RESILIENCE

Grant Agreement 101079792, RESILIENCE PPP

Security Management Plan (SMP)

Title of Deliverable:	Security Management Plan (SMP)		
Deliverable Number:	D2.7		
Type of Data:	Report		
Lead Beneficiary:	FSCIRE		
Publishing Status	Public		
Last Revision Date:	28/11/2023	**by:**	Rudy Demo, FSCIRE
Verification Date:	29/11/2023	**by:**	Board of Directors
Approval Date:	[DD/MM/YYYY]	**by:**	[Name]
Document Name:	RESILIENCE_WP2_D2.7_Security_Mgt_Plan_01.00_FINAL		

Funded by
the European Union

Change History

Version Number	Date	Status	Name	Summary of Main Changes
00.01	17/11/2023	DRAFT	Initial Draft	
00.02	22/11/2023	DRAFT	First Revised Text	Revision according to comments from KU Leuven Team members
00.03	27/11/2023	DRAFT	BoD Revised Text	Minor comments
01.00	29/11/2023	FINAL	Final Version	

Author(s)

Name	Beneficiary	Role
Rudy Demo	FSCIRE	WP2 Team member

Distribution List

Name	Beneficiary	Role
Public	All	

Table of Contents

Acronyms

Acronym	Full Name
AAI	Authentication and Authorization Infrastructure
CI	Continuous Integration
DAST	Dynamic Application Security Testing
DPO	Data Protection Officer
ERIC	European Research Infrastructure Consortium
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
IaC	Infrastructure as Code
SMS	Information Security Management System
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
SMS	Information Security Management System
KPI	Key Performance Indicator
ORCID	Open Researcher and Contributor ID
OWASP	Open Web Application Security Project
PDCA	Plan-Do-Check-Act
PII	Personal Identifiable Information
RESILIENCE RI	RESILIENCE Research Infrastructure
RI	Research Infrastructure
RI-DPO	Research Infrastructure Data Protection Officer
RI-OSO	Research Infrastructure Operational Security Officer
RI-PSO	Research Infrastructure Project Security Officer
RI-SM	Research Infrastructure Security Manager
RI-SO	Research Infrastructure Security Office
SaaS	Software as a Service
SAST	Static Application Security Testing
SCM	Security Checked Member
SDLC	Secure Development Lifecycle
SIEM	Security Information and Event Management
SMART	Specific, Measurable, Assignable, Realistic, Time-bound
SMP	Security Management Plan
SPP	Security Policy and Procedures

Definitions

Term	Definition
Security Management System	A Security Management System (SMS) is a comprehensive organizational framework designed to manage and oversee all aspects of security, including policies, procedures, and controls, to protect an organization's assets, people, and operations from security risks and threats.

List of Figures

List of Tables

1 Introduction

1.1 Objectives of this document

1.1.1 From the proposal

Extract from [R1]:" The Security Management Plan is elaborated to define all aspects of the working practices of the project to guarantee secure delivery. It contains a Secure Coding/Development Guidelines aligned with "ISO/IEC 27034 Information technology – Security techniques", the OWASP Developer Guide, Testing Guide and Top-10 Application Security Risks."

1.1.2 Long-term objectives

The Security Management Plan for a research infrastructure like RESILIENCE is a comprehensive document that encompasses the entirety of the project's security landscape. The plan needs to cover not just the technical nuances of software development and deployment, but also the operational, administrative, and physical aspects of security. Therefore, RESILIENCE aims at offering a holistic approach to security that touches every facet of the infrastructure, ensuring all components, from data storage mechanisms to software application layers, are fortified in accordance with international best practices such as ISO/IEC 27034.

Central to our objectives is **the safeguarding of research data and providing our research community** with the confidence that the offered infrastructure can maintain their work's privacy and integrity.

RESILIENCE security approach is fully integrated into the RI IT development process. The plan emphasizes **embedding security practices throughout the software development lifecycle** (See also RESILIENCE Software Development Template). This covers every phase, from initial design and development to testing, deployment, and ongoing maintenance. An essential part of this objective is to provide **adequate training and raise awareness on security** among all staff, developers, and stakeholders. RESILIENCE seeks to familiarize them with critical resources, notably the OWASP Developer Guide, Testing Guide, and the Top-10 Application Security Risks.

Continuous security monitoring of the infrastructure is vital for real-time threat detection and rapid response, ensuring minimal system downtime and offering robust defense against potential attacks. Moreover, a meticulously planned access control and authentication system will be in place to ensure that researchers have access only to the tools and data pertinent to their work. This serves the dual purpose of enhancing usability while safeguarding against unauthorized intrusions.

Auditing and logging stand as pillars of our security strategy, providing a comprehensive record of pre-defined user actions and system events. Where necessary, a logging mechanism will allow for regular audits, ensuring timely detection of any anomalies or breaches in the system.

Given the evolving nature of security threats, the infrastructure will undergo **periodical security assessments to identify vulnerabilities and ensure protection against the latest risks**. In tandem with this, RESILIENCE will establish a clear incident response plan to address any breaches, ensuring that affected parties are informed promptly and that measures are in place for swift remediation.

Ensuring security is not just limited to RESILIENCE immediate infrastructure. All third-party vendors, software, and integrated services should report adhesion to similar security standards. With the ever-growing pervasiveness of data in the research domain, we will prioritize the establishment of **robust data backup processes, coupled with a disaster recovery plan**, ensuring the seamless continuity of research even in the face of data loss or significant system failures.

Remaining **compliant with national and international data protection and privacy regulations** is of paramount importance such as GDPR, and RESILIENCE will continuously update its systems and practices to meet these standards. Finally, RESILIENCE believe that collaboration is key to security. Thus, RESILIENCE aims to foster an environment of **active collaboration between researchers, developers, and other stakeholders**, allowing for shared insights and continuous feedback. Through this collective effort, the RESILIENCE Research Infrastructure is poised to uphold the sanctity of religious studies and the trust of its researchers via best-in-class security practices.

1.2 Scalability of the Security Management Plan

For the understanding of this document, it is important to emphasise that it considers the need and possibility of the RI to grow and scale up during the following phases.

The following two points inform the decision to take scalability into account:

1) It is at this point uncertain what the eventual size and budget of the RESILIENCE RI will be for the entire decades' long lifespan of the RESILIENCE ERIC.

2) It is important to account for the size and scale of an organisation in planning security management. For example, depending on the size of the central technical infrastructure, the roles of the security office could be implemented by a team of several security staff or while the RI is still in its emerging phase, by a part-time staff member endorsing several roles. The same remark is valid for processes, meetings and reports that can be reduced, aggregated, or expanded depending on the size and budget of the RI. Also, some services might be implemented by third-party stakeholders that might also impact the security resources involved in carrying on the SMP.

Because the eventual size and budget of RESILIENCE is difficult to predict, it is therefore beneficial to be able to scale up in the future and to plan for this scalability.

The evolution of presently existing technologies and its future costs is also constantly changing. This means that the feasibility of certain measures can improve over time.

Therefore, this document covers both what is minimally required for a security management plan and the ideal implementation for a firmly established RI. During the coming phases of the RI more measures can be implemented as they become possible and/or necessary.

1.3 Discriminative Application of the Security Management Plan

The Security Management Plan (SMP) must be discriminatively applied to effectively manage the diverse nature of resources within the Research Infrastructure (RI). The application of the SMP takes into consideration the distinction between in-kind contributions and in-house created resources.

This section delineates the tailored application of the SMP to these factors.

Application of the SMP to in-kind contributions:

- Contributors of in-kind resources are expected to adhere to a baseline security protocol as recommended by the RI. They will be asked to confirm this adherence when submitting their contribution meta-data.
- The RI will not directly manage or store highly sensitive data from in-kind contributions. Contributors must ensure that data is properly anonymized before integration into the RI's systems.
- A disclaimer will be provided to contributors of in-kind resources, outlining the non- liability of the RI concerning the security of these resources and the obligation of contributors to meet a minimum recommended set of security standards. These standards include essential security measures such as virus-checked data before submission, documenting the level of respect of OWASP Application Security Verification Standard (level 1 to 3), usage of data encryption for data depending on their sensitivity, access control, and user authentication compatible with the RI recommendations, etc.

