Integrated cyber-physical security for health services

Updated Quality Plan Deliverable 2.5

Lead Author: EOS

Contributors: All Partners

Deliverable classification: (PU)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	*D2.5 updated Quality Plan*
Prepared By	*Elodie Reuge*
Approved By	*Ludivine Blanchet*
Version Number	*V0.1*
Contact	Elodie.reuge@eos-eu.com

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
V0.1	23/04/2019	1st draft	ER	ER
V0.2	24/04/2019	EOS internal review	JP	JP
V0.3	24/04/2019	KUL internal review	EB	EB
V0.4	25/04/2019	ISEP internal review	IP	IP
V0.5	29/04/2019	APHM internal review	LB	LB
V0.6	30/04/2019	EOS integration of comments	ER	ER
V1	30/04/2019	EOS Final version	ER	ER

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Contents

List of Figures

List of Tables

List of Acronyms	
AB	Advisory Board
EAB	Ethics Advisory Board
CA	Consortium Agreement
D&C	Dissemination and Communication
DL	Deliverable Leader
DoA	Description of Action
GA	Grant Agreement
KPIs	Key Performance Indicators
QM	Quality Manager
SAB	Security Advisory Board
SO	Security Officer
WP	Work package

Table 1 - List of Acronyms

The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that rapidly increased in magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well weapons to impact the population. As Europeans, we know now that we must increase our awareness of these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers.

Threats cannot be analyzed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones. They are widely reliant on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability.

The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

Introduction

This Deliverable focuses on updating the rules and guidelines, assuring the quality of the SAFECARE deliverables as well as the material produced by the project and disseminated to the external stakeholders. Specifically, in the first section, the Consortium presents the updated "Quality Management" concept as well as how it has been implemented so far and the way it will be implemented for the rest of the project. Additionally, 2.5 focuses on the targets which have been reached and the material used until now.

The second section presents how the responsibilities initially described per partner type have been put into place and how to better refine them if needed. Since SAFECARE is comprised of 21 partners with different roles within the project, all parties are involved in the quality assurance process but in different ways. It is also explained in this process how the Security Officer (SO), Security Advisory Board (SAB) and Ethics Advisory Board (EAB) are also involved in the process.

Thereafter, the following section is divided into two linked processes, explaining how the deliverables and the dissemination material quality management process have so far been implemented. Here, the Consortium presents in detail the process followed for the whole life cycle of the project to assure maximum quality. The last part of this deliverable analyses whether the Key Performance Indicators (KPIs) have been reached yet and/or need to be readjusted.

Deliverable 2.5

Within this deliverable, the Consortium analyses the specific guidelines described in the Initial Quality Plan.

The most important aspect of this document is the analysis of the initial Key Performance Indicators (KPIs) and their adjustment. These indicators have a scale starting from satisfactory to non-satisfactory and do not only include requirements for the authors of documents, but also question for the internal reviewing process of SAFECARE.

This document receives, amongst others, inputs from:

- The SAFECARE Grant Agreement (GA)[1]
- EU Grants: H2020 AGA — Annotated Model Grant Agreement – ARTICLE 19 – Submission of Deliverables
- Deliverables related to Data Protection and Privacy
- The first 8 months of the project

[1] It has to be added that the Consortium is currently working on an addendum (the draft version has already been sent to the PO).

Quality Management

The past 8 months have shown that the quality management principles are still considered vital for the production and validation of project outcomes and dissemination material. With the Consortium being composed of 21 partners, it has been proven that strict quality management principles are crucial for the smooth implementation of SAFECARE. For the Project to achieve appropriate quality in the deliverables submission, SAFECARE has introduced certain standards which have been followed by the entire Consortium and have been measured against the quality KPI's.

Quality Targets

The metrics used for the quality identification of SAFECARE material and outputs is qualitative, and recorded as either "yes" or "no", the former presenting the acceptability of the KPI and the latter the need for improvement. If no, then the author is required to make the required changes:

Key roles and responsibilities. This process thus aims to achieve:

- The high quality outputs as the Consortium assumed in detail in the DoA;
- The creation of a homogeneous internal approach embracing consistency through the project;
- The showcase of SAFECARE to external stakeholders in a consolidated manner and with common messages;
- The assurance of the delivery of the project outputs in a timely manner.

Key roles and responsibilities

For the purposes of this quality management process in this section the Consortium are presenting the role of each partner in addition to the roles of the different Advisory Boards (AB). As it is crucial that Consortium partners clearly understand their role in the process and embrace the responsibility from the beginning of SAFECARE, the table below has been strictly followed. Mitigation risks are also presented in the Section *Quality Risks and Mitigation Actions*.

Type of partner	Role	Reports to
Project coordinator: APHM	Final recipient of Deliverables: The project coordinator receives all relevant material from the Quality Manager (QM) for final submission to the EC. The Coordinator makes the final adjustments, if necessary, to the text and material produced by the Consortium partners.	European Commission
Quality Manager (QM): EOS	Intermediary recipient of Deliverables: The QM creates the delivery process with the contribution of all partners. The QM assures the implementation of this process and report to the Coordinators should delays in delivery occur. Additionally, the QM is the only partner that is allowed to review all RESTREINT UE deliverables before their final submission.	Project Coordinator, technical coordinator and scientific coordinator
Project Security Officer (PSO)	The party submits all RESTREINT UE deliverables to the EC: The PSO will inspect all the deliverables that are security sensitive and give inputs to the Consortium if further amendments or additions to the text are needed.	Independent to the Consortium

	Any presentation given to the public and based on content has to be inspected by the PSO in case of sensitive and classified information.	
Security Advisory Board (SAB)	Provides suggestions to the Consortium regarding deliverables related to security. The SAB provides input related to classified material as well as security issues being / have been raised during the project.	Independent
Ethics Advisory Board (EAB)	Provides suggestions to the Consortium regarding deliverables related to ethics: The EAB provides input related to deliverables including ethical components and issues being raised during the project.	Independent
WP leaders	The leaders of the SAFECARE 8 WPs are responsible for: - Consistency within their WP; - Definition of a 6 month work plan to align outputs of their WPs with others; - Regular updates to and transparency with the WP partners; - Timely Delivery of results within the WP; - Communication delays and re-adaptation of the work plan; - Participation in the WP leader conference calls and meetings	Project Coordinator

	and provision of regular updates to the Project coordinator and to the other WP leaders.	
Task leaders	The SAFECARE Task Leaders are responsible for: - Successful implementation of their Tasks; - Coordination and communication amongst contributing Tasks partners; - Successful delivery of Task objectives; - Provision of regular updates to WP leaders.	WP leaders Project Coordinator
Deliverable leader	The SAFECARE Deliverable leaders are responsible for: - Successful and timely delivery of their reports; - Coordination of deliverable contributors and internal assignment of contributions; - Creation of a 6 month timeline to ensure timely submission; - Delivery of the document for review to the internal reviewers and the QM; - Assignment of further contributions, if necessary, after the internal reviewers report;	Task leader WP leader Project Coordinator Quality Manager

	- Inform the Project Coordinator and the QM in case of possible delays the earliest possible; - Inform the Project Coordinator and QM about underperforming partners (as defined with the CA).	

