07-05-2021

Deliverable D8.12

GÉANT Community Requirements for Business Continuity Planning

Deliverable D8.12

Contractual Date:	30-04-2021
Actual Date:	07-05-2021
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 1
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	MARnet/UKIM
Document ID:	GN4-3-21-43C319
Authors:	Anastas Mishev (MARnet), Vladislav Bidikov (MARnet), Michel Gerdes (DFN-CERT), Dankmar Lauter (DFN-CERT), Christine Kahl (DFN-CERT), Sarunas Grigaliunas (LITNET)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract
This document gives an overview of Business Continuity Management (BCM) and provides guidelines for NRENs on implementation. It shows relations with and dependency on other processes and gives guidance on how to make optimal use of combining security and continuity improvements from different angles.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The increased importance of the National Research and Education Networks (NRENs) as service providers in the pan-European research, education and innovation environment requires that they should give increased focus to their resilience and robustness. To that end, adopting appropriate Business Continuity measures, plans and frameworks becomes crucial.

Based on the positive experience of some of the NRENs, surveys and analysis of the current situation, this deliverable is intended to help NRENs identify their requirements regarding Business Continuity Management (BCM). It gives an overview of BCM, describes the current status of NRENs' business continuity preparations and provides guidelines on implementation. It shows relations with and dependency on other processes and gives guidance on how to make optimal use of combining security and continuity improvements from different angles. While focusing on NRENs, the information and guidelines are equally relevant to the other organisations that make up the GÉANT community (universities, research institutions, etc.), notwithstanding the differences in business and BCM priorities.

Business Continuity Management comprises all the controls, actions and processes that prepare an organisation to handle serious disruptions of its business activities. However, limited resources, human, technical or financial, can limit the feasibility of preparing for every possible disruptive situation that can occur. That is why each organisation, and especially NRENs, should define its own approach based on identifying the core business processes that need to be addressed in the BCM, enabling it to react to disruptions in an ordered and professional manner and minimising their impact.

The BCM lifecycle includes five phases: operational planning and control, business impact analysis and risk assessment, business continuity strategy, establish and implement business continuity procedures, and exercising and testing.

Other business processes that are relevant in the context of BCM are:

- Risk Management (RM) – the identification and assessment of potential risks that could disturb the business, as well as the treatment of those risks in a feasible way to minimise the probability of their occurrence.

  Recommendations for NRENs regarding RM in the context of BCM include ensuring management support, and supporting a risk-based approach towards information security.

- Incident Response Management (IRM) – the main objectives of which are to react to and stop incident-causing events and to restore acceptable levels of service quality and availability as quickly as possible.

Recommendations for NRENs regarding IRM in the context of BCM include closely aligning the two sets of processes and procedures, though keeping the respective teams separate where feasible, and ensuring a defined communication protocol between them.

- Data Protection Management and, in particular, Personal Data Breach Management – the activities conducted by an organisation (controller) that focus on compliance for its processing of personal data, including accountability guaranteeing the security of the processing. These are important since violations of the security of personal data can have a highly negative and potentially disruptive impact on an organisation.

  Recommendations for NRENs include placing an emphasis on the first stage of detection and analysis of an incident; documenting the approach; and conducting internal checks and external audits.

Implementing full-scale Business Continuity Management (BCM) covering the entire organisation can be a complex endeavour. The S7 Business Continuity Framework introduced in Section 5.2 is based on the Lean BCM approach and was developed by GN4-3 WP8 T1 building on the work carried out for the Dutch NREN SURF in 2017, as described in [FBC]. The framework's light-touch requirements and iterative approach are especially advantageous for NRENs introducing BCM or conducting a Business Impact Analysis (BIA) for the first time. It enables NRENs to get a head start in conducting and implementing BCM by prioritising their most important processes based on the decisions of their senior management, while continuing to work on the remaining processes in due course. In addition, it introduces the concept of maturity levels, to help NRENs select an appropriate set of controls for their current implementation cycle. The S7 BCM Framework measures are grouped by seven subject areas: Governance, Strategy and Policy; Crisis Management and Communication; Emergency Continuity; Restore and Recovery; Exercising and Testing; Awareness and Training; and Foundation.

To increase resilience, the S7 BCM Framework should be implemented alongside two other frameworks: the Security Baseline for NRENs and the Trusted Introducer (TI) services. Parts of these frameworks may overlap and therefore NRENs may not need to apply them all in all areas; a mapping of recommended controls is therefore provided.

WP8 asked several NRENs to review the proposed framework and identify which processes they considered most important. One key finding that emerged from their responses was that most NRENs have not made any special efforts to address BCM, due to a lack of resources or awareness. NRENs that have performed the GÉANT Security Baseline self-assessment were found to be more aware of the need for BCM.

The S7 Framework is a starting point for future development and improvement which will help the community, and especially NRENs, to address BCM through an approach that is tailored to their needs. Meanwhile WP8 will continue to work to better understand NRENs' needs and priorities, and help address them, by providing practical tools and guides, for example, in order to establish BCM in a structured and affordable manner.

1 Introduction

This document gives an overview of Business Continuity Management (BCM) and provides guidelines on implementation. It shows relations with and dependency on other processes and gives guidance on how to make optimal use of combining security and continuity improvements from different angles.

The Research and Education (R&E) community faces considerable challenges as all R&E activities become increasingly dependent on network connectivity and distributed services as well as on accessing facilities remotely. The indispensable growth of remote learning and working resulting from the COVID-19 pandemic emphasises this even further. National Research and Education Networks (NRENs) play a significant role in this as their constituents are increasingly dependent on continuous service delivery and ubiquitous access.

This means NRENs are responsible for delivering services that are are robust, resilient to smaller disturbances and able to quickly recover from disruptions to ensure Business Continuity (BC), defined in [ISO 22301, p. 2] as the *capability of an organisation to continue delivery of products or services at predefined acceptable levels following a disruptive incident*.

At the basis of resilience and recovery are preparation and prevention. By putting in place a number of preventive measures an NREN can assure there will be fewer disturbances, as the whole infrastructure will be less vulnerable. As achieving perfect security is unfeasible, incident response processes and business continuity measures are required for sound corporate governance.

This report describes NRENs' requirements for business continuity. It provides background information and describes the current status of business continuity preparations at NRENs, based on the results from several surveys. The report describes and compares a number of standards and frameworks to provide recommendations for NRENs, and the wider GÉANT community, on implementing business continuity. These recommendations will assist NRENs and the GÉANT community in developing a Business Continuity Plan (BCP) that enables them to react to disruptions in a coordinated manner by responding appropriately and bringing services and processes back to normal as soon as possible, using a structured and well-thought-through approach.

2 What is Business Continuity Management?

Business Continuity Management (BCM) comprises all the controls, actions and processes that prepare an organisation to handle serious disruptions of its business activities. Although most of these are activated during or in the aftermath of disruptions of business processes, BCM also focuses on preventive measures. The most important aspect of business continuity is to identify threats to the organisation and then implement technical (or organisational) controls,[1] thus reducing the risks of disruptions or mitigating their impact on an organisation's business processes. As it is neither feasible nor indeed possible to eliminate all risks completely [NIST-SP800-30, p. 40], preparations in terms of technical or organisational measures to be activated to handle disruptions when these occur are also necessary.

However, limited resources often mean it is also not feasible to prepare for all possible disruptive situations that may arise. Depending on the nature of an organisation and the context within which it operates, its business continuity approach may therefore require focusing on a few core business processes or general plans that enable it to react to disruptions in an ordered and professional manner and minimise their impact. The number of selected core business processes will depend on available resources and the specific context.[2]

Table 2.1 below lists some key business continuity terms and their definitions.

Business Continuity (BC)	All measures enabling an organisation to handle disruptions of its business processes.
Business Continuity Management (BCM)	The management discipline of managing business continuity measures. This includes identification of threats as well as assigning, creating, testing and maintaining response plans including responsibilities.
Business Continuity Programme	The ongoing management and governance process to steer and maintain the BCM. Usually conducted by top management (Steering Committee). Finally approves the BCP.
Business Continuity Strategy	Describes the overall BC approach of the organisation. This includes analysing the results of the Business Impact Analysis (BIA) and its risk assessment and addressing them in the BCP to meet the overall BC approach of the organisation
Business Continuity Plan (BCP)	A plan or set of plans that prepare an organisation to handle disruptions of its business processes. This includes at least assigning responsibilities, defining

[1] Examples: enhancing robustness of processes by redundancy of technical solution, or a two-man rule.

[2] A network provider for critical infrastructure may implement more thorough Business Continuity Management compared to a service provider that provides only a limited number of services, none of which may be categorised as critical.

	acceptable data loss and disruption criteria, preparing spare remote capacities as well as incident handling action lists and checklists. Units may have dedicated BCPs that integrate into the organisation-wide BCP. Updated BCPs must be stored in a location accessible during every disruption.
Business Continuity Manager	The person responsible for delivering and maintaining the BCP. They report directly to the BC Steering committee. While the Business Continuity Manager does not execute the organisation's incident response, they should be consulted in view of their extensive knowledge of the organisation. Where feasible (e.g. in larger organisations), certain business-critical departments may require and employ a dedicated Business Continuity Manager, reporting to the overall Business Continuity Manager.
Business Continuity Framework	A Business Continuity Framework defines the structure of the BCP, especially how it is divided into sub plans.
Business Continuity Team	The group of people creating and maintaining the BCP, led by the BC Manager.
Incident Response Team	The team that should first react to an incident. It receives reports and is tasked with the first response to get an incident under control to enable it to be managed afterwards. After the Incident Response Team has managed an incident, Business Restoration and finally Business Resumption Teams can take over.

Table 2.1: Definitions

Even though an increased awareness of BCM has been noted, a 2020 study found that organisations still have many open questions, especially on planning BCM activities with respect to their organisation's specific features. Yet implementing BCM is a necessity for businesses nowadays [Sawalha]. The concept of BCM is based on assigning responsibilities for specific situations and preparing and enforcing action plans for disruptions before they arise, rather than under pressure at the time when they do occur. As in most situations, decisions made are usually more effective when prepared for and discussed with plenty of time for investigation and reflection compared to those made under stress and tough time constraints [Mather] [Bergland].

The remainder of this section describes the most important elements of BCM, based on both accepted standards and best practices.

2.1 Business Continuity Management Lifecycle

Organisations should follow the standardised BCM lifecycle so that they can continue to deliver their key products and services in the case of a disaster, and thus survive a crisis [ISO 22313:2020]. The BCM lifecycle includes five phases: operational planning and control, business impact analysis and risk assessment, business continuity strategy, establish and implement business continuity procedures, and exercising and testing, as shown in Figure 2.1.

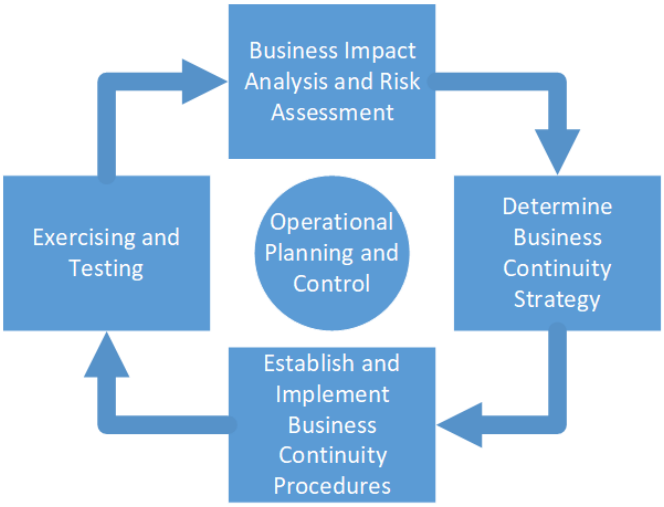

Figure 2.1: BCM lifecycle [ISO 22313:2020, p. 15]

For organisations about to take their first steps in BCM, a good place to start is the Planning phase.

2.1.1 Operational Planning and Control

As in most management disciplines, the implementation of BCM should be organised as a project, whereas the management service operation that follows should implement processes for continuous improvement (e.g. [NIST-SP800-34, pp. 31–33]). As in any project, objectives and timescales need to be identified, resources must be allocated, and roles and responsibilities assigned to competent individuals.

A busines continuity framework assists in preparing an organisation's BCP by proposing a division of content into various plans and chapters. The BCP details the roles, processes, instructions and resources required to manage business operations amid a disruption and restore processes to resume normal business operations. The BCP also defines quality requirements for acceptable levels of the overall BCM response. It is important to also identify and include the dependencies of processes. The BCP must document all known additional resources on which critical business processes rely (e.g. federated login, computing resources (IaaS, SaaS etc.)). The BCP must assist an organisation in responding effectively to any disruption. Decision trees based on the type of disruption help to structure the information and guide the response.

2.1.2 Business Impact Analysis and Risk Assessment

The objective of all business continuity actions is the restoration of key business activities after a disruption has occurred, minimising interruption and damage (e.g. data or productivity loss) as far as possible and within specified time frames. For this purpose, an organisation must identify its mission-critical activities, which are then formally designated in a Business Impact Analysis (BIA), an important milestone in business continuity preparations [Balboni, pp. 23–24]. While it is up to organisations to define what their mission-critical activities are, these are usually deduced from contractual obligations, public acceptance or revenue generation.

A BIA provides the foundation for a business continuity programme. The preparations needed for conducting a BIA include identification of the business processes for each department, and of the personnel resources and technologies needed to support them [Snedaker]. Once these and the corresponding legal and regulatory requirements are determined, they serve as a foundation upon which to conduct a BIA. A BIA should follow a structured format,[3] ensuring the collection of uniform information across departments and including professional stakeholders in the process [Snedaker]. While no methods for conducting a BIA are outlined here, much documentation is available on the topic (e.g. [NIST-SP800-34, pp. 29–33]). The results of a BIA should include two requirements to be identified for each business activity:[4]

- The **Recovery Time Objective (RTO)** is the time frame after which the business activities must be resumed following a disruption. This has direct consequences for the type and amount of spare processing capacities that are prepared and provided for disruptions, as well as for the pressure that is put on the restoration team to recover and resume the business activities.
- The **Recovery Point Objective (RPO)** is the time frame that indicates how much data can be lost. This is the interval between two backups, directly affecting the backup-and-restore strategy for data.[5]

Conducting a BIA also includes an assessment of the risks associated with each identified business process in order to rank them. Risks should be mitigated where feasible or addressed in the BCP. A BIA and risk assessment are key prerequisites for BCM [Păunescu].