Application of the SMP to in-house created resources:

- In-house created resources must fully adhere to the security framework developed by the RI. This framework will include advanced security measures and controls tailored to the specific risks associated with these resources. Exceptions to this compliance might be defined by the RI Security Office.
- Regular security audits and assessments will be conducted to ensure that in-house resources maintain the highest level of security integrity.
- In-house resources should not include sensitive data as the RI does not recommend hosting this data on the RI platform. For the storage of this data, researchers should use secure environments only.

1.4 Protection of Data

RESILIENCE is committed to data protection. In alignment with our policies, RESILIENCE does not host sensitive or personally identifiable information (PII). Here is how RESILIENCE ensures the protection of the data:

- **Data Hosting Policy**: RESILIENCE RI only hosts and manages non-sensitive, non-personal data. Researchers must ensure that any data classified as sensitive or containing PII is appropriately anonymized prior to submission to our infrastructure.
- **Data Anonymization Confirmation**: Prior to hosting data, RESILIENCE requires researchers to confirm that all datasets have been stripped of PII or any sensitive information, and that they comply with applicable data protection standards.
- **Security Measures for Non-Sensitive Data**: Even non-sensitive data is protected with robust security measures including encryption in transit and at rest, along with secure storage solutions to safeguard against unauthorized access and potential security threats.
- **Access Control**: Access to restricted research data, while non-sensitive, is still controlled and monitored. RESILIENCE implements the principle of least privilege, ensuring that only authorized staff have access to the data necessary for their role.

- **Regular Security Audits**: security protocols of the RI are subject to regular internal audits to verify that data is managed in a secure environment and that the infrastructure remains in compliance with established data protection standards.
- **Training and Awareness**: Comprehensive training on data security is provided to all staff members, emphasizing the importance of maintaining the non-sensitive nature of the hosted data and the procedures to manage it securely.
- **Transparent Data Policy**: A clear and transparent data policy is communicated to all researchers, detailing the types of data RESILIENCE can host and the responsibilities of researchers in ensuring the non-sensitivity of their data before sharing it with RESILIENCE.

Data Protection Officer (DPO) Engagement: RESILIENCE engages with a designated DPO to oversee the data protection policies and ensure that RESILIENCE does not host sensitive data.

2 RESILIENCE Security Approach

RESILIENCE Security[1] approach will ensure that all aspects of the RESILIENCE services, ranging from data storage to software and services application layers, are secured according to international best practices, leveraging frameworks and standards such as ISO/IEC 27000 series standards.

- Adoption of ISO/IEC 27000 series for the definition of a security framework and guidelines.
- Adoption of DevSecOps as Software Development Lifecycle oriented towards security.
- Adoption of OWASP (Open Web Application Security Project) guidelines for a standardized and consistent way of performing security assessments.
- A Plan-Do-Check-Act approach, which ensures monitoring and continuous improvement of results.
- A Security Office team performing at RI level.

2.1 Standard Frameworks and Best practices

The Standard Frameworks proposed to establish the RESILIENCE Security Policy and Procedures (SPP) will include the **ISO27K security standards** such as:

- ISO/IEC 27000 Information security management systems – Overview and Vocabulary
- ISO/IEC 27004 Information security management
- ISO/IEC 27033 Network security
- ISO/IEC 27034 Application security
- ISO/IEC 27035 Information security incident management
- ISO/IEC 27036 Information security for supplier relationships, in case the RI would consider requesting products and/or services from suppliers.
- ISO/IEC 27040 Storage security

Among the best practices it is worth mentioning **OWASP**. Adopting OWASP best practices for RESILIENCE is a strategic decision that ensures a comprehensive application of security, aligns with global industry

[1] Covering in-house contribution and central services hosted by the RI.

standards, and effectively mitigates common vulnerabilities. OWASP's extensive, up-to-date guidelines and resources support the creation of secure software vital for research and data management. This adoption may not only enhance credibility and trust in our infrastructure but also ensure compliance with data protection regulations. Additionally, OWASP's community support and cost-effective, open-source tools provide an adaptable, scalable solution that grows with the RI's evolving needs, making it a practical and forward-thinking choice for safeguarding its IT environment.

2.2 RESILIENCE Security Management System (SMS)

Maintaining robust RI security is not just a necessity but a cornerstone for success and reliability. At RESILIENCE, the Security Management System (SMS) will be designed to safeguard infrastructure, data, and human resources from a wide array of security threats. The SMS at RESILIENCE will be a comprehensive framework that integrates advanced tooling, rigorous policies, effective governance, and continuous human resource development. RESILIENCE SMS should embody a proactive, strategic approach to managing risks, ensuring compliance with regulatory standards, and fostering a culture of security awareness throughout the organization. The following sections delve into the key components of the RESILIENCE SMS, illustrating how each element contributes to creating a secure, efficient, and resilient research environment.

2.2.1 Security Policy and Procedures (SPP)

The cornerstone of the SMS at RESILIENCE will be a robust and comprehensive Security Policy and Procedures (See SPP at section 8.1) to be defined at the start of the Implementation Phase. This policy will outline an approach to protecting both physical and digital assets, data integrity, and the welfare of all personnel and stakeholders involved. The SPP will encompass guidelines on acceptable use of resources, data handling procedures, incident response protocols, and specific policies addressing areas like remote access, mobile device management, and encryption standards. Regular reviews will ensure that the SPP stays aligned with evolving threats, technological advancements, and regulatory changes, particularly in the context of religious studies research.

2.2.2 Governance

At the heart of RESILIENCE's SMS will be a strong governance structure, ensuring accountability and efficient oversight of security practices. The governance framework includes a dedicated Security Office, responsible for strategy, policy development, and compliance monitoring. This office works in conjunction with various stakeholders, including IT teams, department heads, and external advisors, to ensure a holistic security approach. Periodical security audits, risk assessments, and management reviews will be conducted to maintain high standards of security and to adapt to new challenges and opportunities in the field of research infrastructure.

2.2.3 Tooling

The implementation and selection of security tools are pivotal aspects of the Security Management System (SMS) at RESILIENCE. Such an approach bifurcates to address the diverse security needs of our federated RI entities (as described in our proposed 4T security model See more at section 8.2) and the centralized IT infrastructure and offices of the members of RESILIENCE.

1. **Federated RI Entities (Trusted Organizations and Workplaces):**

- In these entities, which are integral parts of our federated structure, each member is considered a 'Trusted Organization' providing 'Trusted Workplaces'. They are responsible for implementing their own security measures.

2. **Centralized IT Infrastructure and Offices of RESILIENCE:**
   - The security of the core IT infrastructure and RESILIENCE's offices falls under the direct responsibility of the Security Office team.
   - While the technical infrastructure will be set-up by the RI or provided by a third-party entity, the centralized security toolset will encompass advanced cybersecurity software, including sophisticated intrusion detection systems, enterprise-level firewalls, and comprehensive antivirus solutions.
   - For data protection, if needed, RESILIENCE will utilize advanced encryption methods to secure data both at rest and during transmission.
   - To maintain the highest security standards, RESILIENCE will leverage automated tools for consistent security assessments, vulnerability scanning, and compliance checks. This ensures that the security measures are continuously updated and effective in countering emerging threats.

3 Governance Structure

The security office is a scalable entity, designed to adapt its size and functions according to the RESILIENCE ERIC's evolving needs, budget, and infrastructure.

3.1 RI Security Office

The Security Office will oversee defining the RI information security strategy, identifying security risks in the critical activities, and, as a result, approving the strategic security measures and plans for mitigating the risks to within acceptable margins and the achievement of the defined security goals.

The Security Office will oversee the creation, approval, revision and dissemination of the information Security Policy, Procedures and Norms, as well as the provision of the economic, technical, and human resources needed to achieve the RI strategic security plans.