Table 2 – Partner Responsibilities

The roles, as defined in the table, have proven their efficiency during the first 8 months and no change of process is needed.

Quality Management for Deliverables

In this section the process from the drafting to the delivery of written outputs and other material is described in detail. The roles described in the Key Roles and Responsibilities Section are interlinked and their responsibilities are explained further.

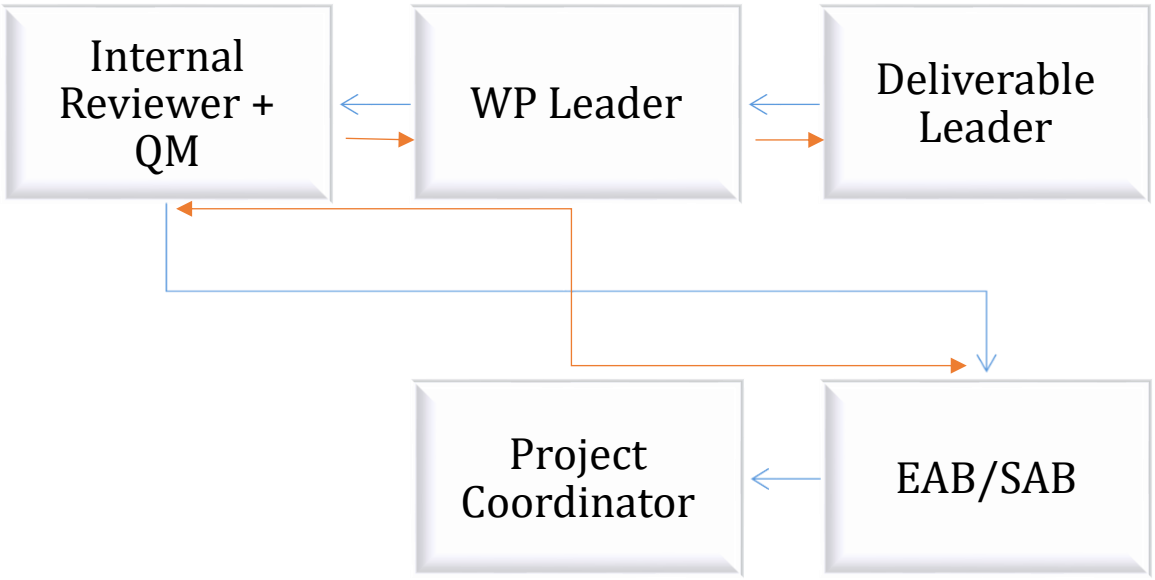


Figure 1 - Quality Management Process

The process starts with the **Deliverable Leader** (who is the partner that is the main author of the deliverable), who - as mentioned - has the responsibility to assign contributors, create a timeline for an on-time submission and communicate any difficulties faced during the writing process to the Project Coordinator and the Quality Manager. The Deliverable Leader has a delivery date specified in the Description of Action (DoA) which must absolutely be met. That deadline is the starting point for planning the actions to achieve the deliverable objectives that

have to happen in conjunction with the **WP leader** to avoid miscommunication and duplication of work within the WP.

The Deliverable Leader has to send the outline of the deliverable to the **Internal Reviewers and the QM**, 25 days before submission. 10 days before the official submission of the deliverable, the Deliverable Leader must send a full draft to the Internal Reviewers and to the Quality Manager. In the case that the deliverable contains ethics or security issues, the deliverable has to be sent to the Internal Reviewers and to the Quality Manager, 30 days and 14 days before submission respectively.

The Internal Reviewers and the Quality Manager have 7 and 5 days respectively to provide the authors with a Deliverable Review Sheet (DRS), which is provided by the Quality Manager. A copy of this template is located in Annex 2 –. Depending on the comments/feedback received the author has 3 days to implement the changes and submit a final version to the **Quality Manager and to the Project Coordinator** for final checks.

Quality management for External Material and Dissemination

Due to the sensitive nature of SAFECARE, the Consortium has decided to implement a standard approach to Dissemination and Communication material, including key messages. This has been thoroughly explained in D8.1 Dissemination and Communication Strategy (D&C), submitted at M3. The D&C lead and the QM are from the same organisation, EOS, which monitors the compliance to the quality standards set in this document, but also in WP8, Dissemination, exploitation and standardization.

According to the DoA, partners organize events that assure SAFECARE exploitation (Focus Groups, Awareness and commercial events), but also attend different scientific, technical and policy activities. For this purpose, SAFECARE required a common, reliable and exploitable brand. To achieve such a brand representation, materials that are produced for these types of activity have to follow specific criteria.

Except from the templates which have been produced by the QM, in terms of Deliverables and Presentations, the WP8 lead created flyers, roll-ups and eventually the website to compliment these activities. Further to that, the impact of these activities is measured by the WP8 lead and, depending on the results, the partners have received further material, if deemed necessary. The reasons for concentrating the production of such material is to ensure the consistency.

Additionally, all workshop invitations, data protection and management of participant information are managed by WP8, and always with the guidance of KUL. This allows the consortium to follow a standard process for activities involving external stakeholders in terms of messaging, and also handling of personal information.[2]

[2] The Awareness Event will take place on the 18th September 2019. As it will be the first workshop open to external stakeholders, the consortium is currently establishing the standard process to use, with the guidance of KUL and in respect with the GDPR.

The SAFECARE lexicon

To achieve a consolidated vision throughout the Consortium and establish a brand, the creation of the lexicon of common language and definitions used in the area of healthcare has been identified as crucial for the project. Partners have been called upon to propose common definitions used in their stakeholder groups and after consulting with the Management Team, SAFECARE presents a list. The SAFECARE Lexicon that has been developed can be found in Annex 1.

Key Performance Indicators (KPIs)

The KPIs related to deliverables within SAFECARE are separated into two categories: a) Format Review and b) Content Review. The format review contains the editing, phrasing and structure of the document as well as its adaptation to the template. The Content Review is the content style of the document, writing style, coherence, methodology and factual components. After 8 months of using the above mentioned methodology, its efficiency has been proven.

Format review – What should exist in the document	Yes Completely Agree	Agree	Partially Agree	No Disagree	**N/A**	**Comments**
Deliverable number and title on the front page and on the header.						
Grant Agreement number						
Lead Beneficiary (and the people involved) and Contributing Beneficiaries (and people involved)?						
Dissemination level						
Release history table						
Table of contents						
List of tables						
List of figures						
List of acronyms						
Executive Summary						
Introduction						
Conclusion						
Appropriate font: - Cambria, 11pt for the core text - Cambria, 10pt for the footnotes						

Paragraph space (1.15 between the lines)						

Table 3 - Key Performance Indicators

Content review	Yes Completely Agree	Agree	Partially Agree	No Disagree	N/A	Comments
Is the content presented clear and consistent?						
Is the Executive Summary self-contained and includes the main ideas of the document?						
Does the introduction make clear what is the purpose, structure and presents some main results?						
Is the conclusion different from the executive summary and the introduction?						
Does the Conclusion present key results?						
Does the content of the document match the description in the DoA?						
Is the document complete?						
Is there any superfluous or unnecessary content in this document?						
Are all references in the document included in the						

references section?						
Is the document clearly understood and well written?						

