneficiary	Role
Public	All	All

Table of Contents

Acronyms

Acronym	Full Form
BoD	Board of Directors
CAB	Change Advisory Board
CAP	Corrective Action Plan
DPAs	Data Processing Agreements
DPO	Data Protection Officer
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IRT	Incident Response Team
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
OMP	Operational Management Policy
OWASP	Open Web Application Security Project
PIR	Post-Incident Review
RCA	Root Cause Analysis
RI	Research Infrastructure
SCC	Service Coordination Committee
SDP	Software Development Plan
SLA	Service Level Agreement
SLR	Service Level Requirements
SLO	Service Level Objective
SRL	Services Requirement Levels
TLS	Transport Layer Security
VPN	Virtual Private Network
WP	Work Package
WU	Working Unit
CTO	Chief Technical Officer
TB	Technical Board
IP	Implementation Phase

Definitions

Term	Definition
In-kind Contributions	Many RIs may rely on some forms of in-kind support. This can be related to the use of donated scientific equipment or the exploitation of time machine or personnel costs (this is particularly true for pan-European RIs, which rely heavily on in-kind contributions from national members). They can also refer to technical components or equipment supplied by one of the partners (e.g. one Member State as a share of its contribution) and made available in-kind to the RI. (**from:** StR-ESFRI Study. GUIDELINES ON COST ESTIMATION OF RESEARCH INFRASTRUCTURES)
In-house Contributions	In-house contribution and/or services refer to resources that are directly invested by the Research Infrastructure itself. These contributions are typically financial but can also include resources like staff time, equipment, and facilities that are owned and operated by the RI itself. In-house services represent the internal commitment and investment of the RI into its own operational and project activities, as opposed to resources sourced from external partners or stakeholders.

1 Introduction

1.1 Objectives of this document

1.1.1 From the Proposal

This Operational Management Policy (OMP) document is created in alignment with the D2.9 Services Requirement Levels (SRL)[R2].

The Operational Management Policy for RESILIENCE outlines comprehensive best practices and standards for operational governance, risk management, service-level objectives, and continuous improvement processes. This policy ensures that all operational aspects, not limited to software development, are consistent, structured, and robustly managed within RESILIENCE, thereby supporting the project's overall integrity and effectiveness.

This Operational Management Policy (OMP) is closely connected to Deliverable D2.1 — Services Preparation & Implementation Strategy [R3], which defines the catalogue, guiding principles and phased roll-out of services. The OMP therefore describes "how" those services will be governed once RESILIENCE transitions from the current Preparatory Phase (PP) to the Implementation Phase (IP).

1.1.2 Long-term Objectives

The Operational Management Policy for RESILIENCE provides a strategic framework designed to ensure the sustainable, secure, and efficient operation of services within the RESILIENCE Research Infrastructure. It addresses the comprehensive management of operational activities, resource allocation, compliance with relevant standards, risk management, and user satisfaction, ensuring that RESILIENCE consistently meets the evolving requirements of the religious studies research community.

A primary objective of this policy is to establish consistency and standardization across all operational aspects, extending beyond software development. This unified approach guarantees seamless integration, effective collaboration, and optimal resource management across different projects and operational activities within RESILIENCE. The policy aims to achieve operational excellence through clearly defined roles, responsibilities, and processes, enhancing transparency and accountability.

Security and privacy management constitute another fundamental pillar of the policy, reflecting the sensitive nature of data typically encountered in religious studies. The Operational Management Policy mandates advanced security measures, data protection strategies, and stringent compliance with relevant privacy regulations, thereby safeguarding the integrity and confidentiality of user data.

This policy places significant emphasis on user-centric service provision. Every service under RESILIENCE is created and maintained with the end-user's perspective at the forefront, ensuring intuitive use, comprehensive documentation, prompt support, and high user satisfaction. The policy fosters an environment of collaboration, promoting integration capabilities both within RESILIENCE's internal systems and with external platforms, positioning RESILIENCE as a pivotal hub for collaborative research.

Continuous improvement is a critical component of the Operational Management Policy. Through regular monitoring, feedback mechanisms, and performance assessments, RESILIENCE is committed to ongoing refinement of operational practices and service offerings. This dynamic process ensures that RESILIENCE remains adaptive to technological advancements, user feedback, and changing operational demands.

Sustainability and maintenance strategies are clearly articulated within the policy, emphasizing the long-term relevance and operational efficiency of RESILIENCE services. Detailed strategies for regular service updates, preventive maintenance, incident resolution, and, if necessary, comprehensive service overhauls are incorporated to ensure sustained operational performance.

In conclusion, the Operational Management Policy embodies RESILIENCE's dedication to delivering high-quality, secure, and user-focused operational services, underpinning the research infrastructure's capacity to effectively support the dynamic needs of the religious studies research community.