The Security Office will also be responsible for the promotion of the information security culture among the RI partners' staff, with the commitment and support of each RESILIENCE partner, defending the strategic security goals.

The Security Office will establish a "community of security practices" where representatives of RESILIENCE partners' security offices, can on a volunteer basis share their experience and information on security best practices allowing the establishment of a more effective security governance.

3.1.1 The RI Security Manager (RI-SM) role

The RI-SM will be responsible for coordinating the RESILIENCE Security Office and orchestrating the security operations within the RESILIENCE Research Infrastructure over the lifespan of the ERIC. The RI-SM's obligations encompass the following key areas:

- Policy Formulation and Evolution:
  - Formulate the Information Security Policy and accompanying procedures, tailoring them to the dynamic needs of RESILIENCE in conjunction with stakeholders involved in RI security.
- Risk Identification and Prioritization:
  - Systematically identify information security risks and orchestrate the development and prioritization of security controls and countermeasures.
- Security Controls Lifecycle Management:
  - Manage the lifecycle of security controls from design to implementation, operation, and ongoing validation, ensuring they adhere to the Security Policy and leverage the Plan-Do-Check-Act (PDCA) cycle for continuous refinement.
- Incident Command and Oversight:
  - Command the response to information security incidents within the RI, ensuring effective management and minimization of operational impact.
- Compliance Supervision:
  - Supervise the adherence to the Information Security Policy and associated procedures, guaranteeing consistent compliance across the RI.
- Training Coordination and Advocacy:
  - Coordinate the planning and execution of information security training and awareness initiatives in line with the Security Awareness Plan, advocating for a pervasive security culture throughout the infrastructure.

The RI-SM will be supported by the Operational and Project Security Officers in all its activities.

3.1.2 The RI Operational Security Officer (RI-OSO) role

The RI-OSO will be responsible for the overall implementation of the RI security policy and procedures including the following aspects:

- Implementation of Security Measures:
  - Execute the strategic security plans and measures approved by the RI Security Office.
  - Ensure operational alignment with the RI's Information Security Policy and norms.
- Security Controls and Monitoring:
  - Monitor the efficiency and effectiveness of security controls.
  - Conduct regular security assessments to ensure ongoing compliance with the established security policies.
- Resource Management:
  - Manage the allocation of technical and human resources for operational security tasks.
  - Oversee the operational budget designated for security implementations.
- Incident Response:
  - Serve as a primary contact for operational-level security incidents.
  - Coordinate rapid response to security incidents, including mitigation and recovery efforts.
- Training and Support:
  - Provide operational-level training and support to RI staff for security-related activities.

- Facilitate the dissemination of security updates and protocols to the relevant operational staff.

- Reporting and Documentation:
  - Maintain thorough documentation of all operational security measures and incidents.
  - Report on operational security status to the RI Security Manager (RI-SM) and the Security Office.
- Partnership and Collaboration:
  - Collaborate with the representatives of the RESILIENCE partners' security offices to incorporate diverse experiences and best practices into the operational security approach.

3.1.3 The RI Project Security Officer (RI-PSO) role

During the life of the ERIC, the Research Infrastructure will implement numerous projects to provide state-of-the art research software and services to the religious studies researchers' community. For each key project endorsed during the ERIC, a RI-PSO might be named by the RI Security Office to ensure that the security policy and procedures applying to a specific project are known and ensured during the lifecycle of the project. These responsibilities endorsed by the RI-PSO cover the following aspects:

- Security Planning for Projects:
  - Develop and maintain project-specific security plans aligned with the overall RI security strategy.
  - Ensure that project plans include appropriate security controls and risk mitigation strategies.
- Risk Management:
  - Identify and evaluate security risks specific to each project within the RI.
  - Prioritize and coordinate the implementation of security measures for projects.
- Security Compliance:
  - Ensure that projects comply with the RI's Information Security Policy and procedures.
  - Coordinate security audits and assessments for projects to ensure adherence to security standards.
- Incident Management:
  - Manage security incidents within project boundaries, coordinating with the RI-OSO and RI-SM as necessary.
  - Ensure that all project-related incidents are properly documented and resolved.
- Security Objectives and Verification:
  - Work with the RI-SM to define measurable security objectives for projects.
  - Verify the achievement of security objectives through regular monitoring and reporting.
- Awareness and Training:
  - Promote security awareness within project teams.
  - Coordinate with the RI-SM to deliver project-specific security training and exercises.
- Collaboration:
  - Act as a liaison between the project teams and the RI Security Office.
  - Facilitate communication and collaboration on security matters between project stakeholders and the broader RI security governance structure.

3.1.4 The RI Data Protection Officer (RI-DPO) role

The RI Data Protection Officer (RI-DPO) plays a crucial role in ensuring that the RESILIENCE Research Infrastructure adheres to data protection laws and best practices throughout its operations. The RI-DPO is responsible for overseeing the implementation of data protection strategies, providing guidance on data privacy laws, and ensuring the rights of data subjects are respected. The responsibilities of the RI-DPO include:

- Policy Development and Implementation:
  - Develop, maintain, and update comprehensive data protection policies in line with current laws and standards.
  - Ensure that data protection measures are integrated into the infrastructure's processes and services.
- Compliance Monitoring:
  - Monitor RESILIENCE's compliance with data protection policies, GDPR, and other relevant laws.
  - Conduct regular audits to ensure data processing activities are compliant.
- Training and Awareness:
  - Lead training initiatives and awareness programs to educate staff on data protection responsibilities.
  - Ensure continuous awareness of data protection across all levels of the RI.
- Advisory Services:
  - Act as an advisor to the RI on all data protection matters, including data processing operations and data security strategies.
  - Provide guidance on data protection impact assessments for new projects or changes in services.
- Risk Assessment:
  - Identify and evaluate the risks associated with data processing activities within the RI.
  - Recommend measures to mitigate identified risks to data privacy and security.
- Incident Response and Reporting:
  - Serve as the point of contact for data protection issues, breaches, and inquiries from data subjects.
  - Report and document any data breaches in accordance with legal requirements and communicate effectively with the supervisory authorities and affected data subjects.
- Data Subject Rights:
  - Ensure mechanisms are in place to respond to data subjects' requests to exercise their rights under data protection laws.
  - Maintain records of data processing activities and ensure transparency with data subjects.
- Liaison with Authorities:
  - Act as the contact point for data protection authorities for all data protection issues.
  - Engage in dialogue with authorities on any actions taken or changes made regarding data protection.
- Review and Audit:

- Oversee the review of processing activities to ensure alignment with the data protection policies.
- Engage with external auditors for independent assessments when required.

3.2 External RI stakeholders' interactions with the Security Office

Each stakeholder category presented below could interact with the RI's security roles in unique ways, focusing on compliance, collaboration, legal and technical consultation, industry networking, and public engagement. These interactions could be vital for maintaining a robust and compliant security posture within the RI, adapting to evolving security landscapes and regulatory environments. These activities undertaken with these stakeholders span a range of natures and purposes, from mandatory and legal compliance to cooperative knowledge exchange, and from expertise-driven strategic consultancy to hands-on operational management, all potentially contributing to a robust and effective security framework within the RI.

1. Regulatory and Compliance Bodies

- **Stakeholders:** Data protection authorities, government regulatory agencies.
- **Interactions:**
  - **RI Security Office & RI-SM:** Ensure the compliance of our RI Security Policy and procedures with security and data protection regulations, report breaches, seek guidance on compliance matters.
  - **RI-OSO & RI-PSO:** Implement and monitor compliance-driven security measures and report compliance status.
  - **RI-DPO:** Regular communication for compliance, reporting breaches, and mandatory consultations.

2. Research Partners

- **Stakeholders:** research institutions, national/international research infrastructures and academic entities.
- **Interactions:**
  - **RI Security Office & RI-SM:** Collaborate on joint security initiatives, share best practices, and partake in joint research endeavours.
  - **RI-OSO & RI-PSO:** Coordinate on project-specific security protocols, especially in collaborative research projects.
  - **RI-DPO:** Exchange information on data protection best practices in research settings.

