GÉANT Security Baseline

A Security Maturity Model for NRENs and R&E Federations

Authors: Nicole Harris, Ivar Janmaat, Vlado Pribolsan, Michael Schmidt, Jule Ziegler

Table of Contents

Introduction

Information systems are an essential part of all today's organisations that enable the execution of processes and the provision of services. However, more and more risks are emerging that threaten the security of information or systems and thus the entire organisation. This concerns Research & Education (R&E) organisations, i.e. universities and research institutions, as well as those in the private sector. National Research and Education Networks (NRENs) enable national and international networks in this context and provide services to users, some of which can be used worldwide. Thus, they are a potential target for attackers but also vulnerable to threats not only within their own organisation, but throughout the entire NREN community. The highly collaborative nature of NRENs results in a high degree of interdependence, which justifies a special need for protection. This framework is intended to support NRENs and affiliated organisations in establishing appropriate security measures necessary for a coordinated security program that takes into account the specific framework conditions in R&E federations.

Purpose

GÉANT Member NRENs vary in size, type, user base, offered services, level of cooperation with academic, scientific and educational communities and many other aspects, but for all NRENs security of services, users and operations is crucial. In order to harmonise the security level of NRENs, the Security Baseline as a common framework has been created. This security baseline can be used in various ways and these are some of them:

- A starting point for NRENs looking to develop or enhance current security practice.
- A tool for benchmarking the current status of NREN development in security.
- A guide for NRENs to reach a minimal level of security offer.
- An opportunity to make NREN security programs comparable.

This framework assists organisations in understanding key aspects of security practices that are part of a security program. It defines requirements to cover R&E specific challenges in a modular way, whereby each module covers an organisational topic, such as risk or supplier management. In this way, NRENs can set up a security programme that is as flexible as possible but whose aspects and level are comparable to those of other NRENs.

Scope

This document applies to NRENs and related sub-contractors. It defines a minimum set of security controls necessary to secure not only an NREN as an organisation itself, but organisations of national representatives interconnected with a large, global research and education community

There are many different ways of assessing security readiness that can be examined from an operational, organisational, technical or legal standpoint. This baseline focuses on the **organisational** requirements for NRENs and core requirements for NREN services. It highlights the most common security areas while focusing on aspects that are **unique to the NREN offer.** The security modules defined provide a high-level starting point for

implementing a security program. In each area, we point to other tools and approaches tailored to the specific needs of NRENs that might help you gain a deeper dive in order to assess aspects of the requirements further.

Security Maturity Levels

This document defines three different levels of maturity which can be used to describe the status of each module. It is not necessary to achieve the highest maturity level for each module, this should be seen as a long-term goal and should be adapted to the criticality of the services offered by the organisation. It is possible that some modules define few or no requirements for a level. This is especially the case with sophisticated processes that do not need to be implemented as a standard.

1 - Baseline

Maturity level 1 matches the title of this framework and defines the so-called "GÉANT Security Baseline". This level defines a GÉANT wide minimum of security and is expected to be met by most NRENs by default and implemented by all NRENs in the short term. This level mainly contains basic requirements that form the basis for an effective security program in an organisation. NRENs should ensure compliance with this level and implement missing requirements as quickly as possible.

Scope: minimum requirements for each organisation

2 - Advanced

Maturity level 2 builds directly on the baseline requirements and extends the modules mainly with organisation-specific adaptations. This level defines modules of a mature security program and provides a good foundation for security management. It represents the medium to long-term goal for NRENs to achieve in order to solidly establish and improve security management. It is expected that most NRENs are partly compliant by implementing just individual requirements and the percentage of fully compliant organisations will grow steady.

Scope: medium to large organisations or such that offer important services or providing access to research collaborations.

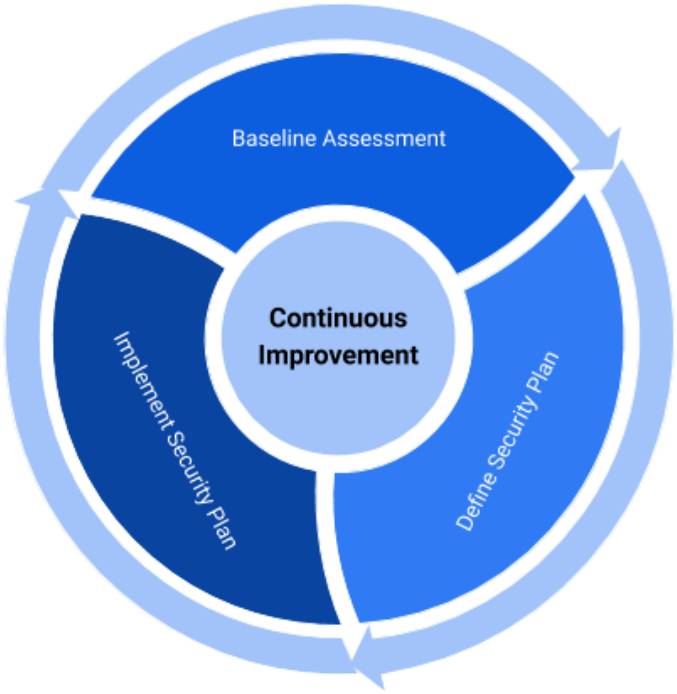
3 - Expert

Maturity level 3 is the highest level and requires a deep understanding of security management and security program. It is expected that only a small part of NRENs will reach this level in the near future. Depending on the services offered, the business cases supported and the risk assessment of your own organisation, some or all of the criteria from this level may be relevant. It is designed as a long term strategic goal for NRENs.