2.1.3 Determining Business Continuity Strategy

The BC strategy describes the overall business continuity approach of an organisation. This includes analysing the results of the BIA and its risk assessment, and addressing them in the BCP to meet the overall business continuity goals of the organisation [ISO 22313:2020, p. 21]. The strategy should achieve a balance between the cost of adding resilience and the benefits to both the business in the face of a disaster. The following elements are considered [ISO 22313:2020]:

- The necessary technological infrastructure and costs are determined to provide acceptable interruption times and data loss.
- The necessary technology and costs are determined to maintain critical systems continuously except in the case of major disasters.
- Requirements are determined separately for all systems and presented to management for approval.

[3] A structured guide will be prepared following the publication of this deliverable.

[4] As this analysis is focused on NRENs it does not include production of goods as a business activity. Where an organisation produces goods, these processes and facilities will also be affected. Therefore, analogous continuity preparations must be considered for these.

[5] It is also worth noting that creating a new backup should not start with overwriting or deleting the previous backup, in case a disruption occurs during the creation of the new backup.

2.1.4 Establishing and Implementing Business Continuity Procedures

Establishing and implementing business continuity procedures includes writing and maintaining the BCP and its subsequent plans, including the Incident Management Plan or Business Recovery Plan. The overall BCP is more general and links to more detailed and focused plans.

Implementing business continuity procedures includes addressing risks using preventive and protective measures as well as effectively enforcing the BCP, which demands that the required services, protocols and infrastructure must be provided.[6] The BCP must finally be communicated to staff to raise awareness. This requires senior management commitment.

2.1.5 Exercising and Testing

Exercises and rehearsals are vital to building confidence in the BCP and identifying any errors and omissions it may contain. This phase also includes ensuring that everyone in the organisation receives basic BCM awareness training and that those with specific responsibilities are trained accordingly .

Another important part of BCM is testing of established business continuity plans and preparations. This can identify concepts and processes that should be improved before a disruption happens and should result in an improved response. This in turn results in less frequent, shorter disruptions with less data lost.

Finally, a formal audit and review process, as required by the relevant ISO standards, may help to ensure that each element of BCM remains up to date and fit for purpose [ISO 22301, p. 20]. The audit process increases confidence in the BC strategy.

[6] See [ISO 22313:2020, p. 28 –32] for specific examples.

3 BCM and Risk Management

The main purpose of Risk Management in the context of Business Continuity Management is the identification and assessment of potential risks that could disturb the business, as well as the treatment of those risks in a feasible way to minimise the probability of their occurrence.

The overall goal for an organisation is the sustained ability to respond to and survive both anticipated and unanticipated strategic threats and crises. Evaluating this approach and the organisation's preparedness level can identify any missing elements. There are multiple preparedness level models for BCM (see e.g. [Supriadi]). For example, to achieve the highest level of the Marsh BCM preparedness level, an organisation needs to have integrated BCM into its overall risk management and operational strategy.

One of the key prerequisites for successful implementation of BCM is a thorough understanding of potential risks. Risks can be positive, negative or neutral. A risk is often defined as an event or a consequence [Gratt]. Some examples of risks include interruption of the business cycle or business process arising from government regulations, economic conditions, social conditions, weather systems, natural disasters, and other sources. But risks can also have a positive influence on the business cycle, such as positive changes in policies or technology developments bringing benefits to the business.

Risk management (RM) is a process that has the objective of reducing the impact of uncertainty on an organisation's ability to meet its objectives [SIG-ISM_WP]. RM has long been a key part of project management, but in recent years it has become an increasingly important part of organisational best practices [Crispim]. Organisations have realised that in addition to reducing the negative impact of crises, effective RM can also provide further benefits and cost savings [Saeidi]. RM as a business process allows IT managers, for example, to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organisation's missions, although its benefits are not unique to the IT environment. Minimising the negative impact of uncertainty and crises on an organisation is the fundamental reason organisations implement a RM process for their IT systems.

Risk assessment (RA), a key activity in the RM process, can be performed at different levels, depending on requirements, policies or available resources, starting with an overall RA, followed by an RA of business processes, and finally an RA of each of the systems implementing a business process.

Management support for RA is crucial. One important element of this is that a policy should be in effect that supports a risk-based approach towards information security. All results of the RAs should be reported back to management to ensure that any corrective actions are implemented where needed. The involvement and commitment of senior management therefore ensure the successful balancing of risk mitigation techniques and BCM.

4 BCM, Incident Response Management and Personal Data Breach Management

In this section, the relationship between Business Continuity Management and Incident Response Management (IRM), as well as between Business Continuity Management and Personal Data Breach Management (PDBM), are described. Some findings from surveys sent out to several NRENs are also presented.

4.1 How Incident Response Management Relates to BCM

Incident Response Management (IRM) includes all activities related to receiving and reviewing incident reports and appropriately responding to an incident. For IT-related incidents, these tasks are conducted by a dedicated Computer Security Incident Response Team (CSIRT).[7]

IRM contributes to BCM as its main objectives are to react to and stop incident-causing events and to restore acceptable levels of service quality and availability as quickly as possible. The intention is to minimise impact on business operations to resume "normal service operation", intended as the level of service specified by the relevant service-level agreements (SLAs).

A questionnaire was sent out to selected CSIRTs of European NRENs,[8] to take a snapshot of their Incident Response (IR) processes as relevant to business continuity planning. The responses[9] were normalised, anonymised, evaluated and assessed according to a traffic-light scheme[10] to compare the NRENs.

The questionnaire covered different tasks typically performed by CSIRTs. It was divided into sections relating to *Incident Handling* (namely Breaches), *Incident Response Plan*, *Incident Investigation*, *Collecting and Storing Network Traffic Data*, *Transferred over the Internet* and *Incident Management*. Four of the contacted CSIRTs responded to the questionnaire, which were assigned the reference numbers 2834, 3915, 6331 and 7924.

[7] Or Computer Emergency Response Team (CERT).

[8] CSIRTs were selected on the basis that they should have different maturity levels if possible. These were DFN-CERT (Germany), and the CSIRTs of CyNet (Cyprus), GRNET (Greece), and SWITCH (Switzerland). The intention was not to conduct a comprehensive survey, but to gain some first insights.

[9] For full details see Appendix A.

[10] Green indicates an advanced stage of maturity, yellow an intermediate stage of maturity, and red a significant need for improvement, while no colour means that not enough data was provided to assess maturity in handling the task.

The responses to each section were summarised for each CSIRT and, in the absence of a binding evaluation scheme at that time, subjectively assessed by the evaluators, assigning a score first to each single answer, then to each section as a whole, and finally overall. While efforts were made to include all information pointing to different maturity levels in different areas, the main intention was to allow subsequent categorisation which could, as far as possible, be compared with other evaluation schemes, e.g. GÉANT Security Baseline and Trusted Introducer categories.[11]

According to the evaluation results (Table 4.1), all of the responding NREN CSIRTs were rated on average more or less yellow, with some differences; for instance, not all of the NRENs already have standardised IRM processes and procedures. However, most of them have IR plans and different responsibilities and assigned roles for IRM and BC. Furthermore, BCPs are in place or are currently being developed.

Questions for the CERT/CSIRT	2834	3915	6331	7924
Breaches				
Incident response plan				
Incident investigation				
Collecting and storing network traffic data				
Transferred over the Internet				
Incident management				

Table 4.1: IR Survey

Incidents can have a very significant impact on ordinary business operations, reducing their efficiency or completely disrupting them. Examples of such incidents include large-scale, distributed denial-of-service (DoS) attacks using botnets against web-based student portals (affecting registrations for courses and exams), exfiltration of secret research results or the encryption of IT systems of university administrations using malware with the aim of extorting ransom money, i.e., ransomware attacks.

Detecting signatures of attacks[12] at an early stage and being able to respond to them promptly and in an appropriate way requires standardised and documented IRM processes. These processes are intended to avert any attacks and minimise their impact. Adequate IRM thus serves as an essential component of BCM.

4.1.1 Recommendations for NRENs on IRM and BCM

Although they have different goals and requirements, IRM processes and procedures and BC arrangements should be closely aligned. Where possible, the CSIRT and BCM should not be run by the same staff, at least for larger NRENs. For smaller NRENs, the head of the CSIRT may also hold the role of BC Manager. Each team should have a defined and binding assignment of competencies and

[11] See Section 6 of this report for more details and comparisons.

[12] Attack signatures are special data or patterns that reveal an attacker's attempts to exploit a known vulnerability.

responsibilities, covering different, complementary skill sets. Responsibilities should be clearly assigned (communication) and process documentation updated based on dedicated plans (IR Plan, IM Plan, Communication Plan), and these aspects should be addressed in the BCP.

Furthermore, a defined communication protocol is required between the CSIRT and the BC Manager,[13] for example to ensure timely reporting in a standardised form. It is just as important to coordinate mitigation measures, in which case the BC Manager plays a central role. The BC Manager has a tactical role here, while the CSIRT has an operational role in handling incidents.

4.2 How Data Protection Management Relates to BCM

Violations of the security of personal data as well as unlawful processing of personal data or inadequate Data Protection Management (DPM) can have a highly negative impact on an organisation.[14] Possible negative effects include but are not limited to financial sanctions as well as a ban of the processing by supervisory authorities,[15] with the latter effectively resulting in disruptions of business processes. Implementing DPM is important to ensure business continuity by preventing disruptions and setting up a management system that is able to deal with gaps in the security infrastructure protecting the processing of personal data. DPM comprises all those activities conducted by an organisation (controller) that focus on compliance for its processing of personal data. Compliance also requires accountability guaranteeing the security of the processing.[16]

One particularly time-critical process in DPM is the handling and management of violations of the security of personal data, known as Personal Data Breach Management (PDBM). A Personal Data Breach (PDB) is defined by the General Data Protection Regulation (GDPR) in Art. 4 Nr. 10 as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". The GDPR stipulates notification obligations for the controller if the breach results in some risk for the data subject, including notification of the supervisory authority (Art. 33 GDPR) if any risk is assessed, and additionally a notification of the data subject if a high risk is assessed (Art. 34 GDPR).

4.2.1 Data Protection Management at NRENs

There are no special requirements for DPM solely targeting NRENs. All stipulations from national and sectoral legislation apply. Further demands may result from contractual clauses, especially if members or customers of the NREN are public bodies which themselves are subject to regulation. DPM requirements may specifically result from a data processing agreement, with the NREN being the processor. In this case, the contract between the controller and the processor may stipulate obligations regarding DPM for this processing activity at the processor (which must be in line with Data Protection legislation).

[13] Or the person responsible for planning the organisation's BCM.

[14] Due to limited resources (especially language barriers) this analysis is limited to the legal situation within the European Economic Area (applicability of GDPR).

[15] Under applicability of the GDPR, the supervisory authorities are by Art. 58 (2) GDPR authorised to impose an administrative fine (lit. i) or a temporary or definitive limitation including a ban on processing (lit. f).

[16] Under applicability of the GDPR: Art. 24 (1, 2) with Art. 32 GDPR.

Most of GÉANT's members are small and medium-sized enterprises[17] [Compendium]. Data Protection legislation usually stipulates a risk-oriented approach to DPM,[18] considering the potential and limitations of organisations and in all cases requiring the approach to be appropriate. It remains important to justify and document decisions during the implementation of DPM to account for the appropriateness of controls (e.g. Art. 5(2) GDPR).

A survey[19] was conducted among NRENs of the GÉANT community about their approaches to DPM, and specifically PDBM. The objective was to take a snapshot of DPM at NRENs and propose recommendations for improvements. The results of the survey will be published at connect.geant.org. The findings deemed most important for the purposes of this report are summarised below:

- Two-thirds of the NRENs have workflows in place for handling PDBs. PDBs are handled similarly to IR rather than through dedicated PDB processes. The major differences between IR and PDB handling concern different roles and notification obligations. While two NRENs utilise dedicated tools for managing PDBs, most NRENs use task management software and documentation or forms.
- Two-thirds of the NRENs also test their PDB handling, even though the amount and scope of tests carried out varies.
- 40% of the NRENs have a business continuity strategy in place. Of these, three out of four consider DPM as an important task within BCM.

It may be concluded that 50% of the NRENs are already at a mature stage of implementing requirements from Data Protection regulation, but others achieved only little. Every NREN faces different challenges.

4.2.2 Recommendations for NRENs on PDBM

The NRENs also shared some lessons learned on PDBM:

- *The first stage of detection and analysis of the incident is very important.*
- *Documenting the approach is very important.*
- *A couple of NREN representatives complained that cooperation with system administrators is not satisfactory.* While this may be true for a few NRENs, it might not be a valid complaint for all NRENs. Raising awareness of data protection principles and requirements may help improve cooperation.

It is important to execute compliant handling of disruptions and incidents. This includes respecting the confidentiality and integrity of personal data, e.g. by investigating confidential data only where documented evidence points to it. The final recommendation is to conduct internal checks, and

[17] For 2018, all NRENs reported a staff count matching the definition of SME. For 2019, three NRENs reported staff numbers exceeding the limits of that definition [Compendium]. The definition of SME depends on the region. For Europe the following rules apply, based on the number of employees: enterprises with fewer than 10 employees are micro enterprises, those with fewer than 50 employees are small enterprises and those with fewer than 250 employees are medium-sized enterprises [2003/361/EC].

[18] E.g. Art. 24 (1), 32 (1) and 39 (2) GDPR.

[19] Responses were received from 27 NRENs. The answers given were heterogeneous in quality, scope and detail.

external audits and verifications of the DPM approach regularly as well as if any major changes are made to it.

4.2.3 Training and Awareness of Staff

The organisation is required[20] to train all staff[21] regularly on the detection and reporting of breaches, as not all types of breaches can be detected automatically by services. The organisation must conduct appropriate levels of training. Proper data protection training covers multiple areas: raising awareness, identification and reporting of suspected incidents, and training on avoiding situations that may develop into an incident.

4.2.4 Handling of Incidents and Breaches

One way to optimise process handling is to integrate PDBM and IRM workflows. The main recommendation is to provide a single point for reporting incidents and the subsequent collaboration between PDBM and IRM. The IRM team notifies a dedicated PDB-handling taskforce of an incident which violated the security of personal data. Subsequently, both teams coordinate to respond to the incident and fulfil their notification obligations.

[20] This requirement deviates from Art. 32 GDPR for processing personal data.

[21] Even though not all roles process personal data, everyone working for the organisation should be qualified to detect and report personal data misuse (e.g. facility management should be able to report if personal data records are not secured properly or if these records are not destroyed appropriately, even though they do not usually process personal data).

5 BCM Methods and Standards

Implementing full-scale Business Continuity Management (BCM) covering the entire organisation can be a complex endeavour, requiring awareness as well as substantial investments of resources in time and expertise. NRENs, being mostly SMEs, usually do not have these resources, as they may have limited staff or high staff turnover [Compendium]. The Lean BCM approach described below enables organisations with limited resources to implement BCM, thus providing service operation continuity to their users. The S7 Business Continuity Framework introduced here is based on the Lean BCM approach and was developed by GN4-3 WP8 T1 building on the work carried out by Verdonck, Klooster & Associates for the Dutch NREN SURF [FBC] in 2017. The framework's light-touch requirements are especially advantageous for NRENs introducing BCM or conducting a Business Impact Analysis (BIA) for the first time. A comparison of the S7 Framework to other frameworks is also provided.