Table 4 - Content Key Performance Indicators

Quality Risks and Mitigation Actions

This section reflects the same content that the "common" issues already underlined by the Consortium in D2.4. It has been decided not to change the list below as SAFECARE has not faced one of the issues described, or any other. The mitigations foreseen to be used in case of trouble are still accurate.

1. Underperforming partners

Issue:
In many occasions in EU funded projects, it has been observed that some partners may not perform as indicated in the DoA. This will result in delays to submission of the specific documents and internal conflicts. SAFECARE is a consortium of 21 partners with multiple nationalities, expertise and cultures, thus, differences in operational capacity between the partners are expected.

Mitigations:
- It is expected that the processes are explained as clearly as possible, partners are encouraged to ask questions or mention issues with those specific processes from the beginning of the project, and for its efficient continuation.
- WP Leaders are encouraged to inform the Coordinator if such behavior is beginning to affect project outcomes. The Project Coordinator together with the Management Board will make an informed decision about the specific partner and inform their upper management if such behavior continues.

2. Deliverable submission delays

Issue:
Each deliverable mentioned within the DoA has a specific deadline. The QM has established a timeline for timely submission which partners are encouraged to follow. If this is not the case deliverables will start being delayed globally due to the fact that SAFECARE's deliverables, in most cases, are cascading deliverables. Most deliverables are based on the previous one.

Mitigations:
- The Task or Deliverable leaders are responsible to contact the Project Coordinator and Quality Manager when these issues occur. Once the two parties have been informed, they will contact the relevant partners to understand what the situation is in detail. Actions will be taken thereafter in the Management Board.
- Meanwhile the QM will identify other partners that could potentially replace the initial contribution. If the QM anticipates a delay in submission, the Project Coordinator will be informed and he will be in a position to contact the PO.

3. Lack of quality in deliverables

Issue:
Low quality deliverables in content and in writing are reasons for rejection of the deliverable by the PO, but also discourages the brand name SAFECARE is trying to establish. The quality of the deliverable whether in content or in writing is the responsibility of the Deliverable Leader.

Mitigations:
- It has been specified during the kick-off meeting that the QM and Internal Reviewers will not be a revision mechanism for any deliverable, editing the content is the responsibility of the partner leading the drafting of such report.
- The suggestions and feedback of the QM and the Internal Reviewers is not compulsory, but it is advisable. The Internal Reviewers or the QM should not change the meaning of the text they are reviewing, but only make comments and small adjustments.
- Every partner responsible for a deliverable is obliged to undertake an internal editing of the text before sending the document to the QM and the Internal Reviewers.

4. WP Objectives are not met holistically

Issue:
Due to the cascading component in SAFECARE, in the case that one WP cannot complete or partially-achieve its objectives, this will cause an issue throughout the project. Delays will occur, and low-quality results will be produced.

Mitigations:
- In this case the WP leader has to inform the Management Board. In these circumstances the Management Board will discuss amendments and actions to consider in order to achieve the WP objectives.

5. Objectives and intended results per task and their benefit for the overall project are not clear

Issue:
In the proposal, objectives were mentioned, both technical and societal. These objectives were a planning of how the Consortium sees the topic it was applying for. Implementation of such actions can bring up some challenges not anticipated in the proposal phase. One re-occurring issue is the interlinkages between WPs and Tasks. Non-communication or isolated Tasks can not only lead to coordination issues, but also delays in submission of deliverables and milestones.

Mitigations:
- Mailing lists have been established for all WPs for their internal coordination. That induces transparency and accountability as well as good internal communication to avoid unclear Tasks.
- An internal newsletter with the highlights of the projects will be circulated internally every 4 months in order to interlink and inform all WPs.

Conclusion

In the first version of the Quality Plan (submitted at M3), SAFECARE partners have decided on several measures to assure the efficient delivery of their outputs in the quality that it is required. During the first 8 months of the project, the Consortium has followed all these guidelines and will continue to do so for the whole duration of the project. The project coordinator (AP-HM) remains the partner to whom to report. The Quality Manager can also be contacted if additional issues occur or amendments are necessary. The guidelines mentioned in D2.4 are currently used by the Consortium. They have been measured and hereafter will be measured against the KPI's after the first six months in order to assess what will work and what will not in terms of process.

In D2.5, the Consortium also presents a common lexicon to be used by all partners in order to align the language used in deliverables and dissemination material. The second version of the quality plan is considered as the definitive rulebook to be followed. Deliverables and material up to that point will be processed by the Internal Reviewers and the Quality Manager as stated in the text above.

Annex 1 – SAFECARE Lexicon

Acceptable Risk: The level of risk (likelihood of occurrence and consequence of impact) for any activity or situation that is sufficiently low that society (or an organization within society that is managing the risk) is comfortable with it. Society (and an individual organization) does not generally consider expenditure in further reducing such risks justifiable.
(Source: ICDRM/GWU 2010)

Access Control: To ensure that access to assets is authorized and restricted based on business and security requirements.
(Source: ISO 27000-2018)

Accessibility: All access including emergency exits.

Accountability: Property that ensures that the actions of an entity may be traced uniquely to that entity.
(Source: ISO 2382:2015)

Alert: Alert police officers and police.

Alert Stage: Classification of a situation or a situation with regard to the measures to be taken.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

APT (Advanced persistent threat): A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors. The advanced persistent threat: pursues its objectives repeatedly over an extended period of time; adapts to defenders' efforts to resist it; and is determined to execute its objectives.
(Source: Adapted from NIST)

Asset: Any element having value for the organization.
(Source : ISO 27001)
Primary (or business) asset: Information or process judged to be important for the organization.
Supporting asset: Asset on which primary (or business) assets depend. IT systems, organizations and premises are distinguished in particular.

Attack: Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
(Source: ISO 27000-2018)

Audit: Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
(Source: ISO 27000-2018)

Audit scope: extent and boundaries of an audit (3.3)

(SOURCE: ISO 19011:2011)

Authentication: Provision of assurance that a claimed characteristic of an entity is correct.
(Source: ISO 27000-2018)

Availability: Property of being accessible and usable on demand by an authorised entity.
(Source: ISO 27000-2018)

Base measure: Measure defined in terms of an attribute and the method for quantifying it.
A base measure is functionally independent of other measures.
[Source: ISO/IEC/IEEE 15939:2017, 3.3, modified / ISO 27000-2018)

Block: Block the dynamics of malicious action.