1.2 Discriminative Application of the Operational Management Policy

While RESILIENCE rigorously manages operational processes for internally managed resources, a discriminative approach is employed for in-kind contributions due to practical limitations regarding detailed evaluation and governance.

Even for the in-house contributions, it is important to note that the policies in this deliverable present a proposed framework for the Implementation Phase of RESILIENCE and - if successful - its establishment as an ERIC (IP, planned 2027 at the earliest). Until the IP is well underway and/or the ERIC has been formally established, the proposed measures are advisory only and will be piloted where feasible.

1.2.1 Application to In-kind Contributions

- Contributors are expected to view this Operational Management Policy as a recommended framework.

- Contributions must adhere to basic standards, including anonymization of sensitive data before integration.

- Contributors must comply with minimum recommended security measures, including virus checking, OWASP Application Security Verification Standard adherence, data encryption based on sensitivity levels, and access control procedures.

1.2.2 Application to In-house Created Resources

Once the Implementation is well underway and/or - if successful - the ERIC has been established:

- In-house resources must fully comply with this Operational Management Policy and associated security frameworks, incorporating advanced security controls specific to identified operational risks. Exceptions require approval from the RI Security Officer.

- Regular security audits ensure continuous alignment with the highest security standards.

- Sensitive data is explicitly excluded from hosting on the RESILIENCE platform; alternate compliant storage solutions must be used.

By clearly delineating these tailored applications, RESILIENCE ensures appropriate governance and operational integrity across all its resources.

2 Operational Governance

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

2.1 Organizational Structure

The organizational structure for managing operations of the IT Services within RESILIENCE Technical Infrastructure includes dedicated governance bodies and roles, specifically aligned with the overarching RESILIENCE governance model:

- Director

Holds overall responsibility for ensuring strategic alignment of IT operational management.

- Chief Technical Officer

Provides executive oversight for compliance, security, resource allocation, and approves significant operational changes or improvements.

- Service Coordination Committee (SCC)

Oversees day-to-day coordination of IT infrastructure services. This committee is directly responsible for operational performance, continuity of services, monitoring and reporting, and executing service-level objectives.

- IT Support Office

The operational entity dedicated explicitly to IT management, responsible for direct implementation, maintenance, and daily operation of the technical infrastructure. This unit is led by the designated Chief Technical Officer and comprises technical and operational staff from the partner institutions.

- Infrastructural administrator

Located at the RESILIENCE headquarters, this person provides administrative support specifically tailored to the needs of IT operations, including procurement, documentation, and communication related to IT service issues and incidents.

2.2 Roles and Responsibilities

The effectiveness of IT service operations within RESILIENCE depends on clearly defined and communicated roles:

- **Director:**
  - Approves strategic IT service management policies.
  - Makes strategic decisions regarding substantial investments or changes in IT services.
- **Chief Technical Officer:**
  - Directly responsible for operational management of IT services.

  - Ensures adherence to defined service-level objectives (SLOs), security policies, and operational guidelines.
  - Manages the IT operations team, coordinates technical maintenance activities, and resolves escalated incidents.

- **Service Coordination Committee (SCC):**
  - Coordinates the IT Support Office's activities with other operational units.
  - Monitors service-level performance, incidents, and user satisfaction.
  - Facilitates regular operational reviews and recommends improvements to the Director.

- **IT Support Office:**
  - Provides logistical and administrative support for IT operational processes.
  - Liaises for IT-related communication towards other governance bodies.
  - Responsible for daily operation, maintenance, and monitoring of IT infrastructure.
  - Handles technical support, incident management, routine updates, security audits, and compliance checks.
  - Oversees compliance with operational standards and security frameworks.
  - Reports directly to the Chief Technical Officer and indirectly to the SCC through regular service performance reporting

- **Infrastructural Administrator:**
  - Coordinates procurement, documentation, inventory management, and communication related to infrastructure services.

2.3 Decision-Making Processes

Effective IT operational governance relies on structured, transparent decision-making:

- **Strategic IT Decisions** (e.g., major infrastructure investments, new service adoption): Approved by the Director, based on recommendations and strategic analysis presented by the SCC and Chief Technical Officer.
- **Tactical IT Decisions** (e.g., routine service-level adjustments, operational improvements): Managed and decided by the Service Coordination Committee and the Chief Technical Officer, based on ongoing operational assessments, performance monitoring, and user feedback.
- **Operational IT Decisions** (e.g., daily management, incident response, maintenance activities): Handled directly by the Chief Technical Officer and IT Support Office, with regular reporting and coordination with SCC.
- **Incident and Problem Management Decisions**: Follow defined escalation processes, clearly documented in the Service Level Requirements (SLR) [R2] and approved by the SCC. High-impact incidents require immediate notification and potential intervention or approval by the Director.

All decisions are documented, monitored, and regularly reviewed to ensure ongoing compliance and operational excellence.