Scope: organisations processing sensitive and critical information or providing critical services and infrastructure

How to Use the Baseline

This framework supports security managers in establishing and improving a security program by describing important security aspects while listing essential requirements for them. In addition, by using maturity levels, it offers the possibility to continuously improve the organisations security level through the targeted implementation of individual measures.
At the beginning, a review of the requirements against the existing security measures should take place to determine the current status of the organisation. Subsequently, missing requirements should be assessed and appropriate measures planned to increase the maturity level of the organisation. This cyclical process of continuous improvement should be aligned with the organisation's strategic goals and plans to ensure long-term success.



1. Baseline Assessment
The first step is a complete security review. The aim is to check whether the existing security program has already reached a given level of maturity and which requirements for the next level of maturity are still missing.

2. Define Security Plan
Review your risk appetite against the baseline report. Have a clear understanding of budget / resource you have to develop security practices in given areas. Develop a plan to establish security measures to meet missing requirements based on available resources and business objectives.

3. Implement Security Plan
Implement the plan to support the development of new security goals on an annual basis. It is not required to improve the maturity level every year, but at least fulfil individual requirements.
The cycle then begins again with the review.

NREN Organisation Baseline (NO)

This section describes the different security areas and their requirements. This Baseline covers the areas Policy, People, Threats and Operations. Each theme defines a number of modules, each of which describes a specific management aspect. The focus is clearly on the organisational security aspects and not on the technical ones. Each module consists of a general description, requirements grouped by maturity level and supporting references. These refer to other resources relevant to the topic in question. The baseline attempts, whenever possible, to refer to existing documents from other EU projects such as AARC, REFEDS, ENISA or national organisations instead of reinventing the wheel. For each section, the baseline focuses only on the organisational capability of the NREN for its own operation; **services provided to customers to meet their security requirements are out of scope for this document**.

The requirements are arranged according to the maturity model described above. Since the different levels depend on each other and higher levels often only intensify requirements, it is recommended to implement missing requirements according to this order. It is possible that the requirements that are defined at a lower level are not required at a higher level anymore. In this case, they are replaced at the higher level by other, more restrictive ones that address the same security problem.

It is usually not necessary to use the linked resources to meet the requirements. These are only intended to help establish a process or measure. Only in a few places linked resources are integrated directly into the requirements. Mostly these are specific GÉANT or resources explicitly created for the baseline.

For each module a reference to the Information Security Management System standard ISO/IEC 27001 is provided. This makes it easier for NRENs with an existing management system to integrate the modules accordingly or to assist in setting up such a system.

NO1: Policy and Leadership

Policy and Leadership are essential building blocks for security within any organisation. It is important that leadership and commitment is shown not just in putting in place the right processes, policies and people, but that these efforts are continuously supported in implementation through appropriate resourcing and demonstrable commitment from leadership teams.

<table>
<tr><td>NO1.1</td><td>Management Commitment and Mandate</td></tr>
<tr><td>Description</td><td>Good security planning begins with a firm commitment at an executive level within an organisation. This baseline is built around achieving executive level sign-off for all elements of planning, but management buy-in should be planned from the start. Without this commitment, the teams responsible for executing the plans will experience challenges in terms of understanding the budget available, understanding their scope and parameters in relation to other parts of the organisation, and in getting commitment and cooperation from other departments and organisational staff.</td></tr>
<tr><td>Requirements</td><td>
<table>
<tr><th>NO1.1</th><th>Requirements / Level</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>NO1.1.1</td><td>Member of organisational leadership team is given a direct mandate for security.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO1.1.2</td><td>Security policy and objectives are established and clearly linked to organisational strategy.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO1.1.3</td><td>Budget and resources for security are clearly defined and set annually.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO1.1.4</td><td>Support is provided for the creation and approval of controls to meet GÉANT Security Baseline.</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>NO1.1.5</td><td>The goals for information security and data protection are communicated annually by the top management.</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>NO1.1.6</td><td>Regular reporting of security controls to top management is in place.</td><td></td><td></td><td>✓</td></tr>
<tr><td>NO1.1.7</td><td>The security program is compliant to a national or international standard.</td><td></td><td></td><td>✓</td></tr>
</table>
</td></tr>
<tr><td>Further Support</td><td>Cyber security culture in organisations
Chapter 9.3.1 emphasises role of senior management, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Commitment to information security</td></tr>
</table>

	This paper analysing how to involve senior management to support information security in organisations https://www.researchgate.net/publication/221175434_Senior_Executives_Commitment_to_Information_Security_-_from_Motivation_to_Responsibility Further resources (will be published in later releases of this framework)
ISO/IEC 27001	A5: Information Security Policies, A6: Internal organisation

NO1.2	**Internal Security Policy**
Description	Information security policy is a set of documents which defines organisational and technical measures and rules for designing, implementing and using information systems in order to ensure confidentiality, integrity and availability of NRENs data. Different and wide areas can influence security so just selected topics are given in this document.
Requirements	