Business continuity: Capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruption.
(Source: ISO 22300:2018)

Business continuity management: Holistic management process that identifies potential threats to an organization and the impact those threats, if realized, can cause on business operations, and provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of key interested parties, reputation, brand and value-creating activities.
(Source: ISO 22300:2018)

Business continuity management system (BCMS): Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
(Source: ISO 22300:2018)

Business continuity plan: Documented procedures that guide an organization to respond, recover, resume and restore itself to a pre-defined level of operation following a disruption.
(Source: ISO 22300:2018)

Business continuity programme: Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
(Source: ISO 22300:2018)

Business impact analysis: Process of analysing activities and the effect that a business disruption can have upon them.
(Source: ISO 22300:2018)

Business process: Organised set of activities that use resources to transform inputs into outputs (ISO 9000).

Campaign: A grouping of coordinated adversarial behaviours that describes a set of malicious activities that occur over a period of time against one or more specific targets.
(Source: Adapted from STIX)

Capacity: The combination of all the strengths, attributes and resources available within an organization that can be used to achieve agreed goals.
(Source: World Health Organization (2011) Hospital emergency response checklist. An all-hazards tool for hospital administrators and emergency managers, WHO Regional Office for Europe, WHO Publications, Copenhagen, Denmark, Available at: http://www.euro.who.int/__data/assets/pdf_file/0020/148214/e95978.pdf?ua=1)

Capacity-building: The practice of enhancing the strengths and attributes of and the resources available to an individual, community, society or organization to respond to change.
(Source: World Health Organization (2017b) Protecting health in Europe from climate change:2017 update WHO Regional Office for Europe, WHO Publications, Copenhagen, Denmark Available at: http://www.euro.who.int/__data/assets/pdf_file/0004/355792/ProtectingHealthEuropeFromClimateChange.pdf?ua=1)

Cic: Information and Command Center (place where 17 police help calls arrive and are then handled by sending police crews).

Competence: Ability to apply knowledge and skills to achieve intended results.
(Source: ISO 27000-2018)

Compromise: Violation of the security of an information system.
(Source: Adapted from ISO 21188:2018)

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. The protection of communications or stored data against interception and reading by unauthorized persons.
(Source: ISO 27000:2018)

Conformity: Fulfilment of a requirement.
(Source: ISO 27000:2018)

Consequence: Outcome of an event affecting objectives.
(Source: ISO 27000:2018)

Context establishment: Definition of the external and internal parameters to be taken into account as part of risk management and definition of the study scope as well as the risk criteria for the risk management policy.
(Source: ISO Guide 73)

Contingency plan: Proposed strategy and tactics (often documented) to be used when a specific issue arises or event occurs during the course of emergency or disaster operations.
(Source: ICDRM/GWU 2010)

Continual improvement: Recurring activity to enhance performance.
(Source: ISO 27000:2018)

Continuity: Strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations and events in order to continue operations at an acceptable predefined level.
(Source: ISO 22300:2018)

Control: Measure that is modifying risk.
(Source: ISO 27000:2018)

Control objective: Statement describing what is to be achieved as a result of implementing controls.
(Source: ISO 27000:2018)

Control of spaces: Concept intended to discourage the offender through electronic protection or, failing that, due diligence or constant vigilance.

Cop: Police Operations Commander (Police officer who pilots the intervention in case of mass killings).

Correction: Action to eliminate a detected non conformity.
(Source: ISO 27000:2018)

Corrective action: action to eliminate the cause of a nonconformity and to prevent recurrence.
(Source: ISO 27000:2018)

Countermeasure: Action taken to lower the likelihood of a security threat scenario succeeding in its objectives, or to reduce the likely consequences of a security threat scenario.
(Source: ISO 22300:2018)

Crisis: Unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment.
(Source: ISO 223000:2018)

Crisis committee: Structure/institution that creates the conditions for the coordination of all crisis-related activities and directs crisis management.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Crisis communication: The accumulation of information and opinions during a crisis to prevent or limit damage in an institution.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Crisis management: Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an

effective response that safeguards the interests of the organization's key interested parties, reputation, brand and value-creating activities, as well as effectively restoring operational capabilities.
(Source: ISO 22300:2018)

Crisis management room: Room specifically available to the crisis unit during and after a crisis and in the run-up to the crisis, for coordinating crisis management and carrying out exercises.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Crisis management team: Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency /crisis situation, and providing direction during the recovery process, both pre-and post-disruptive incident.
(Source: ISO 22300:2018)

Critical facilities: The primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency.
(Source: WHO/PAHO (2015) Hospital Safety Index, Guide for Evaluators, Safe Hospitals Initiative, 2nd Edition, World Health Organization and Pan American Health Organization, Switzerland, Available at: http://www.who.int/hac/techguidance/hospital_safety_index_evaluators.pdf)

Critical infrastructure: Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (NIMS 12/08) See also "Key Resources."
(Source: ICDRM/GWU 2010)

Critical infrastructure information: Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:
• Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; or threatens public health or safety.
• The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
• Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation.
(Source: ICDRM/GWU 2010)

Criticality: The measure of the significance of a process in relation to the consequences that a degradation or failure of the process has for the functioning of a facility.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Cyber alert: Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems.
(Source: Adapted from NIST)

Cyber event: Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. A cyber event can consist of something not happening.
(Source: Adapted from NIST and ISO/IEC 27000:2018)

Cyber incident: A cyber event that: jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
(Source: Adapted from NIST)

Cyber incident response plan: The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.
(Source: Adapted from NIST and NICCS)

Cyber resilience: The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
(Source: Adapted from CERT Glossary, CPMI-IOSCO and NIST)

Cyber risk: The combination of the probability of cyber incidents occurring and their impact.
(Source: Adapted from CPMI-IOSCO, ISACA Fundamentals and ISACA Full Glossary)

Cyber security, internet security: Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
(Source: ISO 27032:2012)

Cyber threat: A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.
(Source: Adapted from CPMI-IOSCO)

Cybercrime: Criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.
(Source: ISO 27032:2012)

Cybersecurity: Cyberspace security's preservation of confidentiality, integrity and availability of information in the Cyberspace.

(Source: ISO27032:2012)

Cyberspace: Complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
(Source: ISO 27032:2012)

Cyberspace application services: Application services provided over the Cyberspace.
(Source: ISO 270323012)

Cyber-squatters: Individuals or organizations that register and hold on to URLs that resemble references or names of other organizations in the real world or in the Cyberspace.
(Source: ISO 27032:2012)

Damage/harm: Negatively assessed impact of an event on a risk element.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Ddos (distributed denial of service): A denial of service that is carried out using numerous sources simultaneously.
(Source: Adapted from NICCS)

Deceptive software: Software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions.
(Source: ISO 27032:2012)

Defence-in-depth: Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.
(Source: Adapted from NIST and FFIEC)

Delay: Delay the offender's action.