2.4 Interface with RESILIENCE Governance

The operational governance of IT services within the RESILIENCE Technical Infrastructure maintains clear and structured interfaces with broader RESILIENCE governance entities, as defined in the Governance set-up proceedings [R4] and refined in D1.1 RESILIENCE Statutes and Technical and Scientific Description [R5]:

- **Director:**
  - Acts as the primary interface for strategic and high-level operational alignment, resource authorization, and overall accountability for the performance of IT infrastructure services.
- **Service Coordination Committee (SCC):**
  - Serves as the main operational governance body, regularly interfacing with the Chief Technical Officer to report IT service performance, compliance status, risks, and recommended operational improvements.
- **IT Support Office:**
  - Provides regular, detailed operational reports to the SCC and escalates strategic-level issues to the Chief Technical Officer as required. It ensures transparent and efficient communication of operational metrics, incidents, and service-level adherence.
- **Support Office:**
  - Facilitates routine operational administration and documentation, ensuring seamless communication between operational staff, users, and governance bodies.

By clearly establishing these interfaces, RESILIENCE ensures integrated and robust governance of its IT services, effectively linking operational activities with strategic oversight, compliance, and continuous improvement objectives.

3 Service Level Management

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

The subsections of this chapter are detailed in SLR [R2].

3.1 Service Description

A clear description of IT services provided within the RESILIENCE Technical Infrastructure is fundamental for effective service management. Services include a variety of technical and user-oriented offerings, designed to ensure robust and reliable infrastructure supporting the RESILIENCE research community. Each service is clearly described by outlining its purpose, main functionalities, and essential components, including hardware, software, network infrastructure, and supporting systems.

Non-exhaustive examples of Services Provided:

- **Support Services**: Direct user support addressing queries effectively and promptly.
- **Helpdesk Operations**: A primary contact point providing immediate assistance and problem resolution.
- **Incident Management**: Management and resolution of service disruptions to ensure minimal impact on operations.

3.2 Service Level Objectives (SLOs)

Service Level Objectives (SLOs) define the measurable standards to which the RESILIENCE services adhere. These objectives ensure clarity, mutual understanding, and accountability, and they encompass key metrics such as:

- **Availability**: Defined percentage uptime, including clear descriptions of acceptable downtime and maintenance windows.
- **Performance**: Metrics including response times, throughput rates, and data processing speeds.
- **Reliability**: Specification of redundancy measures, failover mechanisms, and regular preventive maintenance practices.
- **Incident Response Time**: Clearly defined expected timeframes to acknowledge incidents, categorized by priority.
- **Resolution Time**: Timeframes for resolving incidents according to their severity, with procedures clearly outlined for escalation when initial resolution attempts are unsuccessful.

3.3 Measurement Criteria

Effective monitoring and assessment of service delivery rely on precise and clearly articulated measurement criteria, which include:

- **Metrics Definition**: Clearly identified performance metrics, ensuring each is Specific, Measurable, Achievable, Relevant, and Time-bound (SMART).
- **Measurement Methods**: Defined methods and standardized tools for accurate and consistent data collection and validation.

- **Data Collection Processes**: Structured procedures for routine data gathering, analysis, and storage. Regularly collected data is analysed to assess compliance with defined SLOs and to identify trends and opportunities for service improvement.

3.4 Reporting and Monitoring

Regular reporting and proactive monitoring are integral for continuous improvement and transparent communication with stakeholders:

- **Reporting Frequency**: Defined intervals for performance reports (monthly, quarterly, annually), differentiated by metrics as necessary.
- **Reporting Formats**: Clear, accessible formats such as dashboards, detailed reports, and summary presentations ensuring comprehension by all stakeholders.
- **Monitoring Tools and Techniques**: Use of specialized monitoring tools enabling real-time tracking of performance against objectives, proactive identification of issues, and implementation of preventive actions to maintain service standards.

3.5 Roles and Responsibilities

Clear allocation of responsibilities ensures effective service delivery and management. Roles are delineated between service providers and users:

- **RESILIENCE RI Responsibilities**:
  - Maintaining operational standards, managing incidents, performing preventive maintenance, and continuous performance monitoring.
  - Providing clear communication regarding service status and incident management processes.
- **Researchers Responsibilities**:
  - Prompt reporting of incidents, providing necessary information for issue resolution, and adhering to agreed service usage guidelines.
- **Escalation Procedures**:
  - Structured escalation hierarchy with defined contact points, enabling effective resolution of complex or unresolved incidents, clearly specifying levels of responsibility and communication pathways.

3.6 Service Review and Improvement

Service delivery undergoes continuous evaluation to identify and implement improvements:

- **Review Process**: Scheduled reviews of service performance against SLOs involving key stakeholders, ensuring alignment with user expectations and technological advancements.
- **Feedback Mechanisms**: Structured mechanisms to regularly gather and analyse feedback from service users, informing service enhancements and prioritizing improvements.
- **Continuous Improvement Procedures**: Established processes for testing, validating, and integrating improvements into service delivery, maintaining the relevance and effectiveness of RESILIENCE IT services.