NO1.2	**Requirements**	**1**	**2**	**3**
NO1.2.1	Information security policy has been approved by management and it is implemented in the NREN.	✓	✓	✓
NO1.2.2	The information security policy is implemented for new and legacy services and systems.	✓	✓	✓
NO1.2.3	Physical security and using of mobile and personal devices are addressed in the information security policy.	✓	✓	✓
NO1.2.4	Violations of the Internal Security Policy are investigated and dealt with by the security officer.		✓	✓
NO1.2.5	Information security policy is continuously updated, edit least once per year.		✓	✓
NO1.2.6	Reliable mechanisms for monitoring information security policy implementation are in place and results are regularly presented to the top management.			✓
NO1.2.7	Internal security policies are accessible by other NRENs.			✓

Further Support	**Common Sense Security Framework** This is a very simple and easy to follow set of criteria for what you might want to secure as an organisation. https://commonsenseframework.org/

	Master Information Security Policy & Procedures A template master security policy is provided by TrustedCI, the NSF CyberSecurity Center of Excellence. https://trustedci.org/guide/docs/MISPP Further resources (will be published in later releases of this framework)
ISO/IEC 27001	A5: Information Security Policies and A6: Organisation of Information Security

NO1.3	**Acceptable Use Policy**
Description	Acceptable Use Policy (AUP) is a short and easy to understand document, based on information security policy, which defines basic rules of using information systems. All employees, old and new one, permanent and temporary, should be familiar with the content of this document. This AUP covers the core organisational AUP; an NREN may have multiple AUPs for other purposes (e.g. Network).
Requirements	

NO1.3	**Requirements**	**1**	**2**	**3**
NO1.3.1	NREN have AUP based on security policy.	✓	✓	✓
NO1.3.2	The AUP has been signed or accepted by all users of information system including new one.	✓	✓	✓
NO1.3.3	Users are regularly reminded and educated about AUP.	✓	✓	✓
NO1.3.4	Sanctions has been defined and applied to users not complying to AUP.		✓	✓
NO1.3.5	The AUP covers at least the internal and external use of networks, hardware, e-mails and information.		✓	✓
NO1.3.6	Terms and Conditions of Employment cover the AUP.			✓
NO1.3.7	Compliance of users with AUP is subject of regular audits.			✓

Further Support	**Template AUP documents** **NSF AUP Template** Template created by TrustedCI. https://trustedci.org/guide/docs/AUP

	WISE / AARC AUP Template Template created by WISE and the AARC Project. https://docs.google.com/document/d/1FMhvqSwpTm26jBCCg8ZHUrmugNe5r8Rszy-SbqtzSKs/edit?usp=sharing **FIRST AUP Template** Template created by FIRST. https://www.first.org/resources/guides/aup_generic.doc Further resources (will be published in later releases of this framework)
ISO/IEC 27001	A8: Asset Management

NO1.4	**Regulatory and Privacy**
Description	Protection of users' personal data should be NRENs priority. General Data Protection Regulation (GDPR) regulates the processing of personal data related to EEA Member States. NREN should harmonise processing of personal data of its users and employees with GDPR. Wide range of tasks and measures are defined in GDPR so they should be prioritized and applied to data processing in order to maximise protection of personal data and data subjects rights, taking into account the available resources and related risks.
Requirements	

NO1.4	**Requirements**	**1**	**2**	**3**
NO1.4.1	Role of NREN (controller or processor) and legal base for processing of personal data is defined along with a processing policy.	✓	✓	✓
NO1.4.2	A data protection officer (DPO) or equivalent role is appointed by top management.	✓	✓	✓
NO1.4.3	Appropriate privacy notice is available to data subjects.	✓	✓	✓
NO1.4.4	Principles of data protection by design and by default are used when personal data are processed.		✓	✓
NO1.4.5	The response to personal data breaches are part of the security incident management process (NO3.2).		✓	✓
NO1.4.6	Data protection impact assessment (DPIA) should be conducted, where necessary.			✓
NO1.4.7	The NREN is capable of reporting a personal			✓

	<table><tr><td></td><td>data breach to the supervisory authority and data subjects in less than 72 hours.</td><td></td><td></td><td></td></tr></table>
Further Support	**Official GDPR** Text of GDPR is available in official languages of the EU. European Data Protection Board (EDPB) publish Guidelines, Recommendations, Best Practices including GDPR related WP29 Guidelines. **NIST Special Publication 800-53r5-draft** NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.12 focuses on privacy authorization. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf **Policy on the Processing of Personal Data** Policy provided by the AARC Project https://docs.google.com/document/d/1QseGQVzUQqvosqhjkF2qlHUI4Swlhgb8oDe8N6NWcqE/edit?usp=sharing **Privacy Policy** Policy provided by the AARC Project https://docs.google.com/document/d/1QseGQVzUQqvosqhjkF2qlHUI4Swlhgb8oDe8N6NWcqE/edit?usp=sharing Further resources (will be published in later releases of this framework): ● Legal and Regulatory Register for NRENs
ISO/IEC 27001	A18: Compliance with Legal and Contractual Requirements

NO2: People

Besides technology, people themselves pose the highest risk to the security of the organisation. Incidents are often not due to technical weaknesses, but to a lack of understanding of workflows, information and processes. Not only in-house staff are a potential danger, but also employees of service providers and customers. A holistic management of the personal risks includes awareness measures for all persons in the organisation and equally considers risks emanating from suppliers and their employees.

NO2.1	**Training and Awareness**
Description	A Security Awareness Programme trains internal and external staff as well as other individuals with access to the organisation's information. The focus is on the secure handling of IT systems and information in general. The training can take various forms such as classroom training or online training, depending on the topics and culture of the organisation. The aim is to raise participants' awareness of information security issues and provide them with the necessary knowledge to deal with the various threats in their daily work.