5.1 The Lean BCM Approach

As mentioned in Section 2.1.2, performing a BIA is a prerequisite for implementing BCM. This task usually takes up significant time and resources, as the entire organisation's business processes are analysed using a bottom-up approach. As this is a protracted task, should an organisation fail to persevere with it, its implementation may remain unfinished or even cease altogether. Initially devised for organisations in developing countries, the Lean BCM approach can also help introduce BCM in small and medium-sized organisations that cannot easily cope with the financial burden of full BCM [Monahan].

The Lean BCM approach proposes to cut down the BIA by having business processes selected by senior management. This reduces time and resources significantly but introduces the drawback of management bias, as the selection is based on subjective decisions rather than objective evaluation. This might seem contrary to the suggestions of the European Union Agency for Cybersecurity (ENISA) in [Balboni], where the BIA is seen as a key step towards the prioritisation of processes and the development of BCM. However, if management has a thorough understanding of which of their organisation's business processes are core, this drawback is negligible. While a typical BIA takes stock at the beginning, the Lean BCM approach accomplishes completion of the business process inventory using an iterative process over multiple rounds. Changing the perspective of business process selection makes this a top-down approach instead of the usual bottom-up approach. In the Lean BCM approach, the input provided by senior management reduces the number of processes for which a BIA needs to be performed to just 20–25% of all an organisation's business processes [Prabhu].

It is a common misconception to consider Lean BCM to be superficial and not thorough enough. However, based on this approach, once the critical subset of processes initially identified by senior management have been analysed, BIAs should continue to be conducted in subsequent rounds for all

remaining processes, in order of diminishing importance, until every business process has been analysed. The advantage of this approach is that the most important processes are prioritised, and actions in the form of BC measures are implemented for them before all other processes are analysed, ensuring that should a disruption happen during this time, critical processes could continue to operate or be recovered and resumed in a coordinated way. This can also be viewed as a reverse process from the transitional BCM. The rationale for this is that the organisation starts from the recovery plans, further tests them and finally adopts those plans.

5.2 Introducing the S7 BCM Framework

Based on the Lean BCM approach, GN4-3 WP8 T1 has developed the S7 Framework for BCM to enable NRENs to get a head start in conducting and implementing BCM, by prioritising their most important processes based on the decisions of their senior management, while continuing to work on the remaining processes in due course.

WP8 T1 has adapted the S7 BCM framework developed for SURF as described in the *Framework Business Continuity 2017* document [FBC] by introducing enhancements in the way groups are first defined for processes and used later to identify controls. Maturity levels are also adopted to help NRENs (or implementing organisations) to select an appropriate set of controls for their current implementation cycle.

The policies, plans and guidelines adopted by NRENs to manage business continuity are collectively referred to here as the "S7 BCM Framework". This is a systematic and comprehensive framework to ensure NRENs can effectively manage BC in the event of a disruption. The S7 BCM Framework ensures resources are available to business areas to initiate temporary arrangements to continue delivering an NREN's most time-critical business processes.

The S7 BCM Framework was developed to:

- Understand the potential risks of unplanned disruptions, especially those related to the provision of an NREN's key services.
- Prioritise the NREN's time-critical processes/activities/functions, required recovery time frames and hence the restoration priority for business operations.
- Provide strategies for business as usual (BAU) within agreed and acceptable time frames.
- Create action-oriented procedures to respond to a disruption in an efficient, effective and timely manner.
- Establish principles and capabilities that are lean-based such that they enable an organisation to respond to a variety of future disruption events.
- Periodically review, modify, update or revise the business continuity framework to account for new organisational risks.

Figure 5.1 illustrates how the framework impacts all phases of the Plan-Do-Check-Act cycle that is normally used in management. Specifically, where it interacts with the Plan and Check phases a feedback loop may be established where the framework is not suitable to meet an organisation's needs and adjustments are required.

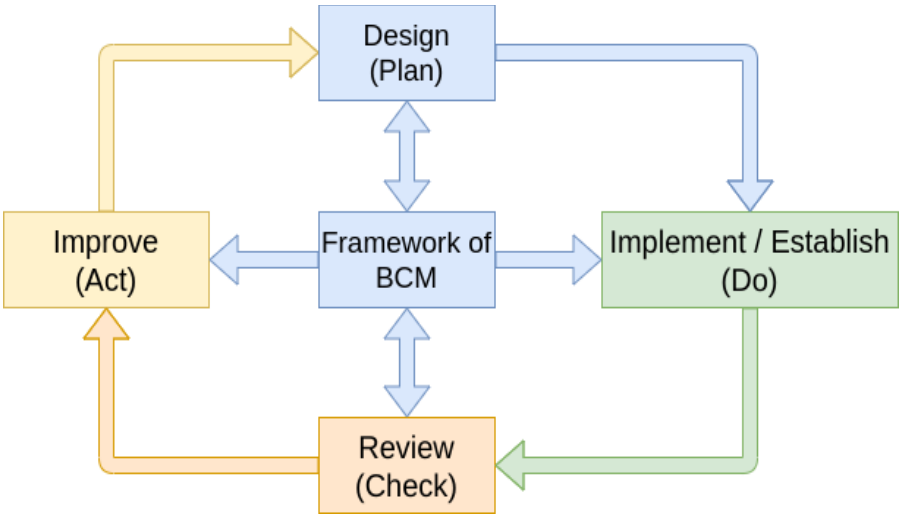

Figure 5.1: S7 BCM Framework cycle mapped to Plan-Do-Check-Act cycle

5.2.1 S7 BCM Framework Subject Areas

In this approach, the S7 BCM Framework measures are grouped by seven subject areas of interest. Together, these comprise the scope of BCM for an organisation, covering all the areas where essential controls should be implemented. These are:

- Governance, Strategy and Policy.
- Crisis Management and Communication.
- Emergency Continuity.
- Restore and Recovery.
- Exercising and Testing.
- Awareness and Training.
- Foundation.

Foundation and Emergency Continuity can be further split into sub-topics for which appropriate measures can be defined (see Figure 5.4).

Review and continuous improvement are built into the framework, particularly as part of Governance, Strategy and Policy, Exercising and Testing, and Awareness and Training, and are the basis of the priority-based, incremental, Lean BCM approach it embodies.

Short descriptions taken from the SUF documentation [FBC] for the subject areas that are not self-explanatory are given below to show how they can be built upon and guide NRENs in their approach. It is recommended that a practical approach be taken to some of the measures, for which implementation advice based on the original document is given. Further detail on all seven areas is provided in Appendix B.

5.2.1.1 *Crisis Management and Communication*

Crisis management is important for the effectiveness of BCM: when a major disruption occurs and (potentially) turns into a crisis, adequate command, control and communication are needed. Crisis communication, founded on a stakeholder-based strategy and plan, can help in the mitigation of impacts through effective provision of information to all stakeholders.

5.2.1.2 *Emergency Continuity*

Emergency Continuity deals with all procedures, solutions and actions needed to maintain an acceptable level of delivery during a disruption. These can be temporary solutions and need to be terminated in a controlled way when the situation has normalised again.

5.2.1.3 *Restore and Recovery*

Restore and Recovery deals with all procedures, solutions and actions that are used to overcome the impact of a disruption and return to a stable and permanent situation. (In parallel, exploring process alternatives may form part of the risk management/mitigation activity.)

5.2.1.4 *Foundation*

The professionalism and robustness of day-to-day operations determine the scope of BCM measures and how often they are invoked. Flaws in operational procedures, incomplete contracts, non-redundant infrastructures, ineffective security, etc. all contribute to making an organisation vulnerable to disruptions. While it is important to define BCM measures where these flaws are found, preventive measures to strengthen the resilience level of operations should be taken, which is the direct responsibility of line management.

The starting point for this are usually the **Foundation** and **Emergency Continuity** cycles (Figure 5.2), which are coordinated to provide better resiliency. Resiliency measures are categorised as protective, detective, responsive and measures for recovery. Protective measures prevent a disruption, while detective, responsive and recovery measures are required for incident response and BCM. Figure 5.3 highlights the elements of Emergency Continuity and Foundation that are coordinated to increase the resilience of an organisation.

The outcomes of the S7 BCM Framework activities outlined in this section will ascertain the applicability of BCM to the NREN and develop an understanding of whether and how BCM is already being used. The value of using the framework when implementing a BCM programme within the NREN is to provide a tried-and-tested starting point tailored to the community's needs, and design criteria that could be used to build internal BCM knowledge and capabilities.

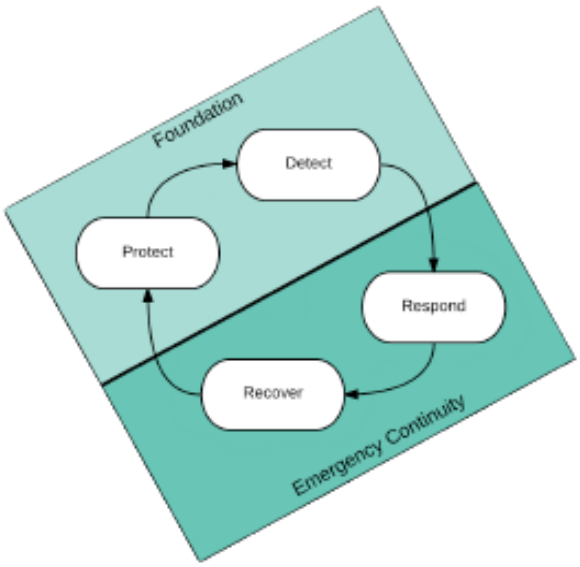

Figure 5.2: Emergency Continuity

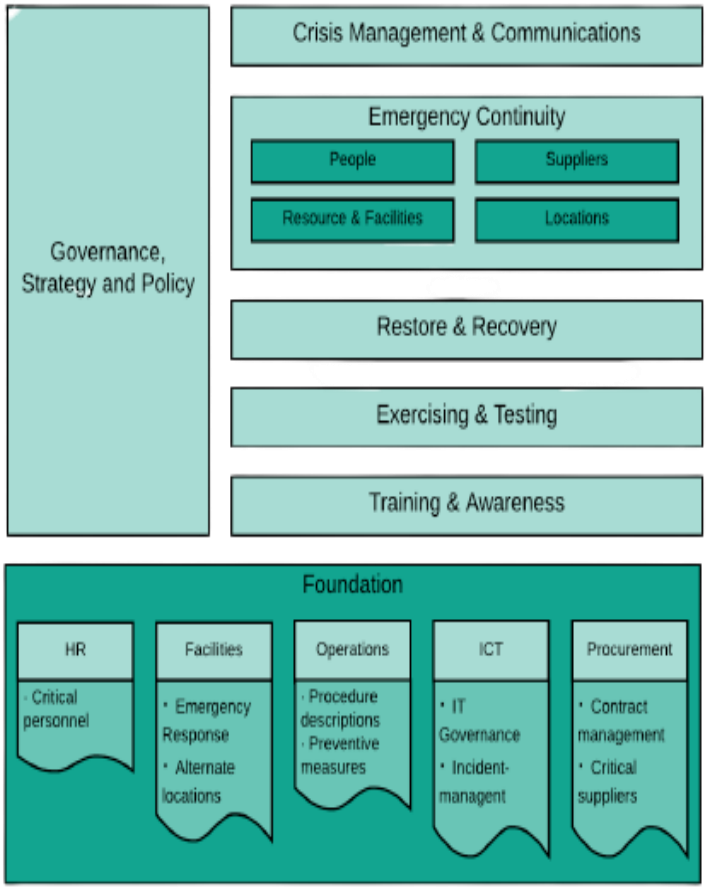

Figure 5.3: Foundation and Emergency Continuity

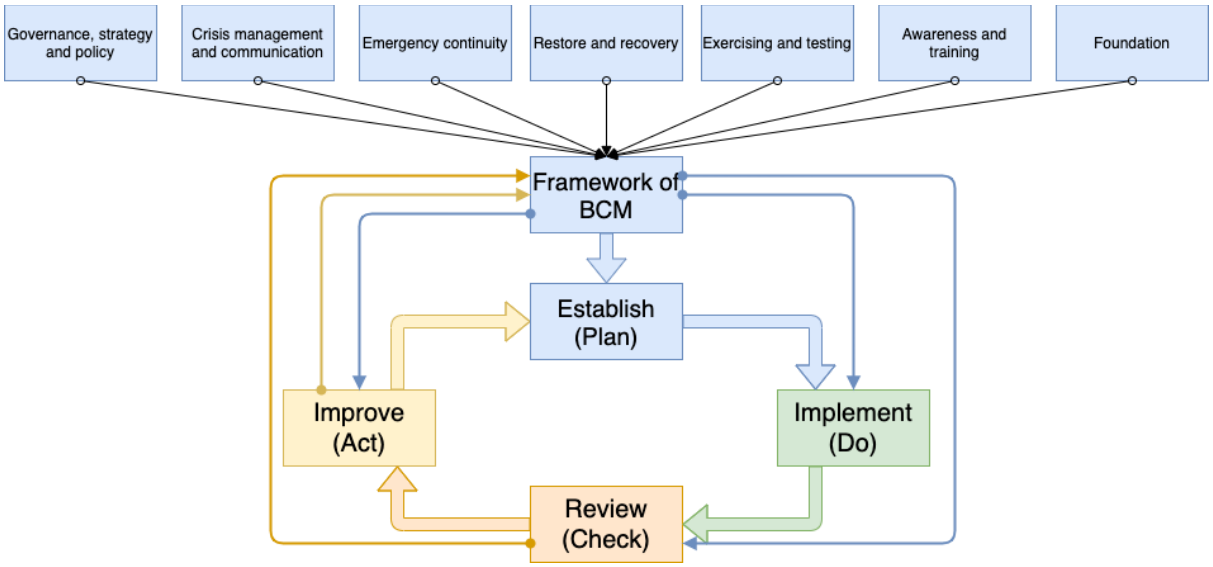

Figure 5.4: BCM Implementation

5.2.2 Maturity Levels

Implementing BCM based on the risk associated with its various processes requires an organisation to determine the appropriate maturity level that should be reached with the first iterations. Determining this target maturity level usually requires expert knowledge both of business continuity and of the organisation. This section provides some guidelines to enable non-experts in BC to select the appropriate maturity level and help NRENs evaluate their business continuity approach.

In order to measure the BCM maturity of an organisation, the five-level scale established in the original SURF document [FBC] is used. This is based on the Capability Maturity Model (CMM), which evaluates the maturity of processes. These five levels are described in Table 5.1.