3.7 Remedial Measures

Defined actions address failures to meet agreed service objectives, ensuring accountability and continuous operational improvement:

- **Failure to Meet SLOs**: Processes for identifying the root causes of performance failures, immediate corrective actions, and detailed documentation of incidents and resolutions.
- **Penalties and Compensation**: Clearly defined terms under which penalties or compensations are applicable, ensuring fairness and accountability.
- **Corrective Action Plans**: Structured corrective plans to prevent recurrence of identified issues, specifying responsibilities, implementation timelines, and review procedures.

3.8 Duration and Termination

Clear contractual terms outline the validity period and conditions governing the conclusion or renewal of Service Level Agreements (SLAs):

- **SLA Duration**: Explicit definitions of contract periods, including start and end dates, and conditions for possible extension or renewal.
- **Conditions for Termination**: Specific conditions under which either party may terminate the SLA, including required notice periods and any related costs or penalties.
- **Renewal Process**: Detailed description of processes for SLA renewal, including timelines, responsibilities, and approval requirements.

3.9 Amendments and Changes

Established processes ensure clarity, transparency, and stakeholder alignment regarding any amendments to the SLA:

- **Process for SLA Amendments**: Clearly outlined procedures for proposing, reviewing, and approving changes to service agreements.
- **Documentation of Changes**: Detailed record-keeping and documentation of all SLA modifications, maintaining version control and historical records for accountability.
- **Communication of Changes**: Transparent and timely dissemination of information regarding SLA changes to all stakeholders, ensuring clear understanding and continued agreement.

4 Operational Standards and Procedures

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

This section outlines the key operational standards and procedures for managing IT services within the RESILIENCE infrastructure. It covers compliance requirements, version control and change management processes, as well as guidelines for incident and request management.

4.1 Compliance with Standards

RESILIENCE will base its infrastructure on service providers that adopt industry best practices and relevant legal frameworks to ensure secure, efficient, and user-focused IT operations. The following subsections outline minimum expected standards in security, privacy, software development, and accessibility. Any specific procedures or controls implemented should be aligned with these overarching principles.

4.1.1 Security and Privacy Standards

Regulatory and Framework Adherence

RESILIENCE services must comply with GDPR requirements, as well as any applicable national regulations on data protection and user privacy.

ITIL security management principles are recognized as a long-term objective; relevant practices and processes should be progressively integrated as resources allow.

Technical Security Controls

While detailed controls (e.g., encryption in transit/at rest, multi-factor authentication) are not mandated in this policy, RESILIENCE service providers must demonstrate sufficient safeguards to protect data, consistent with GDPR and recognized good practices.

Potential examples include encryption, secure access controls, and periodic vulnerability assessments; the specifics of these controls should be defined when implementing the Operational Management Policy.

Compliance Reporting

Monthly reporting to the Chief Technical Officer is required from all IT service providers, highlighting security posture, any detected vulnerabilities, and incidents that occurred or were mitigated.

4.1.2 Software Development and Documentation Standards

All these standards have been developed in the Software Development Plan Template [R6].

Software Development Lifecycle (SDLC)

RESILIENCE follows Agile and Scrum methodologies for software development. All teams involved in developing or maintaining software must plan, implement, and iterate in accordance with these methodologies.

Open Science/Open Source Standards

RESILIENCE encourages use of open-source technologies and aims to align with open science principles. Repositories must be managed in a transparent, collaborative manner, supporting knowledge sharing and community-driven development.

Reference to Existing Documentation Guidelines

A dedicated Software Development Plan (SDP) template [R6] and associated guidelines exist to standardize coding practices, version control usage, and documentation artifacts.

This Operational Management Policy does not introduce additional documentation requirements; rather, it references the approved SDP for details on requirements, design documents, testing, and release notes.

4.1.3 Accessibility and Usability Standards

Public Funding Requirements

Because RESILIENCE is publicly funded, user-facing systems must adhere to commonly accepted usability and accessibility guidelines, such as WCAG 2.1 principles where feasible.

Any interfaces, portals, or websites serving researchers or the public should ensure inclusive access.

Future Testing and Guidelines

Although no formal usability testing framework is in place yet, RESILIENCE acknowledges the importance of user experience (UX) testing. Procedures will be defined to incorporate accessibility and usability reviews into all front-end IT products, projects, and services as they mature.

4.2 Version Control and Change Management

Version Control Tools

Git is the mandated version control system for all software projects under RESILIENCE. Repositories must follow best practices, including clear commit messages, feature branches, and merge reviews.

Change Advisory Board (CAB)

While a dedicated CAB is not yet established, this policy recognizes the importance of having a formal approval process for production-critical changes. The Service Coordination Committee, or a sub-group designated by it, may serve in this advisory capacity until a standalone CAB is formed.