	Awareness training should inform employees about relevant policies and processes and ensure that they are applied. When processes and policies are not followed, it is often unclear to employees why they exist and what threats they are protecting against. A good awareness programme relies on a variety of measures and channels to increase general awareness within the organisation.
Requirements	

NO2.1	Requirements	1	2	3
NO2.1.1	All employees, (sub) contractors, temporaries etc. must perform an information security awareness training regularly.	✓	✓	✓
NO2.1.2	Training records are maintained.	✓	✓	✓
NO2.1.3	A security communication plan including internal and external communication is in place.	✓	✓	✓
NO2.1.4	A plan for role based training is created once a year.		✓	✓
NO2.1.5	All staff are aware of their responsibilities regarding information security and motivated to achieve high standards for security.		✓	✓
NO2.1.6	Regular audits verify the security awareness of employees.			✓
NO2.1.7	Top management is highly aware of security aspects and sets an example to its employees.			✓

Further Support	**NSF Training and Awareness Policy template** TrustedCI provides a very simple template for a basic awareness policy. https://trustedci.org/guide/docs/TAP **NIST Special Publication 800-53r5-draft** NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.2 focuses on awareness and training. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf **CLAW Crisis Management Resources** Materials from the annual GÉANT Crisis Management Exercise can be found at: https://wiki.geant.org/display/gn43wp8/Crisis+management+information+sharing#CrisismanagementillnformationsharingMaterialCLAW2019

	Further resources (will be published in later releases of this framework):
ISO/IEC 27001	A7.2.2: Information security awareness, education and training

NO2.2	**Personnel Management**
Description	People are at the heart of every organisation and are both key to successful security management and one of the most likely points of failure. It's really important to have appropriate policies and processes in place to ensure that staff play a strong role in security management, but it is even more important to ensure that such policies are not just pieces of paper or tick box activities, but become standard behaviour. Staff should be motivated to support security requirements internally rather than seeing processes as a burden or a judgement on them. The processes described here can be supported by good implementation of training and awareness described in NO2.1.
Requirements	

NO2.2	**Requirements**	**1**	**2**	**3**
NO2.2.1	Appropriate screening of applicant's identity, qualifications and competencies is carried out prior to hiring.	✓	✓	✓
NO2.2.2	Appropriate screening in place for contractors to the same standard as staff.	✓	✓	✓
NO2.2.3	Rights and responsibilities of staff effectively, managed, changed or removed when leaving or changing job roles.	✓	✓	✓
NO2.2.4	Employee handbook or contract clearly sets out the responsibilities of staff regarding information security.		✓	✓
NO2.2.5	Where appropriate, staff handling sensitive data have signed NDA.		✓	✓
NO2.2.6	It is ensured that key roles responsible for critical services or processes are redundant.			✓
NO2.2.7	There are appropriate interfaces to all departments in order to carry out necessary actions within 48 hours upon termination or change of a contract.			✓

Further Support	**NIST Special Publication 800-53r5-draft** NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.16 focuses on personnel security. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-

	5/draft/documents/sp800-53r5-draft.pdf If you have access to the ISO27001 and ISO27002 documentation, processes for managing personal are well described. TrustedCI has created a very useful checklist for managing personnel exit that is available at: https://trustedci.org/guide/docs/exitlist. Further resources (will be published in later releases of this framework):
ISO/IEC 27001	A7: Human Resource Security

NO2.3	**Supplier Management**
Description	Services or products used daily by NRENs can be provided by external suppliers. This means that information security measures will need to be extended to suppliers in order to provide an overall security level. Appropriate policies and processes should be in place for contracting suppliers and staff should be informed about these policies and processes when they are involved in the contracting process. The required security levels can be described in a supplier security policy. Staff can then check contracts against this policy. Checking requirements when the contract is signed is important but it is also important to see that contract terms are met and changes to contracts are assessed. This is all part of good supplier management.

Requirements

NO2.3	Requirements	1	2	3
NO2.3.1	A supplier security policy is in place and accessible for staff involved in contracting suppliers.	✓	✓	✓
NO2.3.2	All suppliers have contracts stating relevant security aspects.	✓	✓	✓
NO2.3.3	All suppliers are assessed according to their criticality and business impact and listed at a central location.	✓	✓	✓
NO2.3.4	SLA, SLA reporting, meeting notes and other documents to assess the suppliers performance on a regular basis are available.		✓	✓
NO2.3.5	Changes in the suppliers services are monitored on a regular basis		✓	✓
NO2.3.6	Where appropriate, suppliers services and products are audited or penetration tested.			✓

	NO2.3.7	Where appropriate, suppliers handling sensitive data have signed a NDA.			✓
Further Support	GÉANT Cloud Services: https://clouds.geant.org/resources/cloud-security/fundamental-cloud-security-part-12-supply-chain-in-the-cloud/ Further resources (will be published in later releases of this framework):				
ISO/IEC 27001	A15: Supplier Relationships				

NO3: Threats

A risk is the "effect of uncertainty on objectives" (ISO 31000), where the effect may have negative or positive deviation from expected behavior. However, in security we mostly cover these negative effects represented as threats to information, processes and services. Identifying these threats to an organisation and prioritizing them according to their importance impact within the business area, like research and education is called Threat Modelling. Based on this, the Risk Management uses identified threats and matches them to vulnerable assets of the organisation in order to mitigate the negative effects. While the goal is to mitigate risks as far as possible, it is never possible to eliminate all of them completely. So, Continuity Management considers risks that have a catastrophic impact and defines a strategy to handle them if they happen against all odds. In addition to risk and continuity management, there is also so-called security incident management that defines methods for reacting appropriately to security incidents, regardless of how critical they are. The establishment of an appropriate process and Security Incident Response Team (CSIRT) is one of the first measures an organisation should implement in the area of threat protection.