An increase in maturity should be achieved gradually and usually not exceed one level of increase per year. Where a more rapid increase is necessary, this can be facilitated by narrowing the scope and focusing on fewer measures.

CMM Level		CMM Level Description
0	Non-existent	No process is in place
1	Initial/Ad Hoc	No standardised processes are in place
2	Repeatable but Intuitive	Procedures are followed but there is still a high degree of reliance on the knowledge of individuals
3	Defined Process	Procedures are standardised but not sophisticated enough
4	Managed and Measurable	Compliance with required procedures is measured and significant errors are detected
5	Optimised	A refinement of processes to a good level of practice has taken place and variances are constantly reduced

Table 5.1: CMM levels

For every control, a CMM level is recommended. The recommended level usually describes the control's significance for business continuity. The level is usually set at 2, 3 or 4, with Level 4 requiring the control to be evaluated and adjusted on a regular basis. A simple example of this is the BCM policy itself. When an organisation has defined a policy but has not yet implemented a management process around it, its level is 3. When regular evaluation and adjustment takes place, its level is 4.

The levels recommended in the SURF document are well-founded and are based on the following rules:

- The management process around the control is crucial and cannot be omitted: CMM level 4.
- The control is an essential part of the implementation of business continuity: CMM level 3.
- All other controls are given a start level: CMM level 2.

Applying CMM levels allows NRENs to start the BCM process at a level appropropriate to their size and capacity and to then gradually build up and improve it by focusing on key areas in order to achieve the appropriate target. In the initial process, it is recommended that NRENs select lower levels which are achievable and then focus on smaller areas in order to improve the BCM following its implementation plan. The specific needs of an NREN can be considered to adjust levels as proposed in the document [FBC]. This assessment should be carried out on a case-by-case basis, depending on the NREN's size and the staff and resources that can be allocated to the BCM implementation process.

5.3 Comparison of S7 BCM Framework with Other Models and Standards

Various authors have proposed different development cycles for BCM [ISO 22313:2020], [Gratt], each of which places emphasis on particular aspects of the process. The S7 BCM Framework draws on these approaches and their experience in the field. Each phase defined in Figure 5.3 is illustrated using a standard template which highlights the key activities that must be undertaken, and the associated inputs and outputs. The identified phases are:

1. Programme initiation.
2. Project initiation.
3. Risk analysis.
4. Selecting risk mitigation strategies.
5. Monitoring and control.
6. Implementation.
7. Testing.
8. Education and training.
9. Review.

Effective information management requires the creation of an environment in which information can be shared with any authorised person [Gibb]. BCM and information management have in common

that both address uncertainty. Generally speaking, a lack of investment in BCM can result in loss of revenue at best and cessation of business activities at worst.

Therefore, an organisation (or NREN) will need to consider:

- What is the worst thing that could happen to our business?
- Where would we be operating tomorrow if a disaster occurred?
- How quickly could our business reach the point of no return?
- How quickly can we return to business as usual?

A comparison is drawn between the S7 BCM Framework and five other frameworks in order to assess which areas and phases of BCM they cover and later specifically their applicability to NRENs. Short descriptions of these frameworks are given below:

- A new framework for business impact analysis in business continuity management (with case study) [Torabi]. Applied fuzzy DEMATEL-ANP method. This framework proposes a novel framework to conduct a BIA in organisations in a more systematic and comprehensive way, mostly by relying on some effective multi-attribute decision-making (MADM) techniques.
- Evaluation and Prediction of Business Continuity Risks [Kazakova]. The purpose of this study is to develop the auditor's analytical tools for assessing and predicting the business continuity of audited companies, as well as performing audit assignments using the financial methodology of Due Diligence. The proposed methodology for assessing and forecasting the company's business continuity risks includes four stages: financial results assessment; solvency assessment; identification, calculation and financial risks of the company's business continuity assessment; and forecasting changes in the level of risk of business continuity using the developed calculator for calculating risk factors indicators.
- IT incidents and business impacts: Validating a framework for continuity management in information systems [Järveläinen]. The framework was validated in a survey of IT managers and chief information officers in large private and public organisations operating in Finland. The results of the survey suggest that the embeddedness of continuity practices in an organisation has perceived business impacts whereas, in contradiction of previous theory, there is no such direct relation in the case of organisational alertness and preparedness.
- Business Continuity Management for Supply Chains Facing Catastrophic Events [Suresh]. The first set of frameworks listed above tended to be more structured, reflected in the emergence of standards such as ISO 22301. Organisations are increasingly subject to many types of disruptions and catastrophes, with little or no predictability, and with increasing frequency and high impact. In response to these, organisational risk management has been pursued broadly in two different ways. One approach has been to adopt procedures such as business continuity management (BCM), enterprise risk management (ERM), and related approaches.
- Business continuity-inspired fuzzy risk assessment framework for hospital information systems [Haghighi]. Fuzzy risk matrix. The framework benefits from a fuzzy multi-criteria decision-making method and a fuzzy inference system to quantify and analyse the uncertain information gathered from experts.

A summary comparison of these frameworks, focusing on the S7 BCM Framework subject areas defined in Section 5.2.1, is given in Table 5.2 below.

S7 Area	BCM: a systemic framework	Framework for BIA in BCM	Evaluation and Prediction of BC Risks	IT incidents and business impact validation framework	BCM for Supply Chains Facing Catastrophic Events	BC-inspired fuzzy risk assessment framework
Governance, strategy and policy	Layer 1. Server operating system (environment)	Business impact analysis (BIA)	Risks of untimely settlement of obligations	Perceived business impacts of ISCM	Examine Organisational Context of Supply Chain	Risk analysis
Crisis management and communication	Layer 2. Storage, backup and recovery technologies		Risks of lost profits	Embeddedness of continuity practices	Leadership	
Emergency continuity	Layer 3. Networking infrastructure			Organisational alertness and preparedness	Prevention (Mitigation Tactics)	
Restore and recovery	SysAdmin (Fine-Grained privileges)			Management support	Recovery (Response Tactics)	
Exercising and testing	IT-Governanace (ICT Complance)			External requirements	Assessment of Plans	
Awareness and training	BCM (Busisness Impact Analysis				Continuous Improvement	
Foundation	-	-	-	-	-	-

Table 5.2: S7 BCM Framework areas covered by different frameworks

Table 5.3 below shows which phases are covered by the different frameworks.

Phases	S7	BCM: a systemic framework	Framework for BIA in BCM	Evaluation and Prediction of BC Risks	IT incidents and business impact validation framework	BCM for Supply Chains Facing Catastrophic Events	BC-inspired fuzzy risk assessment framework
Programme initiation	X			X	X	X	
Project initiation	X				X	X	
Risk analysis	X	X	X	X	X		
Selecting risk mitigation strategies	X					X	X

Phases	S7	BCM: a systemic framework	Framework for BIA in BCM	Evaluation and Prediction of BC Risks	IT incidents and business impact validation framework	BCM for Supply Chains Facing Catastrophic Events	BC-inspired fuzzy risk assessment framework
Monitoring and control	X	X			X	X	
Implementation	X	X				X	
Testing	X	X				X	
Education and training	X						
Review	X	X		X	X	X	

Table 5.3: BCM phases covered by different frameworks

Table 5.3 shows the completeness of the S7 BCM Framework, indicating how it covers all areas of business continuity found in the other frameworks summarised above. Using other frameworks that only partially cover the areas, NRENs cannot cover all of them. Therefore, it can be concluded that the application of the S7 BCM Framework represents the most thorough approach and will achieve the best result for NRENs. While the framework offers an optimum starting point, covering all the areas where essential controls should be implemented, prioritisation of those areas, as with the identification of mission-critical activities and the selection of CMM levels, will depend on the specific needs and circumstances of each individual NREN. (Indicative feedback on prioritisation, from a small subset of NRENs, is given in Section 6.4.)

6 S7 BCM Framework Integration with other GN4-3 Standards

The use of the S7 BCM Framework is considered in this section in comparison with two other proven evaluation measures developed by the GN4-3 project, the *Security Baseline for NRENs* [D8.2], produced by the Security work package (WP8), and the TF-CSIRT Trusted Introducer [TI] services, which aim to provide CSIRTs with a common foundation collaboration. The intention is for these three frameworks to strengthen each other to increase prevention and resilience. Parts of these frameworks may overlap and therefore NRENs may not need to apply them all in all areas. For this reason, this section provides a mapping of recommended controls from the BCM Framework with those of the other two frameworks.

The GÉANT Security Baseline provides NRENs with a benchmark for evaluation and comparison that enables them to assess their internal organisation with regard to security aspects in various categories and areas, and to identify and eliminate any specific deficits. Its focus is primarily on organisational aspects for operation of data centers and networks.

On the other hand, the intention of Trusted Introducer (TI) is to create a community of trust for CSIRTs. To a large extent, this is a matter of externally directed processes. Furthermore, TI services provide levels of membership (listed, accredited, and certified) to enable teams from different organisations to communicate with each other on a trustworthy, equal and confidential basis, i.e. to speak the same language and deal appropriately with information exchanged between them.

However, BCM should eventually span the entirety of an organisation and must therefore include an NREN's organisation and operations as well as Incident Response Management (IRM) processes. The approach defined by the S7 Framework keeps the initial effort for the NRENs manageable.

Assessment categories and maturity levels of TI services and the GÉANT Security Baseline are mapped[22] to the categories of the S7 Framework, so that the assessment benchmarks remain comparable, allowing NRENs to seamlessly use the services of all these frameworks.

[22] According to a kind of subjective mapping in mathematical terms.

6.1 The GÉANT Security Baseline and the S7 BCM Framework

The purpose of the GÉANT Security Baseline is to harmonise the security levels of otherwise quite heterogeneous NRENs that are members of the GÉANT Association [D8.2 Section 2]. The Security Baseline specifies three levels of security maturity: Baseline, Advanced and Expert. Their relationship is shown in Figure 6.1.

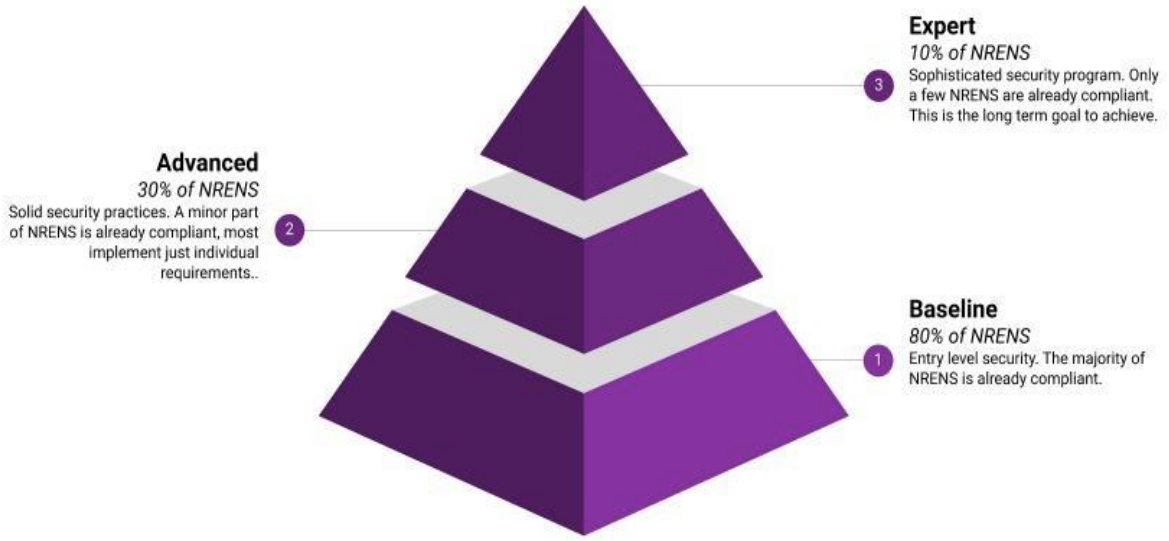

Figure 6.1: Levels used within the Security Baseline [D8.2]

Appendix D shows which areas of the GÉANT Security Baseline for NRENs are covered by the S7 Framework, or which of the categories correlate to it in each case.[23]

6.2 Trusted Introducer Services and the S7 BCM Framework

TI provides a set of de facto standards for CSIRTs, PSIRTs and other security teams [TI_Standards]. Of particular importance in this context is the Security Incident Management Maturity Model (SIM3) [Stikvoort], which was developed as a reference benchmark for the TI certification process of CSIRTs.

The SIM3 reference model consists of over 40 Maturity Parameters in four independent Maturity Quadrants (Organisation, Human, Tools and Processes). Maturity is assessed for each parameter on a scale of Maturity Levels from 0 to 4. This assessment enables easy visualisation of a CSIRT's maturity. The European Union Agency for Cybersecurity (ENISA) also provides a CSIRT Maturity – Self-assessment Tool online, which enables CSIRTs to assess their maturity using the parameters of the SIM3 model [CMSAT].

[23] For full details see Appendix D.

TI also provides services for coordination of Incident Response (IR). NRENs' external IRM was summarily evaluated according to a traffic-light scheme (see Sections 3 and 4.1). In comparison, the categories defined according to the SIM3 model, as used for TI certification, are much more comprehensive. TI categories for IR are well established within the CSIRT community and related to practice, thus are helpful and relevant for defining a BCM framework.

Appendix E shows which areas of the SIM3 are covered by the S7 BCM Framework, or which of the categories correlate to it in each case.[24]

6.3 Comparative Analysis of S7, Security Baseline and TI

While the GÉANT Security Baseline is designed to allow NRENs to self-assess their operations according to the levels Expert, Advanced and Baseline, the SIM3 model used for Trusted Introducer is aimed at incident response teams. In contrast, the S7 BCM Framework is specifically designed to provide NRENs with an easy-to-use method for assessing and developing BCM for their organisations.

BCM includes various aspects of NREN operations, IR setup and IR processes, as well as the organisational foundations, policies and management structures required for these. As such, both the GÉANT Security Baseline and Trusted Introducer have several areas of overlap in terms of assessment categories with the S7 BCM Framework. However, there are significant differences in the weighting and level of detail of the categories used by these standards.

Thus the S7 BCM Framework is not intended to replace the GÉANT Security Baseline or the Trusted Introducer SIM3 model in their respective areas of application. Rather, it is intended to support NRENs in making a quick start in assessing BCM without having to go through the other assessment processes in their entirety. However, it is certainly recommended that NRENs should continue to utilise each framework in the relevant areas of application. The S7 Framework will therefore complement the set of instruments rather than substitute them.