Release Management

Release management procedures (e.g., designated release windows, notifications to stakeholders, and roll-back plans) are defined in the Software Development Plan [R6] This includes tracking release versions in Git and ensuring that any new release meets necessary testing and documentation requirements.

4.3 Incident Management Procedures

Classification of Incidents

RESILIENCE follows the classification system defined in the SLR [R2] document, which categorizes incidents (e.g., Critical, High, Medium, Low) and sets associated response times.

Incident Reporting and Tools

The specific incident management platform is not yet defined. Possible solutions include Jira Service Desk, ServiceNow, or a tailored portal.

Incident reporting should be standardized across RESILIENCE services, ensuring all users know how to escalate issues.

Incident Response

The IT Support Office handles incident responses, investigations, and resolution activities.

ITIL-Informed Practices

RESILIENCE incident response aligns with ITIL principles to ensure consistent processes for triage, analysis, resolution, and post-incident review.

4.4 Request Management Procedures

Differentiation Between Incidents and Requests

Incidents relate to service disruptions or failures (e.g., bugs, outages), whereas Requests (often new features or enhancements) capture user-driven improvements to existing services.

User Request Channels

A service on RESILIENCE portal (e.g. a contact form, or feedback form) will be in place for researchers and other stakeholders to submit requests, directed towards the RI Helpdesk and then forwarded to the relevant body or person. Users should receive clear guidance on how to log feature enhancements or routine service requests.

Prioritization and Approval Workflow

Currently, there is no formal priority-setting workflow for user requests. The Chief Technical Officer, in collaboration with the Service Coordination Committee, is expected to develop a priority management system that ensures transparent evaluation, approval, and scheduling of new requests.

5 Risk Management

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

RESILIENCE recognizes that proactive risk management is essential for maintaining service reliability, protecting data, and ensuring compliance with internal policies and external regulations. This section outlines the framework for identifying, assessing, mitigating, and reporting risks related to IT operations.

5.1 Risk Identification and Assessment

Internal Procedures

RESILIENCE does not currently adopt a formal industry-standard risk management framework (such as ISO 31000 or NIST SP 800-30). Instead, it employs an internal, generic procedure tailored to the organization's scale and resource constraints. This procedure is detailed in section 4 of D6.4 Quality Assessment Plan [R7].

Responsibilities

Both the IT Support Office and the Service Coordination Committee (SCC) are jointly responsible for identifying and reviewing new or evolving risks.

Risks may be discovered through routine operations, incident reports, audits, or ad hoc observations by staff and stakeholders.

Risk Categorization and Matrix

Identified risks are evaluated based on likelihood and impact, plotted on a risk matrix to determine priority and urgency.

Acceptable risk thresholds are established by the SCC in consultation with the IT Support Office, ensuring alignment with RESILIENCE's strategic objectives and available resources.

5.2 Risk Mitigation Strategies

Standard Controls

Backups, disaster recovery testing, patch management, and other preventive controls are documented as part of RESILIENCE's baseline mitigation strategies. These measures help minimize service downtime, data loss, and security breaches.

Budget and Resource Allocation

The Research Infrastructure must forecast budgetary needs to address critical or high-priority risks. Where shortfalls exist, the SCC should be informed of the potential impact on service continuity or data protection, and any decisions to accept residual risks must be formally recorded.

5.3 Risk Monitoring and Reporting

Frequency of Reviews and Audits

- Monthly Risk Reviews: The IT Support Office and SCC conduct regular risk evaluations at least once a month, focusing on newly identified risks, the status of ongoing mitigations, and any changes in impact or likelihood.
- Annual Risk Audits: A more in-depth audit is performed yearly, reviewing the effectiveness of existing controls, identifying emerging threats, and ensuring alignment with the Operational Management Policy.

Reporting Requirements

- Monthly Reports: The Chief Technical Officer consolidates risk-related updates and submits them to the SCC and, if necessary, the Director. These reports summarize new risks, status of mitigations, and potential resource implications.

6 Security and Privacy Management

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

RESILIENCE is committed to safeguarding data integrity, confidentiality, and availability while ensuring compliance with GDPR, national regulations, and best practices in security management. This section clarifies the overarching protocols and responsibilities in maintaining a secure infrastructure and protecting user privacy.

6.1 Security Protocols

Network Security

The RI recognizes the importance of robust network security measures (e.g., firewalls, IDS/IPS, VPNs, and segmentation). However, RESILIENCE itself will rely upon an external IT infrastructure provider (such as D4Science or similar) to implement and maintain these network-level protections.

Physical Security

Since RESILIENCE does not directly manage its own data centres or physical servers, physical security is outside its direct scope. The RI expects all third-party infrastructure providers to maintain industry-standard physical security measures.

6.2 Data Protection and Encryption

Data Classification

RESILIENCE aligns with GDPR principles for classifying and handling data according to sensitivity. Data must be processed in accordance with legal requirements for notice, consent, and purpose limitation.