3. Legal and Advisory Services

- **Stakeholders:** Legal consultants, data protection advisors, external auditors.
- **Interactions:**
  - **RI Security Office & RI-SM:** Seek legal advice on security policies, compliance, and risk management.
  - **RI-OSO & RI-PSO:** Implement recommendations from legal and advisory services in operational and project security plans.

- **RI-DPO:** Consult on data protection laws, regulatory interpretations, and compliance.

4. Technology and Service Providers

- **Stakeholders:** IT service providers, security solution vendors, cloud service providers.
- **Interactions:**
  - **RI Security Office & RI-SM:** Assess and select technology solutions, manage vendor relationships.
  - **RI-OSO & RI-PSO:** Oversee the implementation of security solutions provided by external vendors in operational and project contexts.
  - **RI-DPO:** Ensure vendor compliance with data protection standards.

5. Security Professionals and Industry Organisations

- **Stakeholders:** Cybersecurity forums, data protection organizations, industry groups.
- **Interactions:**
  - **RI Security Office & RI-SM:** Engage in knowledge exchange, stay abreast of industry trends, and participate in collective security initiatives.
  - **RI-OSO & RI-PSO:** Gain insights into industry-specific security challenges and solutions.
  - **RI-DPO:** Network with peers in data protection, share best practices.

6. Public

- **Stakeholders:** General public, individuals whose data the RI processes.
- **Interactions:**
  - **RI Security Office & RI-SM:** Communicate security policies and practices to the public as necessary.
  - **RI-DPO:** Address inquiries and concerns about data privacy, ensure transparency in data handling practices.

4 Implementing the Security Management System

Once defined and agreed upon, the implementation of the SMS will be implemented by using a Plan-Do-Check-Act (PDCA) process approach:

- During the **Plan** phase, the RI Security Management System (SMS) will be designed by the Security Office and eventually supported by security specialists and partners' security offices. A Security Management System (SMS) refers to a systematic, comprehensive process designed to manage security risks and ensure the protection of the RI's assets, including its people, facilities, and information. SMS encompasses various aspects of security including the Security Policy and Procedures (See section 8.1). During this phase, the Security Office will define feasible objectives for the RI security governance that can be transformed into SMART (Specific, Measurable, Assignable, Realistic, Time-bound) indicators at the level of the RI. A couple of examples could be:
  - **For the Software Development lifecycle**: Number of high level vulnerabilities by lines of code, for new systems (e.g., concerning the new software developed by the RI – and if the implemented project approach to security is working well - not only we expect an initial low

number of vulnerabilities by lines of code, but also that this number will diminish over time, as the project will reach cruising speed);
    - **Software as a Services (SaaS)**: Rate of reduction of high and medium level vulnerabilities from first scanning, for existing systems (e.g., let's suppose that a first scan of an existing system shows 20 high/medium level vulnerabilities: the objective might be to have this figure diminished of 50% within 2 months and of 100% within 6 months).
- During the **Do** phase, the implementation of the SMS will be enacted, according to what was designed in the Plan phase.
- During the **Check** phase controls will be carried out by means of audits. Quantitative measures will also be taken wherever possible to have comparable results.
- During the **Act** phase, corrections and updates of the SMS will be applied based on the findings emerged in the Check phase.

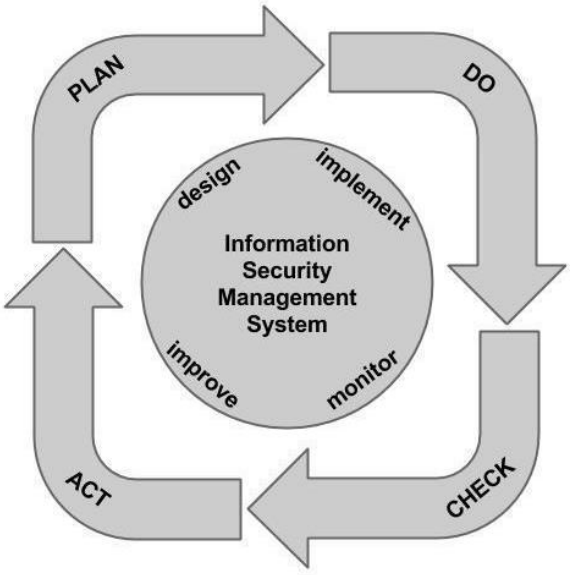

Figure 1: PDCA applied to the SMS

The Act phase of the PDCA cycle is specifically the one that guarantees the continuous improvement process, which is a mandatory characteristic in the fast-changing world of IT Security. Security related objectives will be defined in the Security Policy and monitored during the Act phase.

5 Meetings and reports

The security reports and the list of meetings of the Security Office are adaptable, tailored to reflect the changing scale, activities, and requirements of the Research Infrastructure. Here are presented a non-exhaustive list of meetings and reports necessary for proper SMS management.

5.1 Meetings

Meeting Name	Periodicity	Participants	Description
Security Strategy Meeting	Quarterly	Security Office team, Members IT department heads	Strategic planning for security policies, review of security frameworks, and risk management.
Security Monitoring Meeting including Incident Response Review, DevSecOps Coordination and Security Metrics Review	Monthly	Security Office team, IT Support Staff and development and operations teams	Review of security incidents, response effectiveness, and updates to incident response plans. Coordination on DevSecOps practices, review of security in development pipelines. Analysis of security metrics, KPIs, and performance of the security measures.
Compliance and Audit Coordination	Bi-annually	Security Office team, Compliance officers, external auditors	Discussion of compliance requirements, preparation for upcoming audits, and compliance updates.
Security Awareness Training	Annually	All staff involved in the RI	Training sessions for staff on security best practices, policy updates, and threat awareness.
Third-Party Security Review	As needed	Security Office team, third-party vendors	Assessment and review of third-party vendor security practices and compliance.

Table 1: RESILIENCE Security Management Meetings

5.2 Reports

Report Name	Periodicity	Authors	Description
Security Incident Report	Monthly	Security Office team, IT Support Staff and development and operations teams	Detailed analysis of security incidents, including cause, impact, and remedial actions taken.
Security Metrics and KPIs Report	Monthly	Security Office team, IT Support Staff and development and operations teams	Analysis of security-related metrics and KPIs, performance tracking of security initiatives.

Vulnerability Assessment Report	Quarterly	Security analysts, Security Office team	Overview of vulnerabilities identified in systems and applications, with risk assessments.
Security Policy Review	Quarterly	Security Office team	Assessment of current security policies, recommendations for updates or new policies.
Risk Management Report	Bi-annually	Risk management team	Evaluation of current risk posture, effectiveness of risk mitigation strategies.
Security Training Feedback	After each session	Training coordinators	Analysis of security training sessions, participant feedback, and suggestions for improvement.
Third-Party Vendor Security Review	As needed	Security Office team	Assessment of third-party vendors' security practices and compliance with security requirements.
Data Protection Compliance Report	Bi-annually	Data protection officers	Status of data protection measures, compliance with data privacy laws, and incident reports.
Compliance Audit Report	Bi-annually	Security Office team	Summary of compliance audit findings, compliance status, and recommendations for improvement.
IT Infrastructure Security Report	Annually	IT department heads	Review of the security status of IT infrastructure, including hardware and software aspects.

Table 2: RESILIENCE Security Management Reports

6 Processes

The processes of the Security Office are similarly scalable, evolving in line with the organization's growth and varying needs.

6.1 Secure Software Development Lifecycle (SDLC)

6.1.1 DevSecOps

DevSecOps, an abbreviation of **Development, Security, and Operations**, is an evolutionary outcome of the Agile and DevOps movements. It was conceived to address the increasing need for faster development cycles without compromising on security. This methodology integrates security as a fundamental component at every step of the software development lifecycle (SDLC), rather than treating it as an afterthought or a separate process.