Overlapping categories between the S7 Framework and the Security Baseline and between the S7 Framework and TI are listed in Appendix D and Appendix E respectively. Where categories overlap, it should be noted that the Security Baseline for NRENs goes into greater detail regarding technical parameters (Tools, Cryptography, Access Management, Patch Management) in the area of operations, and SIM3 is much more differentiated in terms of the Process parameters relating to incident handling. Also, while several Tools parameters are covered by the Foundation section in the S7 Framework, these are not defined in as much detail as in the Security Baseline and SIM3 model.

6.4 NREN Feedback on Priorities

As the S7 BCM Framework proposes to perform the Business Impact Analysis (BIA) on a subset of business processes, several NRENs were surveyed to find out about their intended prioritisation. The intention of the questionnaire was to understand if there were any common processes used by all the

[24] For full details see Appendix E.

NRENs. NRENs were also asked whether they assessed themselves according to the GÉANT Security Baseline and what their result was. They were also asked what their participation and member status was in Trusted Introducer. The short introduction to the questionnaire contained Figure 5.3 to provide an overall view of the proposed framework, as well as an initial list of proposed processes. The questionnaire and introduction are attached in Appendix C, which also contains the individual anonymised answers.

The survey was sent to a small set of NRENs, as part of discussions carried out at the SIG-ISM meetings during 2019 and 2020. The results of the survey are summarised below.

Of the seven NRENs that replied to the request for information, three have performed the GÉANT Security Baseline assessment and have marked themselves at the levels Basic (1 NREN) and Advanced (2 NRENs). All contacted NRENs are part of the Trusted Introducer and have status Accredited, although for some the certification was still pending at the time.

The NRENs prioritised the processes as follows:

1. Exercising and Testing: NRENs would like to practise this more frequently, due to high rates of staff turnover, but also technical changes and continuous growth in staff numbers.
2. Governance, Strategy and Policy: due to the relatively infrequent updates of the legal documents governing the NRENs' day-to-day operations as well as lack of strategic planning.
3. Awareness and Training: for similar reasons as those for point 1, as well as the need for training non-technical employees.
4. Foundation: due to outdated procedural descriptions as well as the gap analysis of potential problems.
5. Emergency Continuity: to increase the resiliency of critical infrastructure and identify potential weak points to be closely monitored.

6.5 S7 BCM Framework Implementation

Since the proposed S7 BCM Framework is built upon extensive SURF documentation [FBC], this is reused for the basic guidelines for implementation. This is one implementation path which can be taken and it is compatible with the Lean approach. For this reason, the original Control/Area categorisation is provided as a good starting point. It is expected that future revisions of the S7 Framework will allow some controls/areas to be further developed based on the needs and feedback of NRENs. Figure 6.2 below illustrates how, therefore, starting from the Foundation, the area categories form the pillars of this BCM Framework.

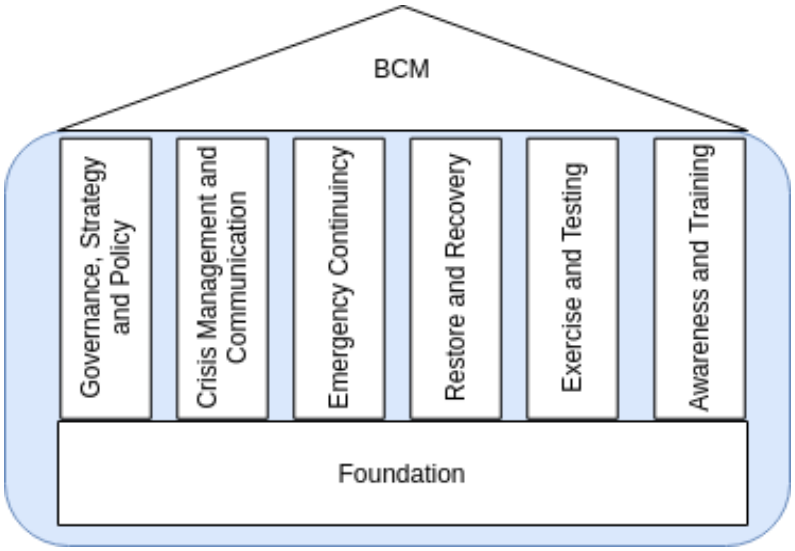

Figure 6.2: S7 BCM Framework

At the point of practical implementation, an NREN can take several different approaches. One approach is to determine their current maturity level on each subject area and then try to improve it. Another approach would be to identify and work first on improving the topic that scores the lowest level.

Practical implementation steps for NRENs for each area are given in Appendix B, along with references to the relevant standards and documents. NRENs who have already conducted a self-assessment based on the Security Baseline for NRENs [D8.2], should use the proposed S7 Framework to provide clarifications and an opportunity to improve their methods for installing the framework.

In summary, the scope of the seven subject areas defined in the S7 Framework is as follows:

- **S7.1 Governance, Strategy and Policy.** The BCM policy and strategy describe the scope and governance of BCM and give the reasons why it is being implemented and how. The main goal of the policy and strategy is to communicate to internal and external interested parties the BCM principles of the organisation and the way BCM is organised and governed.
- **S7.2 Crisis Management and Communication.** Crisis management guides and facilitates the business continuity and recovery efforts that are usually made at tactical and operational levels. Crisis communication targets all relevant internal and external stakeholders and strives to keep them informed and involved.
- **S7.3 Emergency Continuity.** Ensures the organisation can continue delivering its critical products and services during major disruptions, although this could mean the output of delivery is lower than in a normal situation. Whether this temporarily decreased level of delivery is possible at all should be analysed beforehand.
- **S7.4 Restore and Recovery.** Ensures that the organisation returns to a lasting and “stable” mode of operations after a major disruption. This includes any activity related to restoring and recovering the use and performance of people, locations, resources, suppliers, etc.

- **S7.5 Exercising and Testing**. Exercising and testing is the "proof and refinement" for all BCM measures, plans, agreements and procedures that are developed by an organisation. In order to be sure that the measures are effective and can guarantee a process of continuous improvement, periodic exercising and testing are the key activities.
- **S7.6 Awareness and Training.** Ensures that employees and contractors understand their responsibilities and are competent in the roles they have or for which they are considered backup personnel.
- **S7.7 Foundation.** Making sure that major disruptions do not occur and that the impact is manageable and safeguarded by professionalism in each department.

A complete Implementation Guide for the S7 Framework is provided in Appendix B, which gives general guidance on controls where following the formal ISO approach could result in overcomplexity, based on best practices and the pragmatic approach proposed by the Lean BCM philosophy. For any further information on the scope of the framework, readers are referred to the original SURF document [FBC] document.

7 Conclusions and Future Work

In the initial stage of preparing this report, it became clear that there is no “one size fits all” concept for how NRENs should address Business Continuity Management. While being aware of the more “classic” models and frameworks, based on valuable input from the community the approach to implementing BCM considered here involves a more dynamic framework, which is based on the concepts of “how to get there” and “how to improve” while taking into consideration the differences between NRENs in terms of size, capacity, budget, etc.

The S7 Framework promotes a lean approach to BCM. To that end, WP8 asked several NRENs to review the proposed framework and provide their opinion on what processes they consider most important and should be prioritised. One important finding that emerged from their responses was that most NRENs have not made any special efforts to address BCM, due to a lack of resources or awareness. NRENs that have performed the GÉANT Security Baseline [D8.2] self-assessment were found to be more aware of the need for BCM.

The S7 Framework is a starting point for future development and improvement which will help the community, and especially NRENs, to address BCM through an approach that is tailored to their needs and is as widely applicable as possible without consuming too many resources initially. Based on the S7 Framework, by implementing a continuous cycle of improvement and gaining a broader view of their organisation’s needs and of existing platforms such as the GÉANT Security Baseline, NRENs can rapidly improve their BCM process.

WP8 will continue to work to better understand NRENs’ priorities and help them address them in order to establish BCM in a structured and affordable manner. This will include providing practical tools and guides supporting NRENs in implementing BCM following a Lean approach. Future work will include:

- Drafting an NREN business continuity strategy.
- Drafting an example business continuity plan.
- Drafting a checklist to assess maturity against S7 Framework.
- A best practices reference guide for incidents at NRENs.
- Drafting recommendations for (awareness) training and testing.
- A structure for conducting a Business Impact Analysis.

Appendix A Evaluation of Incident Response Management at NRENs

A questionnaire was developed and sent out to selected Computer Emergency Response Teams / Computer Security Incident Response Teams (CERTs/CSIRTs) of European National Research and Education Networks (NRENs) in order to gather some first insights on NREN CERTs'/CSIRTs' level of maturity regarding Incident Response (IR) processes relevant to Business Continuity (BC) planning. The responses were anonymised and evaluated using a traffic-light scheme (green, yellow, red) in order to categorise the NRENs by maturity level. In addition, this will facilitate comparison with other evaluation frameworks, e.g. GÉANT Security Baseline and Trusted Introducer (TI) categories.

The questionnaire for the CERTs/CSIRTs covered different areas of their typical work; these were intentionally not too granular, to allow the responses to be completed within an acceptable time frame. The areas/sections were Breaches (C-3.1), Incident Response Plan (C-3.2), Incident Investigation (C-3.3), Collecting and Storing Network Traffic Data (C-3.4), Transferred over the Internet (C-3.5), and Incident Management (C-3.6).

Four of the contacted CERTs/CSIRTs responded to the questionnaire, and were assigned the reference numbers 2834, 3915, 6331 and 7924.

Each CERT's/CSIRT's responses to each area/section of the questionnaire were summarised and evaluated using the previously mentioned traffic-light scheme in order to preserve information indicating different maturity levels in different areas andalso to allow subsequent categorisation which could as far as possible be compared with other evaluation schemes, e. g. GÉANT Security Baseline and Trusted Introducer categories.

The answers and summaries are presented in Table A.1 below.

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
C-3.1	**Breaches**				
C-3.1.1	How well do you believe that you can detect a breach/hack?	At the moment it is time-consuming to detect a breach/hack. Although, we are planning to install firewalls, IPS, IDS and	Depends on the specific circumstances. No general answer is possible from our point of view.	Very well.	It has room for improvement, nevertheless there are several good practice tools and

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
		cybersecurity developed tools in the foreseeable future.	Regarding network traffic: we have a system in place, that collects data about suspicious network traffic from different suppliers, which is trained on the "usual situation" and raises warnings when it detects anomalies.		techniques in place to discover a breach/hack.
C-3.1.2	Can you assess the effects of system breaches/network hacking?	• Loss of Service (network, email, applications, etc.) • Financial Losses (employee time needed to restore services, etc.) • Loss of Information • Decreased Privacy • Damaged Reputation	Depends on the specific circumstances. No general answer is possible from our point of view. Regarding network traffic: we are using a self developed network monitoring tool that enables us to analyse and mitigate denial of service attacks and enables us to search, based on a given suspicion, for special connections, for example to known command and control servers.	Yes, while in the process of preparing for ISO 27001.	• Loss of customer (trust) • Reputation could suffer • Service interruptions
	Summary	***The differentiated assessment of the effects of system breaches/network hacking allows the impact on the business (continuity) to be rated.***	***Network traffic is continuously monitored and analysed based on trained patterns, which allows detection of breaches and raising of alarms.***	***Breaches/hacks can be detected well, which allows quick alarm raising. Assessment is planned according to ISO 27001 certified procedures.***	***The differentiated assessment of the effects of system breaches/network hacking allows the impact on the business (continuity) to be rated.***

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
C-3.2	**Incident Response Plan**				
C-3.2.1	Do you have an incident response plan?	We do have an incident response plan, validated and approved.	Yes	Yes, it is also included in the policy document.	Yes, we have an incident response plan.
C-3.2.2	When did you last test your incident response plan?	In December this year.	Depends on the service: MailSupport: 2016, next test planned for 2020. AAI: 2019, next test planned for 2020.	We apply our incident response plan daily.	A couple of years ago.
	Summary	***Regularly tested incident response plan provides basis for integrating incident response management in business continuity.***	***Regularly tested incident response plans provide a basis for integrating incident response management in business continuity.***	***Regularly applied incident response plan provides basis for integrating incident response management in business continuity.***	***Incident response plan provides basis for integrating incident response management in business continuity, even if not regularly tested.***
C-3.3	**Incident Investigation**				
C-3.3.1	Does your incident response plan include network forensics?	Yes, in cooperation with National CSIRT.	Not specifically, but depending on specific incident forensics will be conducted.	We monitor traffic flows and then attempt to distinguish malicious patterns in normal traffic based on threshold- and behaviour-based traffic baselines.	Yes, the CERT has the capabilities for network forensics.
C-3.3.2	Does your incident response plan include post-incident investigation?	Yes	Yes	Yes. Our policy includes reactive measures, when possible.	Yes
	Summary	***Network forensics and post-incident investigation support constantly***	***Network forensics and post-incident investigation support constantly***	***Network traffic is monitored and analysed based on trained patterns, thresholds***	***Network forensics and post-incident investigation support constantly***

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
		improving the business continuity planning.	***improving the business continuity planning.***	***and behaviour. Reactive measures, if possible.***	***improving the business continuity planning.***
C-3.4	**Collecting and Storing Network Traffic Data**				
C-3.4.1	How quickly can you analyse it? How long does a query take?	The system (equipment and tools) for collecting and analysing traffic data is in the development phase for the time being.	No specific provisions are existing; depends on specific incidents.	Immediately. We are using Arbor Peakflow appliances with 1:100 sampling for collecting flows from Network. Based on this, query time is minimum.	The CERT can analyse the network traffic data immediately. The query can take from minutes to hours or even days, depending on the search range and the query itself.
C-3.4.2	How long do queries take when run at the same time as the ongoing capture of network traffic?	N/A (see above)	No specific provisions are existing; depends on specific incidents.	Again, query time is minimum.	See answer above.
C-3.4.3	How far back in time can you look to investigate?	After the completion of our system and depending on Incident Severity: High: 6 months Medium: 2 weeks Low: 2 Weeks	Payload contents not at all, sampled netflows and firewall logs 2 weeks.	Quite long archiving time. Comfortable, but might be an issue with privacy regulations. 2 years back.	3–4 weeks
	Summary	***For the time being, there is no running system to regularly collect and analyse network traffic data, for which reason real monitoring is not feasible.***	***The net flows and firewall logs are monitored and collected 2 weeks back, but not stored for longer periods of time due to data privacy law regulations. Especially, content data is not collected at all.***	***A (commercial) appliance is used to collect net flows, which allows quick analysis. This data is stored for 2 years, which might conflict with EU data privacy restrictions, though.***	***Network traffic data can be analysed immediately, whereby the required time depends on the range of the query. Data is accessible 3–4 weeks back.***
C-3.5	**Transferred over the Internet**				