NO3.1	**Risk Management**
Description	Risk management is a key aspect in every organisation these days. Although it is common to implement a set of standard security measures suggested by guidelines and other security frameworks, each organisation or type of organisation has to adjust security controls to their specific needs at some point in time. This adjustment is especially crucial since resources available to implement security measures are limited; it is necessary to identify the most important risks to mitigate to maximize the effect of the resources invested. NRENs are no exception here. However, when managing risks in NRENs there are some special aspects that are not covered in security standards applying to other organisations. Just the fact that each NREN is an infrastructure provider and manages a federation where each organisation involved could potentially influence the security of each other organisation therein is very unique. Furthermore, by being involved in GÉANT and thus deeply connected to other NRENs, their infrastructure, services, employees and users, organisational risks affect similar and same assets of other NRENs. As a result, managing risks in NRENs is not an individual, but a federated activity that relies on risks being shared and maybe mitigated together in the community. This module provides requirements and guidelines compatible to standard risk management frameworks, but covers the aspects specific to NRENS and a federated environment.
Requirements	

NO3.1	Requirements	1	2	3
NO3.1.1	A risk management process is defined, documented and implemented	✓	✓	✓
NO3.1.2	A risk manager responsible for the risk management process is assigned	✓	✓	✓
NO3.1.3	Security measures are approved and implemented based on risk assessment	✓	✓	✓
NO3.1.4	A yearly risk assessment is performed for at least all GÉANT Top 10 Threats, including a review of existing risks and assets.		✓	✓
NO3.1.5	Risks that might affect other NRENs or federated services are reported regularly		✓	✓
NO3.1.6	The asset inventory includes organisation specific and federated (information) assets			✓
NO3.1.7	Organisation specific threat modelling is performed			✓

Further Support

Risk Assessment Templates

AARC project template:
https://docs.google.com/document/d/13eRJuI78ULXA87UucclavygAuhk41ck8ukgJdZ25uiA/edit?usp=sharing
WISE template:
https://wiki.geant.org/download/attachments/53773456/WISE_Risk_Management_Template_v1.1.xlsx

Risk Management Frameworks

Risk Management Overview
ENISA provides a lightweight overview of risk management. This includes a sample process and lots of supporting materials. It is a good starting point to get familiar with the topic.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/introduction

NIST Special Publication 800-53r5-draft
NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.17 focuses on risk assessment.
https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Risk Management Framework for Information Systems and organisations
NIST provides in SP 800-37r2 a comprehensive risk management

framework.
https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

CIS RAM (Risk Assessment Method)
CIS RAM (Center for Internet Security® Risk Assessment Method) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls cybersecurity best practices.
https://www.cisecurity.org/white-papers/cis-ram-risk-assessment-method/

The Risk IT Framework
ISACA provides with Risk IT another extensive framework to manage and govern risk. It is superseded by Cobit 5 for risk, which is part of the commercial COBIT5 framework. However, the older but free Risk IT framework is still very useful.
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

SIG-ISM White Paper: Risk Management
This whitepaper is about how to manage information security risk by performing risk assessments in a National Research and Education Network (NREN) organisation or not-for-profit organisations such as universities. The scope of this white paper is only information security: discussions around disaster recovery and continuity planning are considered out of scope.
https://wiki.geant.org/display/SIGISM/SIG+ISM+white+paper+risk+management

---

Threats

Threats Catalogue – Elementary Threats
A catalogue of elementary threats including a description provided by the German Federal Office for Information Security
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=2

Threat Taxonomy
ENISA provides a structured list of threats. It is a good overview and better structured than the BSI threat catalogue, but lacks the detailed descriptions.
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

---

Further resources (will be published in later releases of this framework):

- R&E specific threat catalogue

	• List of standard NREN asset • Role description Risk Manager
ISO/IEC 27001	A8 (Asset Management), Section 6 (Risk Management)

NO3.2	**Incident Management**
Description	Computer security incidents require fast and effective responses from the organisations concerned. Computer Security Incident Response Teams (CSIRTs) are responsible for receiving and reviewing incident reports, and responding to them as appropriate. As such, a CSIRT team is a fundamental element of security planning. Organisations should establish solutions to detect, monitor and respond to their own internal security incidents, including appropriate reporting requirements to management and other stakeholders. At the very least, organisations should know who responds to an incident, what they are responsible for during the incident and how to report the incident effectively. It is useful to identify interested parties which might be affected by or interested in incidents. A communication plan that lists stakeholders, how and when to contact them does greatly increase the efficiency of incident response. Critical internal stakeholders are typically IT and security management or departments like legal, HR and public relations. In the federated context, federation members or other NRENS might be important stakeholders as well. CSIRTs help deliver the organisation's incident response plan. This plan should cover information dealing with protection of assets and services and incident detection, response and prevention but should also consider broader issues such as disaster recovery and business continuity.
Requirements	