Derived measure: Measure that is defined as a function of two or more values of base measures.
[Source: ISO/IEC/IEEE 15939:2017, 3.8, modified — ISO 27000:2018)

Disaster: Situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected organization, community or society to respond and recover using its own resources.
(Source: ISO 22300:2018)

Disaster Risk Management: The systematic process of using administrative directives, organizations, operational skills and capacities to implement strategies, policies and improved coping capacities in order to lessen the adverse impacts of hazards and the possibility of disaster.
(Source: WHO/PAHO – 2015 - Hospital Safety Index, Guide for Evaluators, Safe Hospitals Initiative, 2nd Edition, World Health Organization and Pan American Health Organization,

Switzerland, Available at: http://www.who.int/hac/techguidance/hospital_safety_index_evaluators.pdf)

Disaster risk reduction: The concept and practice of reducing disaster risks through systematic efforts to analyze and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and property, wise management of land and the environment, and improved preparedness for adverse events.
(Source: WHO/PAHO (2015) Hospital Safety Index, Guide for Evaluators, Safe Hospitals Initiative, 2nd Edition, World Health Organization and Pan American Health Organization, Switzerland, Available at: http://www.who.int/hac/techguidance/hospital_safety_index_evaluators.pdf)

Disruption: Event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), that causes an unplanned, negative deviation from the expected delivery of products or services according to an organization's objectives.
(Source: ISO 22300:2018)

Dissuade: Deter the aggressor from going further in his/her project.

Documented information: Information required to be controlled and maintained by an organization and the medium on which it is contained.
(Source: ISO 27000:2018)

Dos (Denial of Service): Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users.
(Source: Adapted from ISO/IEC 27033-1:2015)

Effectiveness: extent to which planned activities are realized and planned results.
(Source: ISO 27000-2018)

Emergency: Sudden, urgent, usually unexpected occurrence or event requiring immediate action.
(Source: ISO 22300:2018)

Emergency management: Overall approach for preventing emergencies and managing those that occur.
(Source: ISO 22300:2018)

Endangerment: The possibility of an event with a certain intensity arising from a hazard at a specific location, which can cause damage to a risk element /process/protected good.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Escalation model: Mechanism of situation assessment, definition of alert levels and transmission of messages to management.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Evacuation: The organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.
(Source: ICDRM/GWU 2010)

Evaluation: Systematic process that compares the result of measurement to recognised criteria to determine the discrepancies between intended and actual performance.
(Source: ISO 22300:2018)

Event: Occurrence or change of a particular set of circumstances.
(Source: ISO 27000-2018)

Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.
Evidence does not necessarily prove truth or existence of something but contributes to establish proof.

Exploit: Defined way to breach the security of information systems through vulnerability.
(Source: ISO 27039:2015)

Exposure: The condition of being subjected to a hazard or source of risk.

External context: external environment in which the organization seeks to achieve its objectives.
(Source: ISO 27000-2018)

External dependency: An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization.
(Source: CERT Resilience Management Model, Version 1.2/2016)

External entity: An individual, business, or business unit (such as a customer, a contractor, or another group within the same enterprise) that is external to and in a supporting or influencing relationship with the organization that is using a process area.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Extreme event: Extreme events are rare events that deviate greatly from the average and can lead to crises.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Feared event: Generic scenario representing a situation feared by the organization. It is expressed by the combination of threat sources that may be its cause, a primary asset (or business asset), a security criterion, a relevant need of security and potential impacts.

Function: One of the five major activities in the incident command system (which are, respectively, command, operations, planning, logistics, and finance/administration). The term

'function' is also used when describing the activity involved (e.g. 'the planning function'). Other functions, such as intelligence/investigations, may be established if it is required in order to meet incident management needs.
(Source: World Health Organization (2015) Framework for a Public Health Emergency Operations Centre, Public Health Emergency Operations Centre Network (EOC-NET), WHO, Geneva. Available at: http://www.who.int/ihr/publications/9789241565134_eng/en/Gign)

Governance: An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Governance of information security: System by which an organization's information security activities are directed and controlled.
(Source: ISO 27000-2018)

Governing body: Person or group of people who are accountable for the performance and conformity of the organization.
(Source: ISO 27000-2018)

Hacking: Intentionally accessing a computer system without the authorization of the user or the owner.
(Source: ISO 27032:2012)

Hactivism: The act of hacking a network or a website for a politically or socially motivated purpose.
(Source: ISO 27032:2012)

Hardening of targets: Deter the offender from acting out or compelling him to make a significant effort to achieve his ends.

Hazard: Source of potential harm.
(Source: ISO 22300:2018)

Hazard analysis: Involves identifying all of the hazards that potentially threaten a jurisdiction [and/or the organization that is performing the hazard analysis] and analyzing them in the context of the jurisdiction to determine the degree of threat that is posed by each.
(Source: ICDRM/GWU 2010)

Hazard identification: The process of recognizing that a hazard exists and defining its characteristics.
(Source: ICDRM/GWU 2010)

Hazard monitoring function: Activities to obtain evidence-based information on hazards in a defined area used to make decisions about the need for public warning.
(Source: ISO 22300:2018)

Hazard probability: The estimated likelihood that a hazard will occur in a particular area.
(Source: ICDRM/GWU 2010)

Hazard risk: A quantitative product of the probability of a hazard occurring and the projected consequence of the impact.
(Source: ICDRM/GWU 2010)

Health informatics: Scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks.
(Source: ISO 27000-2018)

Health information system: Repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users.
(Source: ISO 27000-2018)

Health professional: Person who is authorised by a recognised body to be qualified to perform certain health duties
(Source: ISO 27000-2018)

Healthcare: Type of services provided by professionals or paraprofessionals with an impact on health status.
(Source: ISO 27000-2018)

Healthcare organization: Organization that provides healthcare services
(Source: ISO 27000-2018)

High-value assets: People, information, technology, or facilities upon whose confidentiality, integrity, availability, and productivity a high-value service depends.
(Source: CERT Resilience Management Model, Version 1.2/2016)

High-value services: Services upon which the success of the organization's mission depends.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Iam (identity and access management): Encapsulates people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.
(Source: Adapted from ISACA Full Glossary)

Identifiable person: One who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
(Source: ISO 27000-2018)

Identification: Process of recognizing the attributes that identify an entity.
(Source: ISO 22300:2018)

Impact: Evaluated consequence of a particular outcome.
(Source: ISO 22300:2018)

Impact analysis: Process of analysing all operational functions and the effect that an operational interruption can have upon them.
(Source: ISO 22300:2018)

Impact area (organizational impact area): An area in which criteria are established to determine and express the potential impact of realized risk on the organization. Typical impact areas include life and safety of employees and customers, financial, legal, and productivity.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Impact valuation: Determines the extent of the impact of operational risk using the organization's risk measurement criteria.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Incident: Situation that can be, or could lead to, a disruption, loss, emergency or crisis.
(Source: ISO 22300:2018)

Incident closure: The retirement of an incident that has been responded to (i.e., there are no further actions required, and the organization is satisfied with the result) and for which the organization has performed a formal post-incident review.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Incident escalation: The process of notifying relevant stakeholders about an incident that requires an organizational response and involves stakeholder actions to implement, manage, and bring to closure with an appropriate and timely solution.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Incident management: The broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all levels of government, utilizing both governmental and nongovernmental resources to plan for, respond to, and recover from an incident, regardless of cause, size, or complexity.
(Source: ICDRM/GWU 2010)

Incident management system: System that defines the roles and responsibilities of personnel and the operating procedures to be used in the management of incidents.
(Source: ISO 22300:2018)

Incident recognition: The first stage of response. It is the time interval and process in which an organization determines if it should activate its Emergency Operations Plan (EOP) and manage actions through EOP mechanisms. The incident recognition process identifies an "anomaly" (independently or through communication from others), develops a rapid situational assessment of the anomaly, and determines whether an "incident response" by the organization may be indicated. "Incident response" is then conducted through processes and guidance presented in the organization's EOP.