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
C-3.5.1	What are the main determinants of the process of integrated cyber risk management and information security on the Internet?	After the completion of our system: • Monitor the Risk Environment • Assess the risks' impacts and actions required • Monitor Data Assets • Create a Risk Plan • Gain Management Support • Prepare Employees • Build Strong External Relationships • Enforce Security Protocols • Evolve with the Technological Environment	Current status: We are discussing the intention of the question and can't provide an answer right now.	The CERT and the Network Operations Center.	
	Summary	***Prospective planning for cyber risk management, even though not really implemented, yet.***		***CERT/CSIRT and NOC are working together on integrating cyber risk management and information security.***	
C-3.6	**Incident Management**				
C-3.6.1	Do you have a management structure in place for dealing with the incident, i.e. people who can make appropriate decisions on behalf of the organisation?	Yes (CSIRT Team Leader)	Yes	Based on the nature and severity of the incident, there are certain people (CISO, CERT members, support) who are responsible for its resolution.	Yes
C-3.6.2	Do you have a site dedicated (Emergency Control) for managing the incident?	Yes (CSIRT Team)	The CSIRT is certified by TI. In addition, a crisis management team, if an	The CERT employs open source software to process, correlate and notify end	No

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
			incident is escalated to status “crisis”.	users about the reports that it receives. Specifically, We have deployed a fork of AbuseIO: an open-source toolkit that can be used to receive and process abuse reports received by network operators.	
C-3.6.3	Do you have an information strategy to inform/for dealing with Staff?	Ongoing Process Design	No	We perform cyber security awareness presentations on an annual basis.	Yes
C-3.6.4	Do you have an information strategy to inform/for dealing with Press?	Ongoing Process Design	Press contacts only with approval of CEOs.	No	Yes
C-3.6.5	Do you have an information strategy to inform/for dealing with Stakeholders?	Ongoing Process Design	No	Yes	Yes
C-3.6.6	Do you have an information strategy to inform/for dealing with the Public?	Ongoing Process Design	No	No	Yes
C-3.6.7	Are your senior management & operational management teams trained in business continuity and managing incidents?	No	Yes	No	Depends on the team. Most teams, including the CERT, can handle incidents (very) well. A bigger problem would be the topic of business continuity.
C-3.6.8	Do you have a regularly updated Business Continuity arrangement that includes	Yes	Yes	No	No

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
	your incident management process, notification procedures, recovery strategy / procedures and the estimated recovery time for your products, services and works?				
C-3.6.9	Have you consulted your suppliers, service and utilities providers during the preparation of plans, and regularly confirmed that they will be able to continue service to you, even in the event of their having an incident?	No	No	Yes	No
C-3.6.10	Who is responsible for business continuity planning?	BCO (Business Continuity Officer)	Heads of departments (senior management).	Company's board of directors.	CISO
C-3.6.11	Have you performed a Business Impact Analysis (BIA)?	It is part of the BCP & RA.	Only for one specific service.	No	Not specific for CERT (but for another department).
	Summary	***Dedicated Incident Response Team and Lead. A Business Impact Analysis has been performed, the Business Continuity arrangement includes Incident Management processes and procedures, a Business Continuity Officer***	***Dedicated Incident Response Team and Lead. Crisis management team handles crises. So far, a Business Impact Analysis has been performed only for a specific service. The Business Continuity arrangement includes***	***Dedicated Incident Response Team and Lead. Business Impact Analysis has not been performed yet. Currently noBusiness Continuity arrangement including Incident Management processes and procedures. However, the***	***Dedicated Incident Response Team. A Business Impact Analysis has not been performed yet for the CERT, but for another department. There is no Business Continuity arrangement including Incident Management***

Questions for the CERT/CSIRT	Area/Section	2834	3915	6331	7924
		is responsible for the BC planning. However, the senior management and operational teams are not trained on BC.	***Incident Management processes and procedures. Heads of departments are responsible for BC planning. No specific information strategies exist, but press contacts are allowed only with approval of the CEO.***	***board of directors is responsible for BC planning, and suppliers, service and utilities providers have been consulted during the preparation of plans.***	***processes and procedures, but dedicated information strategies exist. The CISO is responsible for BC planning.***

Table A.1: Incident management questionnaire answers and summaries

In the area/section **Breaches (C-3.1)**, the overall evaluation of the responses could be assessed as green.

In the area/section **Incident Response Plan (C-3.2)**, the overall evaluation of the responses could mostly be assessed as green as well.

In the area/section **Incident Investigation (C-3.3)**, all CERTs/CSIRTs could again be evaluated as green.

In the area/section **Collecting and Storing Network Traffic Data (C-3.4)**, some significant differences occur between the CERTs/CSIRTs. One, 2834, has to be evaluated as red.

The area/section **Transferred over the Internet (C-3.5)** appeared to be not clear enough. Only two CERTs/CSIRTs have answered at all (2834 and 6331), whereas the other two (2915 and 7924) stated that the question was not understood. The answers for both 2834 and 6331 could be evaluated as yellow.

In the important area/section **Incident Management (C-3.6)**, again all summarised answers could be evaluated as yellow.

Appendix B ISO 22301 Implementation Steps Covered by S7 Framework

This appendix outlines practical implementation steps for NRENs for each area of the S7 BCM Framework, identifying the relevant ISO 22301 standards and related documents.

S7.1 Governance, Strategy and Policy	Objective: The BCM policy and strategy describe the scope and governance of BCM and give the reasons why it is being implemented and how. The main goal of the policy and strategy is to communicate to internal and external interested parties the BCM principles of the organisation and the way BCM is organised and governed.			
Control	**References**			**Recommendations**
BCM policy	ISO22301: 5.3	GPG: PP1		The BCM policy is used to communicate the NREN's BC principles to interested parties'. A lengthy policy is less likely to be read and remembered. The BCM policy should include (but i's not limited to) these elements: the organisation's definition of BC; definition of the scope of BCM; business continuity roles and responsibilities; set of principles, guidelines and minimum standards; clearly defined budget, audit and governance responsibilities.
BCM policy distribution	ISO22301: 5.3	EXP		The policy is published in an accessible location and there is a management summary to enable personnel to quickly familiarise themselves with the content of the policy.
Review of the BCM policy	ISO22301: 5.3	GPG: PP1		The BCM policy should be reviewed and, when necessary, adjusted after every form of testing and evaluation.
Review of the BCM measures	ISO22301: 9.1; 10.2			Continual improvement usually occurs within all phases and should be triggered through policy and principles, audit results, evaluation of disruptions, corrective measures and the management reviews. Changes occurring from corrective measures should be reflected in the documentation.
Review of BCM effectiveness/readiness	ISO22301: 9.1; 10.2	GPG: PP1	EXP	Similar guidelines to theprevious item: both are instances of continual improvement.

S7.1 Governance, Strategy and Policy	Objective: The BCM policy and strategy describe the scope and governance of BCM and give the reasons why it is being implemented and how. The main goal of the policy and strategy is to communicate to internal and external interested parties the BCM principles of the organisation and the way BCM is organised and governed.			
Control	**References**			**Recommendations**
BCM roles and responsibilities	ISO22301: 5.4	GPG: PP1		BCM roles have different responsibilities. Consideration should be given to the responsibilities of the following: 1. Responsible management (Board of Directors, Management Team, BC officer, risk committee). 2. Responsible operations (local management). 3. Support and advisory roles (e.g. risk & compliance departments). 4. Suppliers (vendor management). 5. Independent reviews (internal or external audit personnel/department).
Business impact analysis	ISO22301: 4.1; 6.2	GPG: PP3		Define critical products/services using the organisation's reason for existence. A good starting point is ISO22301: 4.1; 6.2 in order to answer the question: "Which products and services make us the organisation that we are?" A common mistake is not to start with critical products and services, but to think of (internal) processes. This can mean that the focus shifts and that the link with products and services is lost.
BCM in project management	EXP			Consider legal obligations for continuity in the project design phase. Incorporate tests in project planning, such as a fall-back test. Include an alternative plan in the implementation strategy in case of a disruption during the launch event.
Supply chain continuity	GPG: PP1	ISO22301: 4.1; 4.3;	ISO22318: 6.3	"Supply chain" usually refers to all providers of goods/services on which the organisation is dependent. These suppliers can include "common" goods and services such as: utilities – power, gas, oil, telecommunications; raw materials – for manufacturing; office supplies; services – security, transport, maintenance; ICT – ICT related services. Additional measures to consider: involvement of suppliers in tests and exercises; management meetings to review issues and concerns; performance evaluations; service-level agreement (SLA) flexibility to follow wide-scale disasters; legal access to records/reports on previous incidents.

S7.1 Governance, Strategy and Policy	Objective: The BCM policy and strategy describe the scope and governance of BCM and give the reasons why it is being implemented and how. The main goal of the policy and strategy is to communicate to internal and external interested parties the BCM principles of the organisation and the way BCM is organised and governed.			
Control	**References**			**Recommendations**
Monitoring and assessment of supplier services	ISO22302: 8.3; 9.3;	ISO22318: 8;	GPG: PP6	Assessing supplier services often occurs with the use of service-level reporting in the service-level agreement (SLA). Deviations from the SLA can be an early warning of problems which may lead to a disruption in the services.

Table B.1: ISO 22301 implementation steps for S7.1 Governance, Strategy and Policy

S7.2 Crisis Management and Communication	Objective: Crisis management guides and facilitates the business continuity and recovery efforts that are usually made at tactical and operational levels. Crisis communication targets all relevant internal and external stakeholders and strives to keep them informed and involved.			
Control	**References**			**Recommendations**
Crisis management organisation	GPG: PP4	EXP		Crisis management defines the way an organisation deals with a major event that threatens to damage the organisation, interested parties or the general public. This includes both events that may result in a disruption of the delivery of products and services, and events that might damage an organisation's reputation. The team involved should be small and efficient and the roles of chairman, secretary and communications advisor and their replacements need to be appointed. A process for how the crisis management team collaborates with the emergency continuity teams needs to be defined.
Notification and escalation procedure	ISO22301: 5.3	EXP	Lean BCM	Definition of what is considered crisis/disruption. Notification and escalation procedures should be different during work hours and after work. Media channels that will be used for communication within the crisis management team need to be defined (e.g. phone, sms, email, etc.). Plan for how notifications arise and which personnel can use the procedures in order to follow up on them in accordance with the incident management process.

S7.2 Crisis Management and Communication	Objective: Crisis management guides and facilitates the business continuity and recovery efforts that are usually made at tactical and operational levels. Crisis communication targets all relevant internal and external stakeholders and strives to keep them informed and involved.			
Control	**References**			**Recommendations**
				Thresholds should exist in order to escalate to a higher organisational level. These are measured based on impact and the degree of urgency that will allow the crisis management team to be informed in time to take further action if required.
Facilities for crisis management team	EXP			Dedicated facilities for the crisis management team. Standard logistics to improve the process: "war room" on- and offsite where the team works; standard office supplies (projector, flip chart, office supplies); audio/videoconference calling system; additional computers/laptops; internet access and backup internet; additional telephones and SIM cards; physical copies of documentation/policies. Part of these facilities can be shared with the emergency continuity team.
Crisis management process	ISO22302: 8.4	EXP		The crisis management process is based on these steps/procedures: 1. Impact analysis – which covers important questions in a checklist format; list of each decision that was made, with a focus on possible short-term and long-term impact; assessment of all elements of the emergency response (e.g. people, suppliers, resources & facilities, locations); also include financial and reputational consequences in the analysis. 2. Decide on action – decide which plans to invoke, which situational measures to implement. Be aware that information can often be incomplete/unavailable, so the team may need to work with assumptions. 3. Monitoring of progress, registration and reporting – decide in advance how the process and events will be recorded (timing, actions and decisions). 4. Downscaling – consider whether the temporary (emergency) solutions that have been deployed can/should become a part of the "normal" state; all temporary solutions that aren't transitioned to the "normal" state need to be undone (e.g. revoke authorisations in systems and processes, return hired resources, etc.). 5. Aftercare – this is important and cannot be overlooked in any case involving personal damages. Should start immediately after the impact analysis and should be addressed with a basic set of agreements (e.g. contacting the family of personnel).

S7.2 Crisis Management and Communication	Objective: Crisis management guides and facilitates the business continuity and recovery efforts that are usually made at tactical and operational levels. Crisis communication targets all relevant internal and external stakeholders and strives to keep them informed and involved.			
Control	**References**			**Recommendations**
Stakeholder analysis	ISO22302: 8.4	EXP		Stakeholder analysis helps an organisation to prepare the communication effort during a disruption/crisis. Important things that need consideration: internal and external stakeholders; local/social media and other crisis organisations that operate on a regional or industrial level; classification of the stakeholders based on their influence or power and their level of interest (e.g. high influence/power and high interest, high influence/power and low interest, low influence/power and high interest, low influence/power and low interest).
Crisis communication guidelines	ISO22302: 8.4			Define a crisis communication strategy, which should cover the following areas: person who communicates to the media; person who communicates to suppliers; employee reach during a disruption; best channels and tone of voice for each stakeholder; definition of overload/shortage of information being communicated; how questions on (social) media are processed; potential confidentiality of information the organisation wants to communicate externally; provision for the fact that external (social) media can sometimes reach stakeholders before the organisation does.
Crisis communication resources and media	ISO22302: 8.4			Consider media that reach the stakeholders directly instead of basing the choice on internal preferences. Prepare stakeholders. Do not hesitate to communicate to board level so they won't be taken by surprise through other channels.
Monitoring of surroundings	EXP			Responsive representation of the organisation on social media can greatly diminish reputational damage. Also, sometimes the surroundings can provide additional information in the impact analysis which makes crisis management more effective.

Table B.2: ISO 22301 implementation steps for S7.2 Crisis Management and Communication

S7.3 Emergency Continuity	Objective: Ensures the organisation can continue delivering its critical products and services during major disruptions, although this could mean the output of delivery is lower than in a normal situation. Whether this temporarily decreased level of delivery is possible at all should be analysed beforehand.			
Control	**References**			**Recommendations**
General – Emergency continuity organisation	EXP			This is connected to the organisation itself when executing the emergency continuity measures, not the crisis management team. Usually, the responsibilities of the organisation's members are similar to their existing responsibilities, but it helps to document this in a business continuity plan that clearly describes the link with the crisis management team.
General – Characteristics of critical products and services	ISO22301: 8.2; ISO22318: 5;	EXP	Lean BCM	Defines the characteristics of the critical products and services and how they are documented in order to support the impact analysis and the decision-making process on both strategic and tactical levels. This includes supporting business processes and ICT resources. The business impact analysis shows the relation between the critical products and services and the processes that deliver them. A potential risk with the business impact analysis is if it is too detailed and does not really support the objectives of BCM. In this case it takes up valuable time and resources that could be used better. Some additional aspects that need to be considered are: peak moments in the process (monthly, seasonally, etc.) where a disruption has bigger consequences; dependencies between processes and systems; dependencies on generic processes and resources (e.g. call centre, document management); deadlines from external factors such as customer contracts and regulations.
General – Recovery objectives	ISO22301: 8.2	GPG: PP3	EXP / Lean BCM	Recovery time objectives and recovery point objectives (RTOs and RPOs) determine how and which temporary measures should be prepared before a disruption occurs. They define how long a process can remain on hold and how much data can be lost before the consequences become too great. Please note: a chosen RTO is often based on a specific (monthly peak) occasion and isn't as short as on any other given occasion. Because of this criticality it should not be based on internal processes but on the importance of delivering the output to the customers.