NO3.2	**Requirements**	**1**	**2**	**3**
NO3.2.1	An Incident Management process including reporting and escalation approaches is defined, documented and implemented with identified responsibilities.	✓	✓	✓
NO3.2.2	A CSIRT of at least 3 people exists.	✓	✓	✓
NO3.2.3	The CSIRT should be listed in the Trusted Introducer service.	✓	✓	✓
NO3.2.4	The CSIRT have reached accreditation status with Trusted Introducer service and asserts support for the Traffic Light Protocol (TLP) and RFC2350.		✓	✓
NO3.2.5	Critical incidents are responded to within 24		✓	✓

		hours.			
	NO3.2.6	Interested parties of incidents are identified and a communication plan exists to collaborate with relevant stakeholders.			✓
	NO3.2.7	The CSIRT ensures 24/7/365 support.			✓

Further Support

Incidence Management Process

Security Incident Response Procedure
The AARC project has published a security incident response procedure for federated environments.
https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf

Guide to Federated Security Incident
The AARC project has created a guide for federated incident management with a focus on research collaborations.
https://aarc-project.eu/wp-content/uploads/2019/03/AARC-I051-Guide-to-Federated-Security-Incident-Response-for-Research-Collaboration.pdf

Computer Security Incident Handling Guide
NIST provides with SP 800-61 a guide to implement an incident management process, with detailed explanations on how to handle an incident.
https://doi.org/10.6028/NIST.SP.800-61r2

Training and Awareness

CSIRT Maturity - Self-assessment Tool
ENISA provides a self assessment tool for CSIRTs to assess the maturity of your CSIRT team and team approaches
https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey/

TRANSITS CSIRT training
The GÉANT Task Force CSIRT (TF-CSIRT) perform trainings for (potential) CSIRT members.
https://tf-csirt.org/transits

Other

REFEDS SIRTFI
REFEDS has created the Security Incident Response Trust Framework for Federated Identity (Sirtfi) to improve the coordination of incidents across federated organisations.
https://refeds.org/sirtfi

NIST Special Publication 800-53r5-draft
NIST SP 800-53 contains a set of security controls to protect the security

	and privacy of an organisation. Section 3.9 focuses on incident response. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
ISO/IEC 27001	A16: Information Security Incident Management

NO3.3	**Business Continuity Management**
Description	Business Continuity Management (BCM) takes into account risks with catastrophic effects and defines a strategy for dealing with them if they occur against all odds. These disasters can be identified and reduced as risks, but sometimes residual risks still remain with extreme impact. These residual risks must be examined as part of continuity management and appropriate plans drawn up to deal with the consequences. Thus, continuity management is fundamentally based on risk management, however risks are managed with an attempt to reduce the likelihood and impact, while disasters are managed with a Business Continuity Plan (BCM) to deal with the potential consequences. In early stages of maturity, however, the processes are implemented independently. A number of standard disasters from the literature are often used, for example in relation to fire, water, supply networks or pandemics. If continuity management develops further, risks with a particularly high impact from risk management can be considered. The BCM is particularly important for NRENs as they are responsible for many essential services. Such disasters could lead to a breakdown of the national research network or critical services such as the national identity federation. Unlike other organisations where disasters usually have a local impact on the company's customers, NREN disasters have the potential to influence researchers, teachers and students across Europe through the high level of connectivity. While associated risks should be addressed in risk management, it must be ensured that in the event of a disaster all critical services can continue or be quickly restored. The close cooperation in GÉANT and the link between NRENs may require collaboration to resolve the disaster recovery at pan-European level.
Requirements	

NO3.3	**Requirements**	**1**	**2**	**3**
NO3.3.1	A BCM process is defined, documented and implemented.	✓	✓	✓
NO3.3.2	A Business Continuity Manager responsible for the BCM process is assigned.	✓	✓	✓
NO3.3.3	A BCP exists, which covers at least disasters produced by power failure, fire and water.	✓	✓	✓

	NO3.3.4	A list of managers responsible to handle disasters at any point in time is defined.		✓✓	✓✓
	NO3.3.5	The BCP covers all NREN specific disasters from the GÉANT Disaster List.		✓✓	✓✓
	NO3.3.6	The organisation participates yearly in a crisis simulation, such as the GÉANT CLAW workshops.			✓✓
	NO3.3.7	A manager on duty is assigned to be available on call 24/7/365.			✓✓

Further Support

Business Continuity Process

Business and IT Continuity
ENISA provides a good overview of the entire topic continuity management at its website, which is a good start to begin. Additionally, an in-depth guide called Overview and Implementation Principles ready to download.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience
https://www.enisa.europa.eu/publications/business-and-it-continuity-overview-and-implementation-principles

Business Continuity for SMEs
ENISA provides a guide for Business Continuity Management which is tailored to small and medium sized enterprises, which is expected to be particularly useful for NRENs.
https://www.enisa.europa.eu/publications/business-continuity-for-smes

BSI-Standard 100-4 BCM
The German Federal Office for Information Security provides an extensive guide to establish a BCM process
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

Contingency Planning Guide for Federal Information Systems
NIST provides with SP 800-34 a guide to implement a BCM process with an organisation. It has a technical focus and can be used to deepen one's understanding of the topic.
https://doi.org/10.6028/NIST.SP.800-34r1

Example BCP Template
ENISA template of a Business Continuity Plan
https://www.enisa.europa.eu/publications/example-bcp-template

---

Other

NIST Special Publication 800-53r5-draft
NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.6 focuses on contingency

	planning. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf **NIST Special Publication 800-160 Vol. 2** Developing Cyber Resilient Systems: A Systems Security Engineering Approach. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final Further resources (will be published in later releases of this framework): ● Template Business Continuity Plan ● BCM Process Sample ● List of disasters specific to NRENs
ISO/IEC 27001	A17: Information Security Aspects of Business Continuity Management

NO4: Operations

In addition to the organisational security aspects, processes and tools for the protection of the organisation's information systems must be established. It is important to define clear guidelines on how information can be protected against unauthorized access (access management) or disclosure (cryptography). Where possible, organisational policies should be backed up by technical measures that support availability and integrity.