In the context of RESILIENCE, a Research Infrastructure geared towards fostering innovative scientific inquiries, the implementation of DevSecOps is not just beneficial, but essential. DevSecOps, which integrates security protocols directly into the development and operational phases of software and system production, is crucial for ensuring that RESILIENCE's IT resources and infrastructure remain secure, agile, and efficient.

The adoption of DevSecOps offers a proactive stance against potential security threats. By embedding security measures from the very beginning of the software development lifecycle, RESILIENCE can identify and mitigate vulnerabilities much earlier. This early detection is crucial, as it drastically reduces the potential for extensive damage that might occur if these issues are discovered later in the process. Moreover, as DevSecOps involves continuous testing and integration, it allows for ongoing security assessments, ensuring that the infrastructure can swiftly adapt to evolving cyber threats.

DevSecOps also fosters a collaborative culture of shared security responsibility, aligning seamlessly with the RI partners' ethos of collective research and innovation. This integration of security into every development phase ensures both regulatory compliance and adherence to data protection norms, crucial for the integrity of research. Moreover, DevSecOps scalable and flexible framework is instrumental in adapting the in-house IT infrastructure to evolving research demands, ensuring its resilience against the dynamic landscape of technological and research advancements. This approach not only strengthens security but also supports the continuous growth and adaptability of the partners' research capabilities.

6.1.2 The stages of DevSecOps

DevSecOps, which integrates security into the DevOps lifecycle, follows a series of stages where development, operations, and security practices are intertwined. This approach, as presented here below, ensures security is a continuous, integral part of the entire software development and deployment process. Here are the typical stages of the DevSecOps lifecycle:

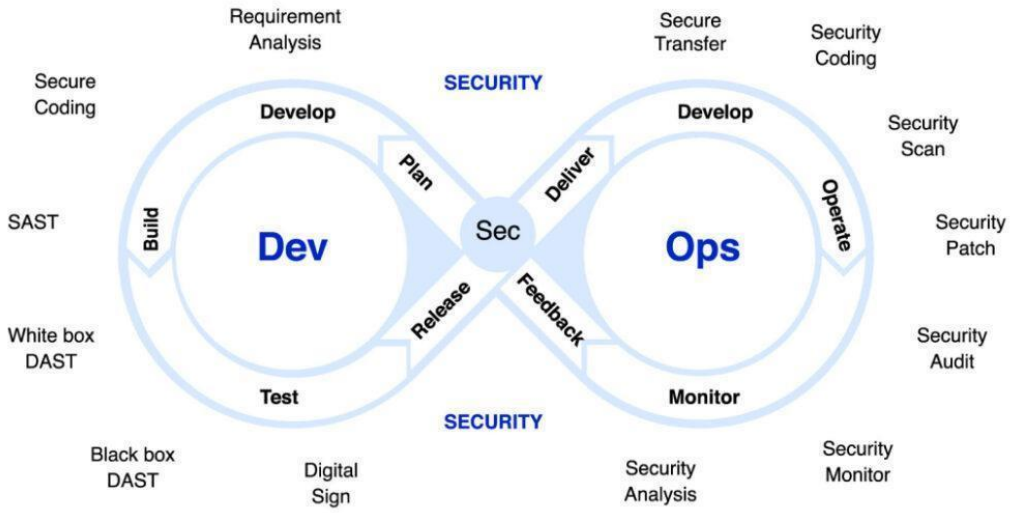

Figure 2: Representation of DevSecOps Lifecycle by Amazic

1. Planning: In this initial stage, teams identify project requirements and objectives. Security teams participate in this phase, helping to identify potential security requirements and considerations early on. This collaboration ensures that security is a foundational aspect of the project from the beginning.
2. Development
    a. Coding/Development: Developers write code, and security is integrated into this process. Secure coding practices are encouraged, and tools like static application security testing (SAST) can be used to identify potential vulnerabilities as code is written. The goal is to catch security issues early in the development cycle.
    b. Pre-Commit/Commit: Before committing code to the repository, developers perform local tests. Pre-commit hooks can be used to automate security checks. When code is committed, it should be reviewed with both functionality and security in mind.
3. Build/Continuous Integration (CI): When code is merged into a shared repository, automated builds and tests are triggered. CI servers can run additional security tools such as software composition analysis (SCA) to check dependencies for known vulnerabilities.
4. Testing: Automated tests are run to ensure the software works as expected. In DevSecOps, this includes comprehensive security testing, such as dynamic application security testing (DAST), to identify runtime vulnerabilities. Penetration testing may also be conducted during this phase.
5. Release/Deployment: When the software is ready for release, the deployment process is automated and repeatable. Infrastructure as Code (IaC) and containerization can be used to ensure consistent and secure environments. Security checks should be integrated into the deployment process.
6. Operations/Monitoring: In the operational phase, the software is monitored continuously for any performance or security issues. Tools like security information and event management (SIEM) systems can be used for real-time security monitoring.
7. Feedback and Improvement: Feedback from operations is looped back to the planning and development stages. Security incidents and operational issues are analysed, and the insights gained are used to improve both security and operational practices in future iterations.

When software or a version of it is decommissioned, it's crucial to ensure that this is done securely to prevent any lingering security risks.

6.2 Third-party Security Providers

OWASP includes guidelines and best practices for securely integrating and managing third-party components and services within an application's architecture. These considerations are part of OWASP's broader focus on web application security and include:

- Secure Integration of Third-Party Components: OWASP provides recommendations on how to securely integrate third-party libraries, APIs, and other external components. This involves practices like vetting for known vulnerabilities, ensuring secure communication channels, and maintaining updated versions of these components.
- Third-Party Vendor Risk Management: OWASP emphasizes the importance of assessing and managing the risks associated with third-party vendors. This includes due diligence during vendor selection, regular security assessments of third-party services, and contractual agreements that include security expectations and compliance requirements.

- **Security in Software Supply Chain**: OWASP stresses the need to secure the entire software supply chain, which includes third-party vendors. This involves monitoring and securing every stage of the development process, from the selection of third-party components to their deployment in the application environment.
- **Vulnerability Management for Third-Party Components**: Part of OWASP's guidelines includes monitoring and responding to vulnerabilities in third-party components, which may involve patch management, configuration changes, or replacing components that pose security risks.

6.3 Training & Collaboration

6.3.1 Trainings

Awareness forms the cornerstone of our security education strategy within RESILIENCE RI, representing the "what" in our approach to influencing security behaviours. Our methods, including various training and activities, will serve as the "how" to implement and reinforce this awareness.

For all personnel involved in RESILIENCE RI, our goals will be:

- To thoroughly understand and internalize the code of conduct, which must be agreed upon before initiating any role within the project, as well as the specific codes of conduct applicable to different roles and responsibilities.
- To have a clear understanding of information security and privacy risks pertinent to their job functions and be equipped with the necessary knowledge and tools to mitigate these risks.
- To minimize security risks through enhanced comprehension of potential threats and legal obligations.

The RESILIENCE RI approach to security and behavioural practices will be anchored in our existing compliance frameworks and corporate standards, along with tailored guidelines that align with the specific needs of the project. This approach will include:

- Security and behaviour orientations as part of staff onboarding and initial training.
- Accessible and continuously updated **Security and Behaviour Guidelines** for all staff throughout the RI lifecycle, available in our digital repository for easy reference.
- Regular induction sessions for new staff/consultants, ensuring they are familiar with the latest security protocols and conduct codes.
- Regular reviews and updates to the guidelines, ensuring alignment with evolving security policies and improvements identified through our Continuous Improvement Program.
- Mission briefings for all personnel engaged in different facets of the project, tailored to their specific roles and locations.
- Targeted awareness sessions as required, to address emerging security trends or issues.
- Delegation of responsibility to Infrastructure and Security Managers to ensure comprehensive support for consultants and effective implementation of security practices across the project.
- Evaluation of awareness initiatives through post-training feedback, periodic assessments by key project contacts, and analysis of security incidents, to gauge the effectiveness of the training and awareness efforts.

- An ongoing commitment to enhancing the RESILIENCE security and behaviour awareness initiatives as part of our Continuous Improvement Program.