(Source: ICDRM/GWU 2010)

Incident response: Actions taken in order to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing events or disruptions, and to recover to a normal situation.
(Source: ISO 22300:2018)

Incident review: A brief review of the incident conducted with the relevant section leaders and other response personnel (as appropriate). This is conducted as soon as possible after the incident, with a primary goal of presenting incident details along a timeline, potentially resolving misunderstandings and providing relevant parties with a more complete picture of "what happened and why." This "IR" is distinct from any After-Action Report meetings intended to capture valuable information for EOP improvement.
(Source: ICDRM/GWU 2010)

Indicator: Measure that provides an estimate or evaluation.
(Source: ISO 27000-2018)

Information: Data processed, organized and correlated to produce meaning.
(Source: ISO 22300:2018)

Information asset: Information or data that is of value to the organization, including diverse information such as patient records, intellectual property, customer information, and contracts.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Information management: The processes that collect, analyze, format and transmit data and information during an incident.
The collection, organization, and control over the structure, processing, and delivery of information from one or more sources and distribution to one or more audiences who have a stake in that information.
(Source: ICDRM/GWU 2010)

Information need: Insight necessary to manage objectives, goals, risks and problems.
(Source: ISO 27000-2018)

Information process: Organised set of processes that use supporting assets to transform input information into output information.
(Source: ISO 9000)

Information processing facilities: Any information processing system, service or infrastructure, or the physical location housing it.
(Source: ISO 27000-2018)

Information security: Preservation of confidentiality, integrity and availability of information
(Source: ISO 27000-2018)

Information security continuity: Processes and procedures for ensuring continued information security operations.
(Source: ISO 27000-2018)

Information security event: Identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant.
(Source: ISO 27000-2018)

Information security: Forensics application of investigation and analysis techniques to capture, record and analyse information security incidents.
(Source: ISO 27035:2011)

Information security incident: Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
(Source: ISO 27000-2018)

Information security incident management: Set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
(Source: ISO 27000-2018)

Information security incident response team: Team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle.
(Source: ISO 27035:2011)

Information security management system (isms) professional: Person who establishes, implements, maintains and continuously improves one or more information security management system processes.
(Source: ISO 27000-2018)

Information security risk: Effect of uncertainty on the attaining of objectives.
(Source: ISO Guide 73)

Information sharing: Exchange of data, information and/or knowledge that can be used to manage risks or respond to events.
(Source: Adapted from NICCS)

Information sharing community: Group of organizations that agree to share information.
(Source: ISO 27000-2018)

Information system: Set of applications, services, information technology assets, or other information-handling components.
(Source: ISO 27000-2018)

Infrastructure: System of facilities, equipment and services needed for the operation of an organization.

(Source: ISO 22300:2018)

Integrated risk management: Incorporation and coordination of strategy, capability, and governance to enable risk-informed decision making.
(Source: World Health Organization (2015) Framework for a Public Health Emergency Operations Centre, Public Health Emergency Operations Centre Network (EOC-NET), WHO, Geneva Available at: http://www.who.int/ihr/publications/9789241565134_eng/en/)

Integrity: Property of accuracy and completeness.
(Source: ISO 27000-2018)

Interdependency: Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.
(Source: ICDRM/GWU 2010)

Interested party (preferred term)/ Stakeholder (admitted term): Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity
(Source: ISO 27000-2018)

Internal attack: Attack perpetrated by people or entities directly or indirectly linked with the legitimate manufacturer, originator of the goods or rights holder (staff of the rights holder, subcontractor, supplier, etc.).
(Source: ISO 22300:2018)

Internal context: Internal environment in which the organization seeks to achieve its objectives
(Source: ISO Guide 73:2009, 3.3.1.2 - ISO 27000:2018)
Internet: Collection of interconnected networks.
(Source: ISO 27032:2012)

Internet crime: Criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime.
(Source: ISO 27032:2012)

Internet safety: Condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Internet which could be considered non-desirable.
(Source: ISO 27032:2012)

Internet service provider: Organization that provides Internet services to a user and enables its customers access to the Internet.
(Source: ISO 27032:2012)

Internet services: Services delivered to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorization and domain name services.
(Source: ISO 27032:2012)

Interoperability: Ability of diverse systems and organizations to work together.
(Source: ISO 22300:2018)

Iocs (indicators of compromise): Identifying signs that a cyber incident may have occurred or may be currently occurring.
(Source: Adapted from NIST)

Irt (incident response team) [also known as cert or csirt]: Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.
(Source: ISO 27035-1:2016).

Key performance indicator: KPI / quantifiable measure that an organization uses to gauge or compare performance in terms of meeting its strategic and operational objectives.
(Source: ISO 22300:2018)

Lawsuit: Operation/function in an institution for providing a service or a product.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Level of risk: magnitude of a risk expressed in terms of the combination of consequences and their likelihood.
(Source: ISO 27000-2018)

Likelihood: Chance of something happening (Source: ISO 27000-2018)
Possibility that something may happen (Source: ISO Guide 73)

Malicious contents: Applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them.
(Source: ISO 27032:2012)

Malware, malicious software: Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. EXAMPLE: Viruses, worms, trojans.
(Source: ISO 27032:2012)

Management: Coordinated activities to direct and control an organization.
(Source: ISO 22300:2018)

Management plan: clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the management process.
(Source: ISO 22300:2018)

Management systems: Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.
(Source: ISO 27000-2018)

Measure: Variable to which a value is assigned as the result of measurement

[Source: ISO/IEC/IEEE 15939:2017, 3.15, modified — ISO 27000-2018)

Measurement: Process to determine a value.
(Source: ISO 27000-2018)

Measurement function: Algorithm or calculation performed to combine two or more base measures.
(Source: ISO/IEC/IEEE 15939:2017, 3.20 - ISO 27000-2018)

Measurement method: Logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale.
(Source: ISO/IEC/IEEE 15939:2017, 3.21, modified - ISO 27000-2018)