In order to prevent security mechanisms from being circumvented by vulnerabilities in software, procedures for dealing with security bugs are necessary. Vulnerabilities must be identified and evaluated as rapidly (vulnerability management) in order to eliminate them as quickly as possible (patch management).

NO4.1	**Tools**
Description	This section describes the use of special security tools that should be available in every organisation. It should be ensured that all systems in the organisation are at least protected by up-to-date antivirus software and secure firewall settings. The division of the internal network into different segments, which represent different security areas, allows the restriction of access and particular protection of critical areas. Access to systems from outside should only be possible through a virtual private network (VPN) client and using multi-factor authentication. In addition, the entire network and the systems within it should be constantly monitored. Various software solutions are available to monitor network traffic and actions on systems.
Requirements	

NO4.1	**Requirements**	**1**	**2**	**3**
NO4.1.1	All software used in the organisation is documented and approved.	✓	✓	✓
NO4.1.2	An antivirus software is deployed on every server or workstation.	✓	✓	✓
NO4.1.3	Every server is protected by a firewall.	✓	✓	✓
NO4.1.4	Access to internal systems from outside the organisation is restricted to the use via VPN.		✓	✓
NO4.1.5	Networks and systems are monitored by an intrusion detection system.		✓	✓
NO4.1.6	Systems are segregated by different networks based on their criticality and function.			✓
NO4.1.7	There are measures in place to mitigate DDoS attacks against federated services.			✓

Further Support	https://www.cyberessentials.ncsc.gov.uk GÉANT provides a range of tools to help and support these requirements. These include: DDoS Cleansing and Alerting: https://www.geant.org/Services/Trust_identity_and_security/Pages/DDoS.aspx Firewall on Demand: https://www.geant.org/Networks/Network_Operations/Pages/Firewall-on-Demand.aspx eduVPN: https://www.geant.org/Innovation/Research_programmes/Pages/eduvpn.aspx Further resources (will be published in later releases of this framework): ● DDoS Mitigation ● Vulnerability Assessment as a Service
ISO/IEC 27001	A.14 System acquisition, development and maintenance

NO4.2	**Cryptography**
Description	The use of cryptography is a way to protect the confidentiality, authenticity and integrity of information. It covers controls like the encryption of data at rest and in transit, the signing of information and the management of cryptographic keys used for the aforementioned actions. Data can be lost in various ways and thus become accessible to unauthorized third parties. Stored data can be disclosed from the outside by breaking into systems as well as from the inside by (unintentional) access by employees. If sensitive information is transmitted, for example by email or on the web, there is always the danger that it will be intercepted and read or even modified. Against all these dangers the use of current cryptographic methods protects the access to the data. But even if state-of-the-art encryption algorithms are used, they are only as secure as the key used. Effective key management poses organisational challenges for SMEs in particular. These can only be mastered by establishing and maintaining processes and procedures for key management. The correct and secure use of cryptography is particularly important for NRENs, as a large amount of personal data of employees, students and researchers is usually affected. However, existing infrastructures or standard software often do not offer the possibility of using secure methods, which is why insecure algorithms or implementations are often used. As with other security controls, a risk assessment should be carried out in this case in order to weigh up the risks and benefits.
Requirements	

NO4.2	Requirements	1	2	3
NO4.2.1	A policy on the use of cryptographic controls and key management is in place, taking into account information that is critical / less critical to the NREN	✓	✓	✓
NO4.2.2	The policy defines rules for data at rest and in transit for each type of critical information.	✓	✓	✓
NO4.2.3	The policy covers at least services/server, e-mails, backups and mobile/portable devices.	✓	✓	✓
NO4.2.4	The use of cryptographic functions or key lengths which are known as insecure is forbidden.		✓	✓
NO4.2.5	A yearly review of the cryptographic policy is conducted.		✓	✓
NO4.2.6	The cryptographic functions and key lengths are based on common (inter)national security standards			✓
NO4.2.7	Federation metadata are signed using a hardware security module (HSM).			✓

Further Support

Cryptographic functions and key management

Guideline for Using Cryptographic Standards
NIST provides in his SP 800-175B a useful overview of cryptographic functions, when to use them and how to manage cryptographic keys.
http://dx.doi.org/10.6028/NIST.SP.800-175B

Cryptographic Mechanisms
Similar to NIST, the BSI provides technical guidelines with recommended algorithms, crypto suites and key lengths to use within the next couple of years.
https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/index_htm.html

Cryptographic Policy Sample
The ISACA cryptographic policy is a simple example how such a document may look like.
https://www.isaca.org/Knowledge-Center/Research/Documents/Cryptographic-Policy_res_eng_0817.PDF

Further resources (will be published in later releases of this framework):