RESILIENCE staff will utilize a blend of formal and informal methods to foster a culture of security awareness, ensuring that all team members are equipped to handle the evolving landscape of security challenges in our field.

6.3.2 Collaboration

When defining the RI Security Policy and Procedures, the Security Office will also foster an environment where researchers, developers, and other stakeholders actively collaborate on security matters, sharing insights and feedback for continuous improvement. To successfully put in place such rich collaboration, the Security Office will consider the following aspects in its procedures:

- **Interdisciplinary Teams**: Encourage the formation of teams that bring together experts from different disciplines. This diversity of perspectives is essential in identifying and addressing the multifaceted security challenges we face.
- **Regular Collaboration Meetings**: Schedule frequent meetings where team members can discuss ongoing security issues, brainstorm solutions, and share updates on recent developments in the field.
- **Feedback Mechanisms**: Implement structured feedback processes allowing team members to provide input on security protocols, practices, and incidents. This feedback is invaluable for continuous improvement.
- **Shared Learning Initiatives**: Organize workshops, seminars, and training sessions where team members can learn about the latest trends in cybersecurity, privacy laws, and best practices. Encourage team members to share their expertise and experiences from their respective fields.
- **Cross-Project Collaboration**: Facilitate interactions between different projects within RESILIENCE RI, allowing for a cross-pollination of ideas and strategies. This helps in developing a more robust and comprehensive security framework.
- **External Partnerships**: Establish partnerships with external entities such as academic institutions, industry experts, and other research initiatives. These collaborations can provide fresh insights and innovative approaches to security.
- **Collaborative Tools and Platforms**: Utilize digital collaboration tools and platforms to ensure seamless communication and information sharing among team members, irrespective of their physical location.
- **Transparent Communication**: Maintain transparency in all security-related matters. Regular updates about security challenges, successes, and changes in protocol help in building a culture of trust and collective responsibility.

6.4 Access Control & Authentication Policy

RESILIENCE will be committed to establishing a secure and efficient access control and authentication framework. The objective of the RI in this respect will be to enable researchers to access only the data and tools that are relevant to their projects, while simultaneously safeguarding the infrastructure from unauthorized access and potential security threats.

6.4.1 RESILIENCE Stakeholders, Roles and Responsibilities

The section 8.4 from the ITSERR Stakeholders Analysis document, proposed as an input for defining RESILIENCE AAI roles and users, provides a comprehensive framework for understanding the various entities involved in a research infrastructure. It breaks down into detailed descriptions of archetypes, stakeholders, and users, each serving a distinct purpose.

Additionally, as the document outlines generic roles like Administrators, Owners, Contributors, Viewers, Collaborators, and Reviewers, each with specific access and control levels within a system. This classification that could be a basis for RESILIENCE, will be crucial for managing user access and ensuring data and resource security. Understanding these roles will be essential for effective user management in the context of a Data Management Plan (DMP), as it helps in structuring access to data and resources, ensuring security, and maintaining the integrity of the research data and infrastructure.

RESILIENCE will need to define a framework to structure user access, ensuring data security, and maintaining the integrity of its research infrastructure. Additionally, section 8.4 provides a guide to adapting the infrastructure to meet the specific needs of various environments, including development, test, and production, ensuring secure and efficient delivery of services to end-users.

6.4.2 Auditing & Logging

RESILIENCE will implement a robust logging system to meticulously record all user activities and system events. This system will capture detailed logs, including access records, system changes, and transaction histories. These logs will be systematically audited at regular intervals to identify any anomalies or potential breaches. The auditing process will be thorough, ensuring continuous vigilance. In the event of a security incident, these logs will serve as a critical resource for tracing the sequence of events, assessing the impact, and formulating an appropriate response.

6.4.3 Security Assessments

RESILIENCE will conduct periodic vulnerability scans to identify weaknesses in its systems, essential for staying ahead of potential security threats. Alongside these scans, RESILIENCE will perform comprehensive threat assessments to understand and prepare for potential security challenges. Following each assessment, RESILIENCE will update its security measures promptly to guard against the identified risks.

6.4.4 Continuous Monitoring & Response

RESILIENCE approach will also include implementing continuous, real-time monitoring of the infrastructure to promptly detect and respond to threats, ensuring minimal downtime. In case of security incidents, RESILIENCE will have protocols in place for swift and effective responses, thereby ensuring maximum resilience against attacks. The monitoring systems will be regularly updated to stay current with the latest security trends and threat intelligence, helping us maintain a robust defence posture.

6.5 Incident Management

Incident Management at RESILIENCE is a vital aspect of the security strategy, meticulously crafted to address security incidents both within the RESILIENCE infrastructure and those involving federated entities.

The chosen methodology ensures swift and effective handling of these issues, tailored to the specifics of each scenario.

For incidents involving federated entities, the process begins with immediate identification and reporting, acknowledging the critical role these entities play in our extended infrastructure. In such cases, our Security Office team engages in close communication and collaboration with the affected entity's security team. This collaborative approach guarantees a coordinated response, utilizing shared resources and expertise. The response encompasses joint efforts in containment, eradication, and recovery, aligning with both RESILIENCE's protocols and those of the federated entity. Following the resolution, a thorough post-incident analysis is conducted. Insights from these incidents are shared across all federated entities, fostering collective improvement in security measures.

In contrast, **incidents internal to RESILIENCE** are exclusively managed by the RESILIENCE Security Office team. This process involves an immediate response to contain and mitigate the incident, followed by comprehensive efforts to address the root cause, and restore affected systems. Communication during these incidents is confined to internal teams and stakeholders, maintaining confidentiality and focus. A detailed analysis follows each incident, providing critical insights that are used to refine the security strategies and prevent future breaches.

Across both scenarios, RESILIENCE maintains a **consistent approach in terms of preparation and tools**. The RI will be equipped with state-of-the-art tools for incident detection, analysis, and response. Regular training and simulations are integral to our strategy, ensuring that the team is well-prepared for various incident types. Continuous improvement is a cornerstone of the RESILIENCE approach; each incident, whether involving federated entities or internal, is viewed as an opportunity for learning and enhancing our security posture. This dynamic approach to incident management underscores our commitment to maintaining robust security and resilience in the face of evolving cybersecurity challenges.

6.6 Data Backups & Disaster Recovery

RESILIENCE will implement regular data backup processes and establish a robust disaster recovery plan, crucial for ensuring the continuity of research in the event of data loss or catastrophic failures. This approach will distinctively address the different scenarios involving data, software, and services hosted on infrastructures managed both internally by RESILIENCE and externally by third-party providers.

For data, software, and services hosted on an **infrastructure directly managed by RESILIENCE staff**, rigorous backup procedures will be instituted. These will involve systematic, regular backing up of all essential research data to secure redundant storage solutions. An internal disaster recovery plan will be tailored to quickly restore operations from these backups, minimizing downtime and data loss in case of system failures or other disruptions.

Conversely, for elements hosted on **infrastructures managed by third-party providers**, the chosen approach will involve closely collaborating with these providers to ensure they have effective backup and disaster recovery plans in place. RESILIENCE will verify that their procedures align with its security and continuity standards, ensuring a seamless integration of their backup systems with our overall disaster recovery strategy. Regular audits and reviews will be conducted to confirm their adherence to agreed-upon protocols and to update these plans as necessary to adapt to evolving research and technology landscapes.

In both cases, our focus will be on maintaining the integrity and availability of research data, ensuring that both internally and externally managed systems contribute effectively to the resilience of the research operations. This dual approach will provide a comprehensive safety net, safeguarding research against a wide range of risks and ensuring the ongoing progress of research.

6.7 Regulatory Compliance

RESILIENCE places a high priority on staying updated with regional and international regulations concerning data protection and privacy. This commitment is essential to ensure that the infrastructure always remains compliant. Recognizing the complexity and ever-evolving nature of these regulations and considering the current absence of a dedicated entity within RESILIENCE with the expertise to define and understand these regulatory requirements, this aspect will need to be addressed by the RESILIENCE Board of Directors.