S7.3 Emergency Continuity	Objective: Ensures the organisation can continue delivering its critical products and services during major disruptions, although this could mean the output of delivery is lower than in a normal situation. Whether this temporarily decreased level of delivery is possible at all should be analysed beforehand.			
Control	**References**			**Recommendations**
General – Business Continuity Plans	ISO22301: 8.2	GPG: PP3	EXP / Lean BCM	The goal of BCM is not only to make plans but to ensure that during a disruption the right measures are taken. Sometimes these measures are easy to identify and/or are embedded in operational procedures. But sometimes the measures to be taken are specific and unique and it is important that they are taken in the right order and the right time. An organisation should not try to write a Business Continuity Plan for a specific scenario since it might end up with a large number of plans and the disruption that eventually occurs may not (yet) be described. It is important to focus on basic scenarios around people, location, facilities, resources and suppliers. The goal of the Business Continuity Plan is to support the execution of the emergency continuity measures. The word "plan" may be confusing since sometimes it is one document and sometimes a documented set of procedures. But its goal is always to guide organisations to respond, recover, resume and restore to a predefined level of operation after a disruption.
People – Outreach	ISO22301: 8.3; 8.4	GPG: PP5	EXP	It is important to determine whether the use of private contact details is necessary and allowed. Contact information should be stored in such a way that it will still be available if the ICT infrastructure is down.
People – Arrangements for replacement	EXP			People arrangements should include additional training and certification plans for colleagues that can step in if personnel are unavailable. One easy way to train is to use holidays / holiday cover to train the temporary replacement to become familiar with the role as they take it for a few weeks and learn on the job.
Locations – Transport to alternative locations	ISO22301: 8.3	GPG: PP5		Plans for transport to and from the alternative locations should be considered for both personnel and resources within a reasonable time frame.
Locations – Teleworking	ISO22301: 8.3	EXP		Teleworking can often be implemented only with limited capacity and cannot fully replace working onsite. Because of this it should only be as a support to the activities of the critical personnel.
Resources and facilities – Availability of critical resources and facilities	ISO22301: 8.3	GPG: PP5	Lean BCM	The scope of critical resources and facilities should not be limited to ICT only. Consideration should also be given to these areas: production machines, transport vehicles, printing and scanning facilities, etc.

S7.3 Emergency Continuity	Objective: Ensures the organisation can continue delivering its critical products and services during major disruptions, although this could mean the output of delivery is lower than in a normal situation. Whether this temporarily decreased level of delivery is possible at all should be analysed beforehand.			
Control	**References**			**Recommendations**
				One preventive measure is to introduce redundancy for ICT. For emergency continuity, the rental of equipment could also be a valid option. In some cases, cooperation with competitors from the same industry also benefits all parties during a disruption.
Suppliers – Availability of critical suppliers	ISO22301: 8.3	ISO22318: 6	GPG: PP1	Consideration should be given to contracting at least two suppliers instead of one. A small stock of resources should be kept onsite when possible, with additional standby contracts that can quickly take effect.
Suppliers – Unplanned ending of services	ISO22301: 8.3	ISO22318: 6	GPG: PP1	Some common measures for unplanned ending of services include special arrangements for source code ownership, return of data in a workable format and/or separate data backups. This minimises risks such as a dependency in case of a bankrupt supplier.
Suppliers – Availability of services	ISO22301: 7.5; 8.3, 8.4	ISO22318: 6	GPG: PP1	Include an SLA in contracts and define which process is followed when the supplier suffers a disruption. This should include: escalation path, emergency numbers, contact details of both parties, etc. This process needs to be jointly developed, with periodic joint testing of its effectiveness.
Suppliers – Partnership with suppliers	EXP			Suppliers need to be seen as partners and, in the event of disruption, their input should be considered valuable.

Table B.3: ISO 22301 implementation steps for S7.3 Emergency Continuity

S7.4 Restore and Recovery	Objective: Ensures that the organisation returns to a lasting and "stable" mode of operations after a major disruption. This includes any activity related to restoring and recovering the use and performance of: people, locations, resources, suppliers, etc.			
Control	**References**			**Recommendations**
ICT restore and recovery	ISO22301: 8.4	Lean BCM		Restore and recovery plans are often limited only to the ICT domain, especially in situations where the delivery of services and products relies on information processing capacity instead of an industrial production process. ICT continuity is then more time critical and is often supported by documents such as checklists and operational procedures developed by management. Management of the restore and recovery activities is usually described in a Disaster Recovery Plan. Restore and recovery plans for people, locations and non-ICT resources are usually not made, because this plan is often dictated by the situation in hand and is less time critical.
Assessment of restore and recovery	EXP			Although the infrastructure may be restored and deemed to be working, this does not necessarily mean that it is usable. That verdict is given by the end-user organisation. The restore and recovery procedures should therefore include some acceptance criteria and instructions on how the acceptance tests are conducted.

Table B.4: ISO 22301 implementation steps for S7.4 Restore and Recovery

S7.5 Exercising and Testing	Objective: Exercising and testing is the "proof and refinement" for all BCM measures, plans, agreements and procedures that are developed by an organisation. In order to be sure that the measures are effective and can guarantee a process of continuous improvement, periodic exercising and testing are the key activities.			
Control	**References**			**Recommendations**
Planning	ISO22301: 8.5	GPG: PP6		Carrying out exercises is considered the most important activity that can increase BCM readiness. The goal is not just to check whether plans and measures work, but to assess the resilience of the organisation. Therefore, an exercise is considered a good start for a BCM initiative, even when there are no plans at that moment in time. Some of the types of exercises that can be considered are: Discussion-based exercises – considered most cost-effective and least time consuming. Tabletop exercises – these exercises use a scenario with a timeline which can run in "real time" or can include small "time jumps" to allow different phases of the scenario to be better enacted. Command-post exercises – several teams on different levels work together to manage a scenario. This can also include suppliers. Live exercises – these follow a real situation (often manually triggered) and usually involve most of the people that are affected by the situation (e.g. periodic evacuation exercise, fire exercise, etc.). Test – a unique and particular type of exercise, which has a verdict of "pass" or "fail" and is usually applied to equipment, recovery procedures or technology and not to people.
Learning strategy	ISO22301: 8.5	GPG: PP6		It is important to know that undertaking too complex an exercise does not speed up the learning curve and only creates a dislike for BCM among the participants. This is why exercises should be challenging but still linked to the maturity of the organisation with regard to BCM and allow several exercise cycles to improve the whole BCM process.
Evaluation	ISO22301: 8.5; 9.1	GPG: PP6		Evaluation is a key component and provides the opportunity for continual improvement in BCM and for the foundation. Evaluation of each exercise or test should be done within a reasonable time frame after its completion, while the impressions are still vivid.

Table B.5: ISO 22301 implementation steps for S7.5 Exercising and Testing

S7.6 Awareness and Training	Objective: Ensures that employees and contractors understand their responsibilities and are competent in the roles they have or for which they are considered backup personnel.			
Control	**References**			**Recommendations**
Awareness	BCI GPG			Organisations risk overloading personnel with information if multiple disciplines try to launch different awareness campaigns. Because of this, a combined effort with the privacy and security disciplines from other departments should be considered. Information should be kept brief and relevant, and additional reading material should be supplied for people interested in finding out more. Topics of interest could include: description of a recent exercise – scenario and lessons learned; visits to alternative locations, which might include photos; commentary on a recent disruption within the organisation or in the media, etc.
Availability of information	EXP			The BCM documentation should not be kept secret. The more access people have, the more they will be aware of what measures are already in place.
BCM role requirements	ISO22301: 7.2			Every employee who has an active role in the BCM organisation should possess and develp skills such as: stress management; decisiveness; conflict management; basic communication mechanisms; focus. Additional and specialised training should be considered in order to develop these personal skills. The results of exercises and tests give a good indication as to whether someone needs training.
Training	EXP			Regular training on different subjects is key to improving the team's capabilities.

Table B.6: ISO 22301 implementation steps for S7.6 Awareness and Training

S7.7 Foundation	Objective: Making sure that major disruptions do not occur and that the impact is manageable and safeguarded by professionalism in each department.			
Control	**References**			**Recommendations**
People – Critical personnel	ISO22301: 8.3	EXP		Limit critical personnel initially to the roles required to perform the critical business processes only, but do not forget to include people who have specific knowledge without assigning them to a critical business process.
Facilities – Critical resources and facilities	ISO22301: 8.3	EXP		Limit access to critical resources and facilities only to the roles required for the critical business processes.
Facilities – Arrangements for critical locations	ISO22301: 8.3	GPG: PP5	Lean BCM	If the alternative location requires particular specifications that can be difficult to find, consider making arrangements with a third party, even with a competitor, who shares those requirement specifications for their own facilities.
Facilities – Emergency response organisation	ISO22301: 8.4	GPG: Intro		The emergency response organisation and crisis management team should be fully aware of each other's activities and try to achieve a synergy in their efforts to manage the disruption. The goal of the emergency response organisation is the safety of people while the goal of the crisis management team is to deal with the organisation as a whole.
Operations – Preventive measures following the business impact analysis	EXP			Close connection with the business impact analysis.
Operations – Documented operating procedures	ISO27002: 12.1	GÉANT Security Baseline		The operational departments have documented their most important procedures; these should provide a useful basis for BCM measures and plans. The fact that the procedures exist and can be invoked makes the continuity plans more exact.
ICT – Change management	ISO27002: 12.1	GÉANT Security Baseline		Change management is crucial for better operations procedures and should be implemented for all services.
ICT – Information backup	ISO27002: 12.2; 12.3	GÉANT Security Baseline		Complete and accurate records should be produced of the backup copies made and documented restoration procedures. The difference between full or differential backups, and the frequency of backups, should reflect the business requirements and the security requirements of the information involved and the criticality of the information for continued operation of the organisation.
ICT – Management of technical vulnerabilities	ISO27002: 12.6	GÉANT Security Baseline		A procedure for management of technical vulnerabilites should exist and be perfomed.

S7.7 Foundation	Objective: Making sure that major disruptions do not occur and that the impact is manageable and safeguarded by professionalism in each department.			
Control	**References**			**Recommendations**
ICT – Assessment of and decision on information security events	ISO27002: 16.1	GÉANT Security Baseline		A possible relation between an information security event and a disruption of the business should be identified as soon as possible. In reality, this can easily be overlooked, which then leads to a lack of escalation in the IT department. Management should be informed as soon as possible in order to enable them to determine whether there are also consequences for business continuity.
ICT – Response to information security incidents	ISO27002: 16.1	GÉANT Security Baseline		Information security incidents should have their own procedures, which need to be aligned with general BCM, especially since these incidents can have an impact on business continuity.
Procurement & supplier management – Critical suppliers	ISO22301: 8.3	ISO22318: 5	GPG: PP3	Critical suppliers are defined as those essential for the organisation's critical products and services or for general continuity (electricity, water, etc.) and can also include relatively small suppliers.
Procurement & supplier management – Managing changes to supplier services	ISO22301: 8.2; 9.1	ISO22318: 6	GPG: PP3	The BCM role should be involved in changes to supplier services in order to assess the specific impact on business continuity when services change and whether an update to BCM is required.
Procurement & supplier management – Controlled ending of services	ISO22318:6	GPG: PP1	EXP	Different service exit strategies may seem unclear during contract negotiations, but should always be well defined before a contractual agreement is signed and should also define how data portability is managed and achieved.

Table B.7: ISO 22301 implementation steps for S7.7 Foundation

Appendix C Questionnaire for Evaluating the BCM Approach

This appendix contains the questionnaire (including the introduction) sent to selected NRENs to find out their process priorities and identifiy any common processes, to support the Business Impact Analysis (BIA) element of the S7 BCM Framework. NRENs were also asked about GÉANT Security Baseline assessment, and about their participation and member status in Trusted Introducer.

C.1 Introduction

Following the lean approach, based on the complexity and different needs of NRENs, it is very important to select a set of topics that are recommended as a starting point in BCM.

Based on previous experience, we propose the following subset of topics to be considered first for the lean approach to BIA. Furthermore, we propose a mapping of the topics based on the GÉANT Security Baseline level.

The initial set of topics which we deem relevant to NRENs is given below:

- Foundation – PEOPLE.
- Training and awareness.
- Emergency continuity.
- Exercising and testing.
- Crisis management and communication.
- Foundation – ICT.
- Foundation – FACILITIES.

We correlate their importance to the GÉANT Security Baseline level in order to allow NRENs to focus on those areas that will help them to achieve the next level. This process follows the lean approach, based on shorter repetitive cycles which are easy to finish and see their results.

Topic	GÉANT Security Baseline NREN Level		
	Baseline	Advanced	Expert
Foundation – PEOPLE	YES	YES	YES
Foundation – ICT	YES	YES	YES
Foundation – FACILITIES	NO	YES	YES
Crisis management and communication	NO	YES	YES
Emergency continuity	NO	NO	YES
Training and awareness	YES	YES	YES

Topic	GÉANT Security Baseline NREN Level		
	Baseline	Advanced	Expert
Exercising and testing	NO	NO	YES
Governance, strategy and policy	NO	NO	YES
Restore and recovery	NO	YES	YES

C.2 Questionnaire

In order to understand the requirements for the BCM from the perspective of the NREN, we would like to receive your input. Based on your input and requirements, a recommendation will be compiled to help the GÉANT community better understand the BCM process and successfully implement it.

(this needs to receive feedback from 12+ NRENS)

NREN Name				
GÉANT Security Baseline Level	Not performed	Baseline	Advanced	Expert
Trusted Introducer Category (for CIRT/CERT)	None	Listed	Accredited	Certified
List of topics, by order of importance for your NREN				
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
	(feel free to list more topics)			
Suggestions and open comments				

Appendix D GÉANT Security Baseline and BCM S7 Framework

Table D.1 below shows which NREN Organisational (NO) areas of the GÉANT Security Baseline for NRENs are covered by the S7 BCM Framework, or which of the categories correlate in each case. The table is followed by a brief commentary on the correlation.