Encryption Requirements

While the RI does not enforce explicit encryption policies beyond current web standards, data in transit (e.g., via HTTPS/TLS) and data at rest should generally conform to recognized best practices.

These requirements are typically handled by the external infrastructure provider, ensuring modern cryptographic protocols.

Key Management Procedures

No formal key management procedures currently exist under the RI's direct control. Where cryptographic keys are utilized by third-party providers, these entities are responsible for secure key generation, storage, and rotation as part of the contractual agreement.

6.3 Compliance with Regulations (GDPR, etc.)

Data Protection Officer (DPO)

A formal Data Protection Officer role is not yet officially appointed within RESILIENCE. However, the policy acknowledges the need for such a role or an equivalent function to:

- Monitor ongoing compliance with GDPR and other privacy regulations,
- Act as a contact point for data subjects and supervisory authorities,
- Advise on data protection impact assessments (DPIAs) and related processes.

Data Processing Agreements (DPAs)

RESILIENCE does not currently have formal DPAs with its external providers or partners. As the infrastructure and services mature, the RI may establish DPAs to clarify responsibilities, data ownership, and compliance obligations for all parties.

6.4 User Privacy and Confidentiality

Access Controls and Authentication

RESILIENCE will adopt federated academic authentication (e.g. based upon Keycloak) or comparable identity management solutions. This approach ensures strict data access controls and robust auditing of user activity.

Data Retention Policies

RESILIENCE is required to retain certain datasets for a minimum of 10 years, in line with EU directives and research funding obligations.

The IT Support Office and SCC must collaborate to develop a formal retention policy, outlining how long data is retained, how it is stored, and how it is eventually deleted or anonymized. This policy must reflect both regulatory obligations and user privacy considerations.

7 Training and Documentation

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

RESILIENCE recognizes that effective training and comprehensive documentation are critical to ensuring that users, developers, and support staff can fully leverage the Research Infrastructure's IT services and platforms. This section outlines the framework for planning, delivering, and continuously improving training programs, as well as managing all relevant documentation.

RESILIENCE Training Services Management Plan (D2.6) [R8] defines the overall model for planning and delivering RESILIENCE training services.

7.1 End-User Training

7.1.1 Structured Onboarding and Training

To satisfy the "onboarding to the RI" requirement, this plan includes:

- **Training Prototypes**: Tested pilot courses that provide models for future training offerings.
- **Training Management Compendium**: A living resource containing standardized guidance on lesson plans, course descriptions, evaluation methods, and didactic best practices.
- **Needs Assessment**: Ongoing mechanisms to identify and prioritize user training needs, informed by user surveys, focus groups, and feedback loops (WP3).

We present also various modes of courses delivery such as:

- **Online/Remote**: Live remote sessions with mandatory helpdesk or orientation components to address technical prerequisites.
- **On-Site/Workshops**: In-person training sessions, often featuring hands-on exercises with physical sources (e.g., archives, libraries, or religious sites).
- **Hybrid Formats**: Where feasible, training materials and sessions may be combined or recorded for asynchronous use (e.g., video tutorials, e-learning modules).

As specified in R8, the on-boarding sessions are called **Orientation Sessions** so that before any multi-day or advanced training, participants are offered (or required to attend) a short online orientation or helpdesk session covering:

- Technical setup (e.g., required software, environment prerequisites).
- Course logistics and expected learning outcomes.
- Guidance on addressing potential technical or disciplinary challenges.

7.1.2 Training Content and Learning Outcomes

What are the Focus Areas of the RESILIENCE Training Management Plan?

- Use of digital tools for text analysis, data management, and collaboration, as highlighted by the prototype "Uncovering Intertextuality through Digital Tools."
- Enrichment of research methods in the study of religion, e.g., exploring tangible and intangible religious sources ("Religion for the Senses").

- Cross-cutting competencies in Research Data Management (FAIR data principles), open science, and ethical/cultural sensitivity.

Our approach to training is endorsed by:

- Interactive Sessions: Group discussions, problem-solving activities, and hands-on tasks after each learning unit.
- Train-the-Trainer: Select courses (especially advanced or highly specialized ones) may explicitly include guidance on how to replicate or scale training in other institutions.

As for any Training plan it is important to continuously evaluate it and improve it through:

- Standardized evaluation forms are distributed immediately post-training to capture participants' feedback on learning objectives, course content, and trainer performance.
- Feedback is analysed by the IT Support Office and Work Package on Training (WU "Training"), leading to iterative improvements in subsequent courses.

7.2 IT Technical and Support Staff Training

7.2.1 IT Technical and Security Awareness

Technical Skill Development

While the Training Services Management Plan [R8] primarily addresses end-user needs, developers and support staff also benefit from many of the same components—especially where new tools, platforms, or prototypes are being introduced.