- GÉANT recommendations for cryptographic controls

ISO/IEC 27001

A10: Cryptography

<table>
<tr><td>NO4.3</td><td>Access Management</td></tr>
<tr><td>Description</td><td>The capability to regulate the access of authenticated users and associated permissions, including emergency suspension during the handling of security incidents. The capability to identify and contact authorised users and service providers.</td></tr>
<tr><td>Requirements</td><td>
<table>
<tr><th>NO4.3</th><th>Requirements</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>NO4.3.1</td><td>An access management policy and procedure is documented and mandatory for all organisational units. As a minimum, this should cover how access is granted and revoked within the organisation.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO4.3.2</td><td>User accounts which are not functional accounts are compliant to REFEDS RAF Cappuccino.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO4.3.3</td><td>User authentications/services are compliant to/require REFEDS SFA.</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>NO4.3.4</td><td>Users are granted only the rights and permissions they need to perform their job (least privilege) and privileged accounts where given are well documented.</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>NO4.3.5</td><td>Organisation supports the use of Sirtfi.</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>NO4.3.6</td><td>Privileged user accounts are compliant to REFEDS RAF Espresso.</td><td></td><td></td><td>✓</td></tr>
<tr><td>NO4.3.7</td><td>Privileged user authentications/critical services are compliant to/require REFEDS MFA.</td><td></td><td></td><td>✓</td></tr>
</table>
</td></tr>
<tr><td>Further Support</td><td><u>Access Management Policy</u>

NIST Special Publication 800-53r5-draft
NIST SP 800-53 contains a set of security controls to protect the security and privacy of an organisation. Section 3.1 focuses on access control, 3.7 on identification and authentication.
https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

REFEDS Recommendations

REFEDS Assurance Framework (RAF)
REFEDS has published an Identity Assurance Framework including the RAF Cappuccino and Espresso Profile.
https://refeds.org/assurance</td></tr>
</table>

	REFEDS Authentication Profiles REFEDS has published two authentication profiles for SAML/OIDC IdPs and SPs. https://refeds.org/profile/sfa https://refeds.org/profile/mfa **Sirtfi - Security Incident Response Trust Framework for Federated Identity** This framework allows entities participating in federations to signal their incident response capabilities. https://refeds.org/sirtfi. Further resources (will be published in later releases of this framework): •
ISO/IEC 27001	A9: Access Control

NO4.4	**Patch Management**
Description	IT vendors regularly publish software and firmware updates (patches) to fix bugs and security vulnerabilities. Manually tracking vulnerabilities for different products on a network is time consuming and expensive. At the large corporate level, costly but effective vulnerability and patch management practices reduce cyber security risks. For small and medium sized organisations, it is recommended to enable automatic updates for software. This will keep standalone devices, operating systems, applications, and security software up-to-date and free of known vulnerabilities. Larger organisations with more resources might improve this by manually applying patches. The benefit is that patches and their influence on software, services and processes can be reviewed and assessed prior to installation. This process is meant to ensure that **security patches** are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts. The patch management process must be applied to the entire organisation, including IT services as well as internal IT systems such as workstations. A process manager is responsible for planning and implementing the process, as well as defining policies on how to deal with software in the organisation. Software used by service providers and customers should also be considered as well.
Requirements	

NO4.4	**Requirements**	**1**	**2**	**3**

	NO4.4.1	A Patch Management process is defined, documented and implemented	✓	✓	✓
	NO4.4.2	A Patch Manager responsible for the process is assigned	✓	✓	✓
	NO4.4.3	All software in the organisation is regularly updated	✓	✓	✓
	NO4.4.4	Security patches are deployed within 2 weeks after release		✓	✓
	NO4.4.5	Patches that treat critical vulnerabilities are deployed within 2 days after release.		✓	✓
	NO4.4.6	A patch management system is used to centrally control software updates for the entire organisation.			✓
	NO4.4.7	Patches and their business impact are reviewed before deployed in production.			✓
Further Support	Further resources (will be published in later releases of this framework): •				
ISO/IEC 27001	A12.6: Operations Security/Technical Vulnerability Management				

NO4.5	**Vulnerability Management**			
Description	A process to **manage vulnerabilities** (including reporting and disclosure) in any software recommended for use within the infrastructure. There should be a process in place to be able to identify, classify, prioritise and mitigate any potential software vulnerabilities. This can be challenging in organisations such as NRENs which can be distributed and have complex software ownership patterns due to service type and collaborative working patterns. Any process defined must be sufficiently dynamic to respond to changing threat environments. Vulnerability Management is closely related to patch management and Incident Management Processes			
Requirements				

NO4.5	**Requirements**	**1**	**2**	**3**
NO4.5.1	A vulnerability management process is defined, documented and implemented	✓	✓	✓
NO4.5.2	A person responsible for the vulnerability	✓	✓	✓

		management process is assigned			
	NO4.5.3	Vulnerability assessment is carried out on a regular basis	✓	✓	✓
	NO4.5.4	Establish a vulnerability triage group		✓	✓
	NO4.5.5	Vulnerabilities are reported to service owners and administrators on a monthly basis		✓	✓
	NO4.5.6	Solutions to handle critical vulnerabilities are introduced within two weeks after reporting.			✓
	NO4.5.7	Invest in vulnerability scanning tools			✓
Further Support	**Vulnerability Management Guidelines** The UK National Cyber Security Center provides useful guidelines to establish a vulnerability management process. https://www.ncsc.gov.uk/guidance/vulnerability-management Further resources (will be published in later releases of this framework): •				
ISO/IEC 27001	A12.6: Operations Security/Technical Vulnerability Management				