GÉANT Security Baseline for NRENs		BCM S7 Framework
NO1	**Policy and Leadership**	
NO1.1	Management Commitment and Mandate	Governance, Strategy and Policy [3.1]
NO1.2	Internal Security Policy	Governance, Strategy and Policy [3.1]
NO1.3	Acceptable Use Policy	
NO1.4	Regulatory and Privacy	
NO2	**People**	
NO2.1	Training and Awareness	Awareness and Training [3.6]
NO2.2	Personnel Management	Emergency Continuity [3.3] (3.5, 3.6)
NO2.3	Supplier Management	Governance, Strategy and Policy [3.1] (1.9, 1.10), Emergency Continuity [3.3] (3.10 – 3.13), Foundation [3.7] (7.12 – 7.14)
NO3	**Threats**	
NO3.1	Risk Management	Foundation [3.7] (7.1 – 7.5)
NO3.2	Incident Management	Crisis Management and Communication [3.2], Foundation [3.7] (7.10, 7.11)
NO3.3	Business Continuity Management	Emergency Continuity [3.3] (3.1 – 3.4), Restore and Recovery [3.4]
NO4	**Operations**	Foundation [3.7] (7.5 – 7.11)
NO4.1	Tools	
NO4.2	Cryptography	
NO4.3	Access Management	
NO4.4	Patch Management	
NO4.5	Vulnerability Management	Foundation [3.7] (7.9)

Table D.1: GÉANT Security Baseline mapped to S7 Framework

NO1: Policy and Leadership basically correlates to the BCM S7 Framework category Governance, Strategy and Policy [3.1]. While the GÉANT Security Baseline is primarily concerned with information security, security policy and data protection at this point, in order to actually implement them similar criteria must be met as for effective BCM.

NO2: People contains the BCM S7 Framework category Awareness and Training [3.6]. In addition, NO2.2 Personnel Management is considered in the BCM Framework under Emergency Continuity [3.3] (3.5, 3.6) and NO2.3 Supplier Management is considered in the BCM Framework under Governance, Strategy and Policy [3.1] (1.9, 1.10), Emergency Continuity [3.3] (3.10 – 3.13), and Foundation [3.7] (7.12 – 7.14).

NO3: Threats deals with Risk Management, Incident Management and Business Continuity Management. Risk Management with regard to people, facilities and operations is considered in the BCM Framework under Foundation [3.7] (7.1 – 7.5). The latter two different but closely related areas are considered in the BCM Framework under Crisis Management and Communication [3.2] and Foundation [3.7] (7.10, 7.11), and under Emergency Continuity [3.3] (3.1 – 3.4) and Restore and Recovery [3.4], respectively.

NO4: Operations consists of a set of 5 different sub-areas, all of which are preventive in nature in terms of Business Continuity Management. These are also essentially dealt with in the BCM Framework under Foundation [3.7] (7.5 – 7.11). Vulnerability management is considered in particular under item [3.7] (7.9).

Appendix E Trusted Introducer Services and BCM S7 Framework

Table E.1 below shows which areas of the Security Incident Management Maturity Model (SIM3) are covered by the BCM S7 Framework, or which of the categories correlate in each case.

SIM3: Security Incident Management Maturity Model		BCM S7 Framework
O –"Organisation" Parameters		
O-1	MANDATE	Governance, Strategy and Policy [3.1]
O-2	CONSTITUENCY	Governance, Strategy and Policy [3.1]
O-3	AUTHORITY	Governance, Strategy and Policy [3.1]
O-4	RESPONSIBILITY	Governance, Strategy and Policy [3.1]
O-5	SERVICE DESCRIPTION	
O-6	(intentionally left blank – not included in "scoring")	
O-7	SERVICE LEVEL DESCRIPTION	
O-8	INCIDENT CLASSIFICATION	Foundation [3.7] (7.10)
O-9	INTEGRATION IN EXISTING CSIRT SYSTEMS	
O-10	ORGANISATIONAL FRAMEWORK	
O-11	SECURITY POLICY	Governance, Strategy and Policy [3.1]
H –"Human" Parameters		
H-1	CODE OF CONDUCT/PRACTICE/ETHICS	
H-2	PERSONAL RESILIENCE	Emergency Continuity [3.3] (3.6), Foundation [3.7] (7.1)
H-3	SKILL SET DESCRIPTION	
H-4	INTERNAL TRAINING	Awareness and Training [3.6]
H-5	EXTERNAL TECHNICAL TRAINING	Awareness and Training [3.6]
H-6	EXTERNAL COMMUNICATION TRAINING	
H-7	EXTERNAL NETWORKING	

SIM3: Security Incident Management Maturity Model		BCM S7 Framework
T –"Tools" Parameters		
T-1	IT RESOURCES LIST	Emergency Continuity [3.3], Foundation [3.7]
T-2	INFORMATION SOURCES LIST	Emergency Continuity [3.3], Foundation [3.7]
T-3	CONSOLIDATED EMAIL SYSTEM	
T-4	INCIDENT TRACKING SYSTEM	Foundation [3.7] (7.11)
T-5	RESILIENT PHONE	Emergency Continuity [3.3] (3.9, 3.10), Foundation [3.7] (7.2, 7.3, 7.12)
T-6	RESILIENT E-MAIL	Emergency Continuity [3.3] (3.9, 3.10), Foundation [3.7] (7.2, 7.3, 7.12)
T-7	RESILIENT INTERNET ACCESS	Emergency Continuity [3.3] (3.9, 3.10), Foundation [3.7] (7.2, 7.3, 7.12)
T-8	INCIDENT PREVENTION TOOL SET	Foundation [3.7]
T-9	INCIDENT DETECTION TOOL SET	Foundation [3.7]
T-10	INCIDENT RESOLUTION TOOL SET	Foundation [3.7]
P –"Processes" Parameters		
P-1	ESCALATION TO GOVERNANCE LEVEL	Crisis Management and Communication [3.2] (2.2)
P-2	ESCALATION TO PRESS FUNCTION	Crisis Management and Communication [3.2] (2.2)
P-3	ESCALATION TO LEGAL FUNCTION	Crisis Management and Communication [3.2] (2.2)
P-4	INCIDENT PREVENTION PROCESS	Crisis Management and Communication [3.2] (2.4)
P-5	INCIDENT DETECTION PROCESS	Crisis Management and Communication [3.2] (2.4)
P-6	INCIDENT RESOLUTION PROCESS	Crisis Management and Communication [3.2] (2.4)
P-7	SPECIFIC INCIDENT PROCESSES	
P-8	AUDIT/FEEDBACK PROCESS	Exercising and Testing [3.3]
P-9	EMERGENCY REACHABILITY PROCESS	Emergency Continuity [3.3] (3.1)
P-10	BEST PRACTICE EMAIL AND WEB PRESENCE	
P-11	SECURE INFORMATION HANDLING PROCESS	
P-12	INFORMATION SOURCES PROCESS	Foundation [3.7] (7.8)
P-13	OUTREACH PROCESS	Crisis Management and Communication [3.2] Emergency Continuity [3.3]

SIM3: Security Incident Management Maturity Model		BCM S7 Framework
P-14	REPORTING PROCESS	Crisis Management and Communication [3.2], Emergency Continuity [3.3]
P-15	STATISTICS PROCESS	
P-16	MEETING PROCESS	
P-17	PEER-TO-PEER PROCESS	

Table E.1: SIM3 mapped to S7 Framework

References

[2003/361/EC] European Commission, Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361. Accessed 12.01.2021.

[Balboni] L. M. Simone Balboni, "Business and IT Continuity: Overview and Implementation Principles," European Network and information Security Agency (ENISA), 2008.

[Bergland] C. Bergland, "How Does Anxiety Short Circuit the Decision-Making Process?," 17 03 2016. [Online]. Available: https://www.psychologytoday.com/us/blog/the-athletes-way/201603/how-does-anxiety-short-circuit-the-decision-making-process.

[CMSAT] CSIRT Maturity – Self-assessment Tool, 13.01.2021 [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

[Compendium] GÉANT Compendium, "NREN service portfolios," 09 10 2020. [Online]. Available: https://compendiumdatabase.geant.org/reports/nrens_services.

[Crispim] José Crispim, Luiz Henrique Silva, and Nazaré Rego. "Project risk management practices: the organizational maturity influence." International journal of managing projects in business (2019).

[D8.2] GÉANT Security Baseline for NRENs, 28.12.2020 [Online]. Available: https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D8-2_Security-Baseline-for-NRENs.pdf

[FBC] Monica de Wit & Sanja Bankras, Framework Business Continuity 2017, Verdonck, Klooster & Associates, 2017 https://wiki.surfnet.nl/download/attachments/11062812/Framework%20Business%20Continuity%20SURF%202017%20v1.0.pdf?version=1&modificationDate=1513262682155&api=v2

[Gibb] Forbes Gibb and Steven Buchanan. 2006. "A Framework for Business Continuity Management." International Journal of Information Management 26(2):128–41. doi: 10.1016/j.ijinfomgt.2005.11.008.

[Gratt] L. B. Gratt. 1989. The Definition of Risk and Associated Terminology for Risk Analysis. In: Bonin J.J., Stevenson D.E. (eds) Risk Assessment in Setting National Priorities. Advances in Risk Analysis, vol 7. Springer, Boston, MA. https://doi.org/10.1007/978-1-4684-5682-0_73

[Haghighi] S. Motevali Haghighi and S. Ali Torabi. 2020. "Business Continuity-Inspired Fuzzy Risk Assessment Framework for Hospital Information Systems." Enterprise Information Systems 14(7):1027–60. doi: 10.1080/17517575.2019.1686657.

[ISO 22301] ISO, “22301 Societal security — Business continuity management systems — Requirements,” International Organisation for Standardisation, Geneva, 2012.

[ISO 22313:2020] ISO 22313:2020. Security and resilience — Business continuity management systems – Guidance on the use of ISO 22301. https://www.iso.org/obp/ui/es/#iso:std:iso:22313:ed-2:v1:en; https://www.iso.org/standard/75107.html

[Järveläinen] Jonna Järveläinen. 2013. “IT Incidents and Business Impacts: Validating a Framework for Continuity Management in Information Systems.” International Journal of Information Management 33(3):583–90. doi: 10.1016/j.ijinfomgt.2013.03.001.

[Kazakova] N. A. Kazakova, M. P. Bobkova and A. E. Sivkova. 2020. “Evaluation and Prediction of the Business Continuity Risks.” in Proceedings of the International Scientific Conference “Far East Con” (ISCFEC 2020). Vladivostok, Russia: Atlantis Press.

[Mather] M. Mather, “Stress Changes How People Make Decisions,” 27 02 2012. [Online]. Available: https://www.psychologicalscience.org/news/releases/stress-changes-how-people-make-decisions.html.

[Monahan] Brendan Monahan, “For Business Continuity, Accept the Unexpected”, Security Management, August 2019, https://www.asisonline.org/security-management-magazine/articles/2019/08/for-business-continuity-accept-the-unexpected/

[NIST-SP800-30] Gary Stoneburner, Alice Goguen and Alexis Feringa. “NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems,” Falls Church, 2002.

[NIST-SP800-34] National Institute of Standards and Technology , “NIST Special Publication 800-34 Contingency Planning Guide for Federal Information Systems,” National Institute of Standards and Technology , Gaithersburg, 2010.

[Păunescu] C. Păunescu, M. C. Popescu and L. Blid. Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions. Management & Marketing. Challenges for the Knowledge Society. 2018 Sep 1;13(3):1035-50.

[Prabhu] Lean business continuity management, 01.11.2020 [Online]. Available: https://www.linkedin.com/pulse/lean-business-continuity-management-keith-prabhu

[Saeidi] Parvaneh Saeidi et al. “The impact of enterprise risk management on competitive advantage by moderating role of information technology.” Computer Standards & Interfaces 63 (2019): 67-82.

[Sawalha] Ihab Hanna Sawalha. “Business continuity management: use and approach’s effectiveness.” Continuity & Resilience Review (2020).

[SIG-ISM_WP] SIG-ISM White Paper on risk management, 01.11.2020 [Online]. Available: https://wiki.geant.org/display/SIGISM/SIG+ISM+white+paper+risk+management?preview=/121343255/121343802/SIG-ISM-White-paper-Risk%20Assessment%20Sept%202016.pdf

[Snedaker] Susan Snedaker, Business Continuity and Disaster Recovery Planning for IT Professionals, April 2011, Syngress

[Stikvoort] Don Stikvoort, 30 March 2015: SIM3 : Security Incident Management Maturity Model, 28.12.2020 [Online]. Available: https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

[Supriadi] L. S. R. Supriadi, L. Sui Pheng. (2018) Business Continuity Management (BCM). In: Business Continuity Management in Construction. Management in the Built Environment. Springer, Singapore. https://doi.org/10.1007/978-981-10-5487-7_3

[Suresh] Nallan C. Suresh, George Lawrence Sanders and Michael J. Braunscheidel. 2020. "Business Continuity Management for Supply Chains Facing Catastrophic Events." IEEE Engineering Management Review 48(3):129–38. doi: 10.1109/EMR.2020.3005506.

[TI] Trusted Introducer Services, 01.11.2020 [Online]. Available: https://www.trusted-introducer.org/services/overview.html

[TI_Standards] Trusted Introducer: De-Facto Standards for CSIRTs, PSIRTs and other security teams, 28.12.2020 [Online]. Available: https://www.trusted-introducer.org/processes/standards.html

[Torabi] S. A. Torabi, H. Rezaei Soufi and Navid Sahebjamnia. 2014. "A New Framework for Business Impact Analysis in Business Continuity Management (with a Case Study)." Safety Science 68:309–23. doi: 10.1016/j.ssci.2014.04.017.

Glossary

BAU	Business as usual
BC	Business Continuity
BCM	Business Continuity Management
BCO	Business Continuity Officer
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DPM	Data Protection Management
ENISA	European Union Agency for Cybersecurity
ERM	Enterprise Risk Management
EXP	Expert (GÉANT Security Baseline level)
GDPR	General Data Protection Regulation
GPG	Good Practice Guidelines
GPG PP1	GPG Policy and Programme Management
GPG PP3	GPG Analysis
GPG PP4	GPG Design
GPG PP5	GPG Implementation
GPG PP6	GPG Validation
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IM	Incident Management
IPM	Intrusion Prevention System
IRM	Incident Response Management
IRT	Incident Response Team
ISO	International Organistion for Standardisation
MADM	Multi-Attribute Decision-Making
NO	NREN Organisational
NOC	Network Operations Centre
NREN	National Research and Education Network
PDB	Personal Data Breach
PDBM	Personal Data Breach Management
PKI	Public Key Infrastructure

PSIRT	Product Security Incident Response Team
R&E	Research and Education
RA	Risk Assessment
RM	Risk Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SIG	Special Interest Group
SIG-ISM	Special Interest Group on Information Security Management
SIM3	Security Incident Management Maturity Model
SLA	Service-Level Agreement
TF	Task Force
TF-CSIRT	Task Force on Computer Security Incident Response Teams
TI	Trusted Introducer
WP	Work Package
WP8	Work Package 8, Security
WP8 T1	WP8 Team 1 Business Continuity