Security and Compliance

Although not formally mandated at present, the OMP envisions periodic security awareness sessions for staff. These sessions would cover:

- GDPR and privacy compliance requirements in daily operations.
- Basic ITIL security management principles (aligned with Section 6).
- Handling sensitive or restricted data in line with best practices.

7.2.2 Continuous Professional Development

It is important that the RI resources are sufficiently trained to maintain the services of the RI. We'll perform this through:

- Internal Workshops**:** Staff members within the IT Support Office and Service Coordination Committee may conduct in-house workshops to share updates on tools, development pipelines, or new methodologies.

- External Training and Certifications: Where possible, RESILIENCE encourages IT and support staff to seek external certifications or specialized training (e.g., advanced data analytics, DevOps, or ITIL frameworks). Any budget considerations for such training are planned in coordination with the Service Coordination Committee.

7.3 Documentation Management

7.3.1 Storage, Version Control, and Accessibility

The storage and versioning of the RI documentation can be hosted in a centralised repository:

- Zenodo: All publicly shareable training materials are deposited in the RESILIENCE community on Zenodo. This approach aligns with FAIR principles, ensuring persistent identifiers (DOIs) and open licensing (e.g., Creative Commons).
- Git: Source code, technical documentation, and certain training guides may be versioned in Git repositories to maintain transparency and enable collaborative updates.

The RESILIENCE Training Management Plan and any core policy documents (e.g., the OMP itself) are treated as living documents, subject to periodic review by the Chief Technical Officer and relevant stakeholders.

7.3.2 Regular Review and Updating

As for any management of documentation, the RI documents must be the subject of periodical review and update. Here is a proposed review schedule.

- **Annual Reviews**
  Training documentation, lesson plans, and reference materials should be reviewed regularly (at least annually) to reflect:
  - Newly identified user needs or emerging tools.
  - Feedback from course evaluations.
  - Updates to regulatory or compliance requirements.
- **Archival and Retirement**
  Outdated materials (e.g., old software guides, deprecated tool instructions) must be clearly labelled as "Archived" or "Superseded" to prevent confusion among trainers or participants.
- **Version Control**
  The Chief Technical Officer oversees version control best practices, ensuring that updates to training documents (lesson plans, compendia, guides) are tracked with clear revision logs and approval workflows.

8 Maintenance and Sustainability

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

RESILIENCE is committed to ensuring the long-term viability and continuous improvement of its IT services. This section outlines the strategies and processes designed to maintain infrastructure stability, implement updates effectively, and plan for future sustainability.

8.1 Maintenance Strategy and Schedule

Preventive Maintenance

All RESILIENCE IT services follow a preventive maintenance schedule to reduce service disruptions and extend the lifecycle of hardware and software components.

Maintenance tasks may include security patching, database optimizations, server reboots, and hardware inspections, coordinated by the IT Support Office.

Scheduled Downtime

RESILIENCE aims to minimize downtime; however, regular maintenance windows (e.g., monthly or quarterly) are communicated in advance.

Where feasible, rolling updates or zero-downtime deployments are preferred to maintain service continuity.

Roles and Responsibilities

The Chief Technical Officer oversees maintenance planning, ensures staffing, and coordinates activities with service providers.

Technical staff in the IT Support Office execute tasks, document outcomes, and report major findings or concerns to the Service Coordination Committee (SCC).

8.2 Update and Upgrade Cycles

Software Versioning

As outlined in Section 4.2, Git repositories track all software changes.

Major, Minor, and Patch releases follow a formal process described in the Software Development Plan (SDP) [R6] ensuring transparency and rollback options.

Hardware and Third-Party Services

RESILIENCE relies on external IT infrastructure providers for hosting and certain network security measures. These providers typically dictate upgrade timelines for underlying infrastructure (e.g., OS updates, virtualization platforms).

The IT Support Office collaborates closely with these providers to schedule updates at times that minimize disruptions.

Security Patches

Critical security patches are applied as soon as practicable, with emergency deployments handled through an expedited change management process.

Monthly compliance reporting (see Section 4.1.1) includes summaries of applied patches and outstanding vulnerabilities.

8.3 Long-Term Sustainability Plan

Resource Allocation

The Director, in coordination with the CTO and SCC, ensures budget forecasts covering ongoing maintenance, anticipated upgrades, and future expansions.

Where critical or high-priority risks (see Section 5.2) require additional resources, the SCC escalates budget requests to the Director.

Lifecycle Planning

Eventual IT assets (servers, software licenses, network components) that would be the property of the RI are inventoried and assigned expected end-of-life dates to facilitate proactive procurement of replacements or renewals.

The Chief Technical Officer periodically reviews these lifecycles to align them with RESILIENCE's evolving needs.

Strategic Partnerships

Collaborations with external IT providers and academic consortia ensure shared expertise, co-development opportunities, and broader stakeholder engagement, thereby strengthening RESILIENCE's operational longevity.