RESILIENCE needs to gather some expertise in regional and international data protection and privacy laws. This team or advisor will be responsible for continuously monitoring legal developments, interpreting how they impact the RI's operations, and implementing necessary changes to maintain compliance. They will also advise the Security Office team on the implications of these regulations for the research activities, data handling practices, and collaborations with international partners.

Furthermore, this focus on regulatory compliance will involve regular training and awareness programs for all RESILIENCE staff to ensure that they understand the importance of compliance and how it affects their respective roles.

7 Annexes

7.1 Annex 1 - Security Policy and Procedures Document

This section briefly describes the scope and the content of the SPP document to be produced by the RI-SO.

7.1.1 Objectives of the Security Policy and Procedures

- **Establish Security Standards:** Define clear and concise security standards and practices that align with the unique needs of RESILIENCE and its focus on religious studies research.
- **Risk Management:** Provide a framework for identifying, assessing, and managing security risks that could impact the RI's operations, data, and stakeholders.
- **Data Protection:** Outline procedures and guidelines to protect sensitive and personal data, emphasizing RESILIENCE's commitment to not hosting sensitive data, while ensuring compliance with legal and ethical standards, including GDPR and FAIR data principles.
- **Compliance Assurance:** Ensure that all activities, projects, and collaborations within RESILIENCE comply with the defined security policies and external regulatory requirements.
- **Incident Response:** Develop a structured approach for responding to and managing security incidents, minimizing potential damage, and preventing future occurrences.
- **Training and Awareness:** Promote security awareness among staff, researchers, and partners. Provide necessary training to ensure everyone understands their role in maintaining security.
- **Continual Improvement:** Establish mechanisms for regularly reviewing and updating the security policies and procedures to adapt to new threats, technological advancements, and changes in the research landscape.

7.1.2 Scope of the Security Policy and Procedures

- **Coverage of Activities:** Applies to all research, operational, and administrative activities conducted under the auspices of RESILIENCE.
- **Applicability to Stakeholders:** Encompasses all individuals and entities involved with RESILIENCE, including staff, researchers, partners, and third-party service providers.
- **Physical and Digital Security:** Addresses both physical security measures (like secure access to facilities) and cybersecurity aspects (such as data encryption, access controls, and network security).
- **Project Lifecycle:** Covers the entire lifecycle of projects and initiatives within RESILIENCE, from initiation and planning to execution, monitoring, and closure.
- **Compliance and Legal Requirements:** Includes guidelines and procedures for adhering to legal, regulatory, and ethical standards relevant to research in religious studies.
- **Data Management:** Details policies related to data acquisition, storage, processing, sharing, and disposal, with specific emphasis on handling non-sensitive data in line with FAIR principles.
- **Emergency Preparedness:** Outlines procedures for emergency response and business continuity to ensure resilience in the face of unforeseen events or crises.

7.2 Annex 2 – 4T, a Trusted Security Model for a decentralized federated security organization

To ensure a decentralized federated security organization, the RI will adopt his standard "**4T Security Model**", based on the following "T's":

- **Trusted Organization,**
- **Trusted People,**
- **Trusted Workplaces,**
- **Trusted Zone.**

Implementing the 4T model in the RESILIENCE RI project will ensure that each layer of interaction—from organizational governance to the individual researcher—upholds the security necessary to protect information and maintain the integrity of the research activities.

7.2.1 Trusted Organizations

This could represent the overarching governance structure of RESILIENCE, which includes all the partner entities and the central coordinating body. Each Trusted Organization ensures that the entire RI network, platform, and services are secured by adhering and respecting to the RI security standards.

Example: The central body of RESILIENCE acts as the RI Security Office (RI-SO), responsible for overarching policies and the enforcement of security measures across the infrastructure. The RI-SO would oversee the coordination of security protocols, training, and incident response within the network of participating universities, libraries, and research centres.

7.2.2 Trusted People

Refers to individuals within the RESILIENCE network who are given access to data and resources. This includes researchers, IT staff, and administrative personnel who have been vetted and trained in handling information and using the RI services.

Example: Scholars and researchers working on topics related to religious studies, who have undergone background checks (i.e., identifying themselves using their ORCID). These individuals would be listed in a Security Checked Member List (SCM List) and would be the only ones with access to certain levels of data and services within the RI platform.

7.2.3 Trusted Workplaces

Within the RESILIENCE Research Infrastructure, Trusted Workplaces are integral components of the RI's Authentication and Authorization Infrastructure (AAI). These secure physical locations are where research is conducted and are fully integrated into the RI AAI system, ensuring that access to research data and resources from these workplaces is systematically controlled and aligned with RESILIENCE's security standards.

Example: An academic department within a participating university that specializes in religious studies might feature advanced access digital copies of reserved digital manuscripts. The integration with the RI

AAI means that all physical access to these rooms is logged and monitored, consistent with the digital security protocols of RESILIENCE, providing a seamless and secure research environment.

7.2.4 Trusted Zone

This represents the secure digital environment where sensitive activities and data storage take place. It includes the IT infrastructure servers, networks, and applications that are configured to meet strict security standards.

Example: A secure cloud-based platform where researchers upload, store, and analyse data related to religious studies. Access to this platform would be strictly controlled, with advanced encryption and multi-factor authentication in place.

7.3 Annex 3 – Proposal of a RESILIENCE RI Disclaimer for our platform(s)

The RESILIENCE Research Infrastructure (RI) services are provided to facilitate the sharing and preservation of research outcomes in the field of religious studies.

By using the RESILIENCE RI services for uploading or accessing data, the researcher agrees to the following:

- RESILIENCE RI is a platform for the open dissemination of research content, accessible to all for non-military purposes.
- Uploaders bear sole responsibility for the content they share on RESILIENCE RI and must ensure compliance with legal standards, including data protection and intellectual property rights. Sensitive personal data must be anonymized or have explicit consent for sharing.
- RESILIENCE RI content is offered "as-is." Users must adhere to any associated license conditions and do not acquire any intellectual property rights by downloading content.
- Users are responsible for their use of the content and agree to indemnify RESILIENCE RI against any related claims. Content hosting is not an endorsement by RESILIENCE RI.
- RESILIENCE RI may modify or remove content or user access at its discretion to ensure compliance with these terms or applicable laws.
- Metadata on RESILIENCE RI is available under the CC0 waiver unless stated otherwise.
- These terms may be updated at any time without notice.

7.4 Annex 4 – RESILIENCE AAI – Stakeholders, users, and roles

This is an extract from the ITSERR Stakeholders Analysis document [R2] that could be considered as an input to the definition of RESILIENCE AAI roles and users.

7.4.1 Concepts: archetypes, stakeholders, and users

Archetypes, stakeholders, and users are different concepts in the context of a research infrastructure.

- **Archetypes** refer to typical patterns or models of entities, processes, or systems that are used to inform the design and implementation of research infrastructures. Archetypes can be used to capture the requirements and needs of various stakeholders, as well as to define the functionalities and services that the infrastructure should provide.

- **Stakeholders** are individuals or groups who have an interest or a stake in the research infrastructure, and who can influence or be affected by its development and operation. Examples of stakeholders in a research infrastructure might include researchers, funding agencies, IT staff, data providers, and regulators.
- **Users** are individuals or groups who use the research infrastructure to access data, tools, and services that support their research activities. Users may be researchers, students, policymakers, or members of the general public, depending on the nature and scope of the infrastructure.

In summary, archetypes are models used in the design of research infrastructures, stakeholders are groups who have an interest in the infrastructure, and users are individuals who use the infrastructure to support their research activities.

7.4.2 Generic roles

In any research project, it is important to have a clear and well-defined system for managing user access and permissions to data and resources.

Different users may have different levels of access and control depending on their role and responsibilities within the system/project. In this context, the following roles are commonly used to manage user access and permissions: Administrator, Owner, Contributor, Viewer, Collaborator, and Reviewer. Each role has specific rights and permissions that allow users to access, create, modify, or delete data and resources within the system. Understanding these roles is essential for effective user management and ensuring the security and integrity of the research data and infrastructure.