Measures, preparatory: Options for action that are developed in the run-up to crises for better crisis management, but are only applied in the event of a crisis.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Measures, preventive: Action steps and means that are developed and implemented or used in the run-up to crises and that reduce the risks for an institution. These include risk-reducing measures that physically protect risk elements or support the functionality of processes through redundant systems or replacement systems. Both aspects contribute to operational continuity.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Mitigation: Limitation of any negative consequence of a particular incident.
(Source: ISO 22300:2018)

Monitoring: Determining the status of a system, a process or an activity.
(Source: ISO 27000-2018)

Multi-factor authentication: The use of two or more of the following factors to verify a user's identity: knowledge factor (something an individual knows); possession factor (something an individual has); biometric factor (something that is a biological and behavioural characteristic of an individual).
(Source: Adapted from ISO/IEC 27040:2015 and ISO/IEC 2832-37:2017)

Neuralgic points: Process areas or individual risk elements whose impairment leads to far-reaching failures or damage.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Nonconformity: Non-fulfilment of a requirement.
(Source: ISO 27000-2018)

Non-repudiation: Ability to prove the occurrence of a claimed event or action and its originating entities.

(Source: ISO 27000-2018)

Notification: Reports with brief and concise information about events, perceptions and circumstances to inform about a situation.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Objective: Result to be achieved
(Source: ISO 27000-2018)

Operational continuity management: Management of measures to maintain business activities, especially in the event of a crisis; for example, activation of a redundant control center (operational continuity management = business continuity management)
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Operational protection objective: Concrete description of a target state to be aimed at, which serves to achieve a strategic protection goal.
(Source: Adapted from Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus)

Operational resilience requirements: Refers collectively to requirements that ensure the protection of high-value assets as well as their continuity when a disruptive event has occurred. The requirements traditionally encompass security, business continuity, and IT operational requirements. These include the security objectives for information assets (confidentiality, integrity, and availability) as well as the requirements for business continuity planning and recovery and the availability and support requirements of the organization's technical infrastructure.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Operational risk: Potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Operational risk taxonomy: Collection and cataloging of common operational risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line of business if operational assets and services are affected by them.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Organization: Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.
(Source: ISO 27000-2018)

Organizational structure: Form of organisation for the performance of tasks as well as determination of responsibilities and communication channels.

(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Outsource: Make an arrangement where an external organization performs part of an organization's function or process.
(Source: ISO 27000-2018)

Owner: Entity that legally controls the licensing and user rights and distribution of the object associated with the unique identifier (UID)
(Source: ISO 22300:2018)

Partial risk: Risk relating to a risk element
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Partial vulnerability: Vulnerability relating to a risk element.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Participant: Person or organization who performs a function related to an exercise.
(Source: ISO 22300:2018)

Patient: Subject of care (3.9) consisting of one person.
(Source: ISO 27000-2018)

Pegase: Piloting Events, Activities Management and Crew Safety (Software developped by Airbus CS and used in CICs.

Penetration testing: A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
(Source: NIST)

People at risk: Individuals in the area who may be affected by an incident.
(Source: ISO 22300:2018)

Performance: Measurable result.
(Source: ISO 27000-2018)

Performance evaluation: Process of determining measurable results.
(Source: ISO 22300:2018)

Perimetry: Space that encloses the fence to the walls of buildings, including openings.

Periphery: Space between the fence or the facade and the environment close to the site (taking into account the elements of context that may affect the safety and / or the safety of the hospital).

Personal health information: Information about an identifiable person that relates to the physical or mental health of the individual.
(Source: ISO 27000-2018)
Personnel: People working for and under the control of an organization.
(Source: ISO 22300:2018)

Phishing: Fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication.
(Source: ISO 27032:2012)

Physical security: As applied to cyber terrorism this term encompasses those actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical information management systems' software and hardware.
(Source: ICDRM/GWU 2010)

Plan, emergency management: An emergency management plan using 'management by objective' explains an organizational structure and defines how the participants in the organization operate to achieve the end goal and interim objectives. A 'plan' may be guidance that is triggered by a defined set of circumstances (such as an Emergency Operations Plan) or may be guidance for actions over a defined time interval (such as an annual Preparedness Work Plan). This contrasts with an Emergency Management Program.
(Source: ICDRM/GWU 2010)

Policy: Intentions and direction of an organization , as formally expressed by its top management.
(Source: ISO 27000-2018)

Potential danger: All possible characteristics of a hazard.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Potentially unwanted software: Deceptive software, including malicious and non-malicious software, that exhibits the characteristics of deceptive software.
(Source: ISO 27032:2012)

Preparedness: Readiness / activities, programmes, and systems developed and implemented prior to an incident that can be used to support and enhance prevention, protection from, mitigation of, response to and recovery from disruptions, emergencies or disasters.
(Source: ISO 22300:2018)

Prevention: Measures that enable an organization to avoid, preclude or limit the impact of an undesirable event or potential disruption.
(Source: ISO 22300:2018)

Prevention of hazards and threats: Process, practices, techniques, materials, products, services or resources used to avoid, reduce, or control hazards and threats and their associated risks of any type in order to reduce their potential likelihood or consequences.

(Source: ISO 22300:2018)

Preventive action: Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.
(Source: ISO 22300:2018)

Privacy: The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Probability: Measure of the chance of occurrence expressed as a number between 0 and 1 where 0 is impossibility and 1 is absolute certainty.
(Source: ISO 22300:2018)

Procedure: Specified way to carry out an activity or a process.
(Source: ISO 22300:2018)

Process: Set of interrelated or interacting activities which transforms inputs into outputs.
(Source: ISO 27000-2018)

Process organization: The process organisation describes and regulates the work processes of an organisational unit taking into account space, time, people and material resources.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Protection: Measures that safeguard and enable an organization to reduce the impact of a potential disruption.
(Source: ISO 22300:2018)

Protection strategy: The strategy, related controls, and activities necessary to protect an asset from undesired harm or disruptive events. The protection strategy is relative to the conditions to which the asset is subjected.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Protocol: A set of established guidelines for actions (which may be designated by individuals, teams, functions, or capabilities) under various specified conditions.
(Source: ICDRM/GWU 2010)

Ps: Police Help. General services units that patrol daily on the public highway and respond to CIC instructions (first responders level one).

Raid: Search Assistance Intervention Deterrence (one of the Special Forces reporting to the French National Police -Level3-).