9 Remedial Measures

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

Remedial measures provide structured responses to service failures, process breakdowns, or inability to meet established service-level objectives (SLOs). This section defines how RESILIENCE addresses, corrects, and learns from such occurrences.

9.1 Procedures for Addressing Service Failures

Incident Detection and Escalation

Incidents that may indicate service failures are recorded using the incident management procedures detailed in Section 4.3.

The Incident Response Team within the IT Support Office classifies the severity (Critical, High, Medium, Low), initiates immediate containment, and escalates to the SCC if needed.

Root Cause Analysis (RCA)

For significant or repetitive failures, an RCA is conducted to identify underlying technical or procedural issues.

RCA outcomes are documented in a Post-Incident Review (PIR), capturing detailed timelines, contributing factors, and recommended fixes.

Service Restoration

Temporary workarounds (e.g., failover, manual processes) may be employed until a permanent fix is implemented.

Once the service is restored, a formal closure process ensures all corrective actions are completed and validated.

9.2 Corrective Action Plans

Plan Development

A Corrective Action Plan (CAP) is prepared when a service failure significantly impacts operations or user satisfaction. This plan includes tasks, timelines, responsible parties, and success criteria.

The Chief Technical Officer drafts the CAP in conjunction with relevant technical staff, then seeks SCC approval where high-impact or cross-functional issues arise.

Ongoing Monitoring

The CAP progress is monitored during monthly risk reviews (see Section 5.3).

The IT Support Office provides updates to the SCC, highlighting any adjustments in scope or timeline to ensure timely resolution.

Reporting and Continuous Improvement

All major service failures and subsequent CAP outcomes are documented in monthly operational reports, shared with the SCC and the Director in case of high impact.

Lessons learned from these incidents inform process improvements, including possible amendments to standard operating procedures, training, or resource allocations.

10 Duration, Amendments, and Termination of the OMP

Note: The policies in this chapter present a proposed framework for the Implementation Phase of RESILIENCE. Until the IP is well underway and/or - if successful - the ERIC is formally established, the measures are advisory only and will be piloted where feasible.

This section clarifies how long the Operational Management Policy remains valid, under what conditions it may be updated, and the scenarios leading to its termination or replacement.

10.1 Policy Duration and Review Schedule

Initial Validity

This Operational Management Policy (OMP) is effective upon approval by the Directo and remains in force until superseded by an updated version or formally terminated.

Review Intervals

The OMP is reviewed annually to confirm its ongoing relevance and compliance with evolving regulations, user needs, and infrastructure changes.

Interim reviews may occur if new services are introduced or significant modifications to existing operations are required.

Responsible Entities

The Chief Technical Officer coordinates the review process in collaboration with the Service Coordination Committee (SCC).

Proposed amendments or major updates are presented to the Director for final approval.

10.2 Amendment Procedures

Proposing Amendments

Any governance body involved may propose changes to the OMP. Proposals must include a rationale, potential impacts, and revised policy text.

Amendments to sections covering compliance, security, or major resource allocation require Director's approval.

Documentation and Version Control

All updates or amendments are recorded with a new version number, date, and summary of changes.

Previous versions are archived for reference, ensuring clear policy evolution tracking.

Stakeholder Communication

Once approved, amendments are communicated to all operational teams and relevant stakeholders.

Mandatory briefing sessions or refresher training may be scheduled if amendments significantly alter roles, responsibilities, or processes.

10.3 Termination Conditions and Procedures

Conditions for Termination

A complete termination of this OMP may be warranted if the RESILIENCE consortium ceases operations, undergoes major restructuring (e.g., merges with another RI), or if a new overarching policy supersedes it entirely.

Notice Period

A written notice must be issued at least 60 days prior to termination, specifying the rationale and the effective date.

Exceptions to this notice period can apply in emergencies (e.g., regulatory directives, severe security breaches) but require explicit justification from the Director.

Transition and Handover

If a new policy or operational framework replaces the OMP, the Director and SCC ensure seamless transition, preserving essential processes and documentation.

The Chief Technical Officer remains responsible for final archival of the retiring policy and for briefing relevant parties on new or updated governance structures.

11 Reference Documents

Reference documents are intended to provide background and supplementary information.

ID	Date	Title/Reference
[R1]	18/08/2022	GRANT AGREEMENT Project 101079792 — RESILIENCE PPP
[R2]	30/05/2024	D2.9 Services Level Requirements (SLR)
[R3]	29/03/2024	D2.1 Services Preparation and Implementation Strategy
[R4]	30/09/2024	D6.1 Governance set-up proceedings
[R5]	28/11/2024	D1.1 RESILIENCE Statutes and Technical and Scientific Description
[R6]	15/11/2023	D2.8 Software Development Plan template
[R7]	30/05/2023	D6.4 Quality Assessment Plan
[R8]	28/11/2024	D2.6 Beta Training Services Management Plan

Funded by
the European Union