- **Administrator**: An administrator is a user who has full access to all the data, services, and features in the system. They have the ability to create, modify, and delete user accounts, set permissions and roles, and manage the system configuration.
- **Owner**: An owner is a user who has ownership rights to specific data or resources. They have the ability to control access to their data or resources, set permissions, and modify or delete the data or resources as needed.
- **Contributor**: A contributor is a user who has the ability to create, modify, and delete data or resources within a specific project or group. They may have limited access to other projects or groups within the system.
- **Viewer**: A viewer is a user who has read-only access to data or resources within a specific project or group. They are not able to modify or delete the data or resources.
- **Collaborator**: A collaborator is a user who has the ability to work on specific data or resources within a project or group. They may have limited access to other projects or groups within the system.
- **Reviewer**: A reviewer is a user who has the ability to review and provide feedback on specific data or resources within a project or group. They may not have the ability to modify or delete the data or resources.

7.4.3 ITSERR Stakeholders

As seen during the Design Phase of RESILIENCE RI, the ITSERR project also has multiple stakeholders including religious studies researchers, project partners, IT staff, end-users, data providers, and regulators. The AAI infrastructure will allow researchers to authenticate and authorize access to research tools and

resources, collaborate, and share research data. Project partners and regulators will provide support for the development and maintenance of the infrastructure. IT staff will manage the infrastructure, and end-users will access research data and resources. Data providers will provide data access and ensure data management, and regulation compliance will be managed by regulators.

By adequately and sufficiently understanding stakeholder needs, ITSERR's objective to create an effective AAI infrastructure can be satisfied.

- **Researchers**: Religious studies researchers are the primary stakeholders who will be affected by the AAI infrastructure. They will use the AAI to access and share research data, collaborate with other researchers, and authenticate and authorize access to research tools and resources.
- **Project partners**: Project partners, such as research institutions and funding agencies, may also be stakeholders who are affected by the research infrastructure (RI). They may be involved in setting the requirements and standards for the infrastructure and providing support for its development and maintenance.
- **IT staff**: IT staff who are responsible for managing and maintaining the software, the IT services as well as the RI are also stakeholders who will be affected by the RI. They may need to provide technical support, perform upgrades and maintenance, and troubleshoot any issues that arise.
- **End-users**: End-users, such as students, policymakers, and members of the public, may also be stakeholders who are affected by the research infrastructure. They may use the research data and resources that are made available through ITSERR, and they may need to authenticate and authorize their access to these resources.
- **Data providers**: Data providers, such as archives and libraries, may also be stakeholders who are affected by the RI. They may need to provide access to their data through the infrastructure and ensure that the data is properly managed and curated.
- **Regulators**: Regulators, such as government agencies and ethical review boards, may also be stakeholders who are affected by the RI. They may need to ensure that the infrastructure complies with relevant regulations and standards, such as data protection laws and ethical guidelines.

7.4.4 Project roles Versus Groups roles

Roles in the ITSERR project are defined as specific responsibilities that individuals have within the project. These roles are determined by the project requirements, goals, and the expertise of the team members. In contrast, **user group roles** refer to the specific functions or activities that individuals are expected to perform within a particular user group.

For example, the ITSERR project has several roles such as researchers, project partners, IT staff, end-users, data providers, and regulators. Each of these roles has a specific set of responsibilities within the project, such as managing data, overseeing infrastructure development, providing technical support, and ensuring regulatory compliance.

In contrast, user group roles may refer to the specific functions that users of the AAI infrastructure will perform, such as accessing research tools, collaborating with other researchers, and sharing research data. These roles may be more broadly defined than the roles in the ITSERR project, as they are intended to encompass a wider range of individuals who will interact with the AAI infrastructure.

Overall, the roles in the ITSERR project provide a framework for managing the project team, while user group roles provide a framework for managing the users of the AAI infrastructure. Both are important in ensuring the success of the project and the effective use of the AAI infrastructure.

7.4.5 Mapping between Generic roles and potential stakeholders

Mapping generic roles to potential stakeholders is an essential step in the development of a research infrastructure. By identifying the roles that different stakeholders can take on, it becomes possible to establish clear guidelines for how the infrastructure should be used, who has access to specific features or resources, and how data should be shared or managed. Understanding the various stakeholders and their roles can help ensure that the infrastructure is tailored to meet the specific needs of the research community, while still being secure and efficient. By mapping generic roles to potential stakeholders, it becomes possible to develop a framework that allows for effective collaboration and information sharing, and that ensures that all users are aware of their responsibilities and the limits of their access.

Stakeholder / Roles	Administrator	Owner	Contributor	Viewer	Collaborator	Reviewer
Researchers		Can control access to their own data or resources, modify or delete their own data or resources, and manage permissions for specific data or resources.	Can create, modify, and delete data or resources within a specific project or group.	Can view specific data or resources within a specific project or group.	Can work on specific data or resources within a project or group.	Can review and provide feedback on specific data or resources within a project or group.
Project partners	Can create, modify, and delete user accounts, set permissions and roles, and manage the system configuration.					
IT staff	Can create, modify, and delete user accounts, set permissions and roles, and manage the system configuration.					
End-users				Can view specific data or resources within a specific project or group.		

Data providers		Can control access to their own data or resources, modify or delete their own data or resources, and manage permissions for specific data or resources.		Can view specific data or resources within a specific project or group.		Can review and provide feedback on specific data or resources within a project or group.
Regulators	Can create, modify, and delete user accounts, set permissions and roles, and manage the system configuration.					Can review and provide feedback on specific data or resources within a project or group.

Table 3: Potential generic roles endorsement by stakeholders

7.4.6 DEVEL, TEST and PROD environments and their impact on the AAI

The **development, test, and production environments** are a critical aspect of the software development process, and they have a significant impact on the implementation of an AAI infrastructure in the context of the ITSERR project. Each environment has its own unique role, and the way in which the AAI infrastructure is implemented and configured can vary depending on the specific needs and requirements of each environment.

- **The development environment** is where the software and services that are part of the ITSERR project are created, tested, and refined. This environment is typically used by the IT staff and developers who are responsible for the creation and maintenance of the software and services. In this environment, the AAI infrastructure will be configured to allow for maximum flexibility and customization, to ensure that developers can easily test and refine their work. The IT staff may have administrative privileges in this environment to allow for easy maintenance and troubleshooting.
- **The test environment** is where the software and services are tested to ensure that they are functioning correctly and meeting the requirements of the project. This environment is typically used by the IT staff, developers, and other stakeholders who are involved in the testing and validation process. In this environment, the AAI infrastructure will be configured to be as close as possible to the production environment, to ensure that the software and services are tested under realistic conditions. The IT staff and researchers may have the role of a reviewer or collaborator in this environment to ensure that the testing process is running smoothly.
- **The production environment** is where the software and services are deployed and made available to end-users. This environment is used by the end-users, who are typically researchers in religious studies, and other stakeholders who need to access and use the software and services. In this environment, the AAI infrastructure will be configured to be as secure and stable as possible, to ensure that the research data is protected and that the software and services are functioning correctly. The IT staff may have the role of an administrator or owner in this environment to ensure that the infrastructure is maintained and that access to data and resources is properly managed.

It might be possible, based on what ICT services are contracted to company, that DEV and TEST environment will be under infrastructure of a software house company, owned and managed by its staff. The PROD environments however will remain under the responsibility of the ITSERR Infrastructure team.

In summary, the development, test, and production environments play a crucial role in the implementation of the AAI infrastructure in the context of the ITSERR project. The specific roles and privileges of stakeholders may vary depending on the environment, and the AAI infrastructure will need to be configured accordingly to ensure that it meets the needs and requirements of each environment. By carefully managing the configuration of the AAI infrastructure in each environment, the ITSERR project can ensure that the software and services are delivered to end-users in a secure, stable, and efficient manner.

8 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	22/02/2023	ITSERR – Stakeholders Analysis

Funded by the European Union