Ramses (evolution ii): Offer of the French Ministry of the Interior for the direct connection of aggression and intrusion type alarms to the security services of the national Police

(Source: decree N° 64-13 of 4 January 1964)

Record: Document stating results achieved or providing evidence of activities performed.
(Source: ISO 22300:2018)

Recovery: Restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organizations, including efforts to reduce risk factors.
(Source: ISO 22300:2018)

Recovery plan: Plan developed to restore an affected area or community.
(Source: ICDRM/GWU 2010)

Recovery point objective (RPO): Point to which information used by an activity is restored to enable the activity to operate on.
(Source: ISO 22300:2018)

Redundancy: Having secondary or backup human and physical resource capacity in case primary resource capacity is impaired or becomes unavailable for any reason.
(Source: World Health Organization (2015) Framework for a Public Health Emergency Operations Centre, Public Health Emergency Operations Centre Network (EOC-NET), WHO, Geneva Available at: http://www.who.int/ihr/publications/9789241565134_eng/en/)

Reliability: Property of consistent intended behaviour and results.
(Source: ISO 27000-2018)

Requirement: Need or expectation that is stated, generally implied or obligatory.
(Source: ISO 27000-2018)

Residual risk: Risk remaining after risk treatment
(Source: ISO 22300:2018)

Resilience: Ability to absorb and adapt in a changing environment.
(Source: ISO 22300:2018)

Resources: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an Emergency Operations Center.
(Source: ICDRM/GWU 2010)

Response: • The phase of Comprehensive Emergency Management that addresses the immediate and short-term effects of the disaster or emergency. It includes activities immediately before (for an impending threat), during, and after a hazard impact to address the immediate and short-term effects of the disaster or emergency. • In disaster/emergency management applications, activities designed to address the immediate and short-term effects of the disaster/emergency. • Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution

of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.
(Source: ICDRM/GWU 2010)

Response plan: Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident.
(Source: ISO 22300:2018)

Response programme: Plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations and critical assets.
(Source: ISO 22300:2018)

Response team: Group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures.
(Source: ISO 22300:2018

Restart: Phase from completion of crisis response to initiation of emergency operation.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Review: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
(Source: ISO Guide 73:2009, 3.8.2.2, modified - ISO 27000-2018)

Review object: Specific item being reviewed.
(Source: ISO 27000-2018)

Review objective: Statement describing what is to be achieved as a result of a review.
(Source: ISO 27000-2018)

Risk: Effect of uncertainty on objectives.
(Source: ISO 27000-2018)

Risk acceptance: Informed decision to take a particular risk.
(Source: ISO 27000-2018)

Risk analysis: Process to comprehend the nature of risk and to determine the level of risk
(Source: ISO 27000-2018)

Risk assessment: Overall process of risk identification, risk analysis and risk evaluation
(Source: ISO 27000-2018)

Risk assessment methodology: Set of methods, principles, or rules used to identify and assess risks and to form priorities, develop courses of action, and inform decision-making.
(Source: ICDRM/GWU 2010)

Risk assessment tool: Activity, item, or program that contributes to determining and evaluating risks. Tools can include computer software and hardware or standard forms or checklists for recording and displaying risk assessment data.
(Source: ICDRM/GWU 2010)

Risk avoidance: Argued decision not to carry out an activity, or to withdraw from it, in order not to be exposed to a particular risk.
(Source: ISO Guide 73)

Risk criteria: Terms of reference against which the significance of a risk is evaluated
(Source: ISO 27000-2018)

Risk element: Individual component of critical sub-processes within the framework of risk management; in the context of this guideline.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Risk evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
(Source: ISO 22300:2018)

Risk identification: Process of finding, recognizing and describing risks.
(Source: ISO 22300:2018)

Risk management: Coordinated activities to direct and control an organization with regard to risk.
(Source: ISO 22300:2018)

Risk management methodology: Set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.
(Source: ICDRM/GWU 2010)

Risk management plan: Document that identifies risks and specifies the actions that have been chosen to manage those risks.
(Source: ICDRM/GWU 2010)

Risk measurement criteria: Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact areas.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Risk mitigation: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Measures may be implemented prior to, during, or after an incident, event, or occurrence.
(Source: ICDRM/GWU 2010)

Risk mitigation plan: A strategy for mitigating risk that seeks to minimize the risk to an acceptable level.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Risk monitoring and review: Risk monitoring: verification, supervision, critical observation or determination of a state in order to constantly identify changes relative to a required or expected level of performance; Review: activity undertaken to determine the adaptation, sufficiency and effectiveness of the object studied to attain the established objectives.
(Source: ISO Guide 73)

Risk perception: Process of subjective recording, processing and evaluation of risk-related information, which originates from personal experience, direct observation, reception of messages conveyed (e.g. by the media) and direct communication with individuals.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Risk policy: Strategy of an institution that defines the systematic handling and approach to risks as well as the framework and objectives for risk management.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Risk reduction: • Long-term measures to reduce the scale and/or the duration eventual adverse effects of unavoidable or unpreventable disaster hazards on a society which is at risk, by reducing the vulnerability of its people, structures, services, and economic activities to the impact of known disaster hazards. Typical risk reduction measures include improved building standards, flood plain zoning and land-use planning, crop diversification, and planting windbreaks. The measures are frequently subdivided into "structural" and "non-structural", "active" and "passive" measures. N.B. A number of sources have used "disaster mitigation" in this context, while others have used "disaster prevention." • Decrease in risk through risk avoidance, risk control or risk transfer. Risk reduction may be estimated both during the decision and evaluation phases of the risk management cycle.
(Source: ICDRM/GWU 2010)

Risk retention: Acceptance of the potential advantage of a gain or the potential disadvantage of a loss arising from a particular risk.
(Source: ISO Guide 73)

Risk threshold: An organizationally developed type of risk parameter that is used by management to determine when a risk is in control or when it has exceeded acceptable organizational limits.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Risk tolerance: Thresholds that reflect the organization's level of risk appetite by providing levels of acceptable risk in each operational risk category that the organization has established. Risk tolerance, as a risk parameter, also establishes the organization's philosophy on risk management—how risks will be controlled, who has the authorization to accept risk on behalf of the organization, and how often and to what degree operational risk should be assessed.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Risk transfer/Risk sharing: form of risk treatment implying the agreed distribution of risk with other parties.
(Source: ISO Guide 73)

Risk treatment: Process to modify risk.
(Source: ISO 27000-2018)

Root-cause analysis: An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Safety: Safety, in the traditional sense, refers to monitoring and eliminating the work-place risk of personnel casualties (injuries and deaths) or reducing it to some acceptable level.
(Source: ICDRM/GWU 2010)

Safety audit: Offer of the French Ministry of the Interior to offer advice or recommendations regarding safety (all the hospitals of the AP-HM were subject to a safety audit)

Scalability: The capability to expand or reduce in size in order to adjust capacity and capability by adding or deactivating organizational modules to adapt to changes in demand without the need for reconfiguration of a basic structure.
(Source: World Health Organization (2015) Framework for a Public Health Emergency Operations Centre, Public Health Emergency Operations Centre Network (EOC-NET), WHO, Geneva Available at: http://www.who.int/ihr/publications/9789241565134_eng/en/)

Scam: Fraud or confidence trick.
(Source: ISO 27032:2012)

Scenario/ scenario development: Acceptance of possible events or sequences of events and their effects on risk elements/processes.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Secret: Data and/or knowledge that are protected against disclosure to unauthorised entities.
(Source: ISO 22300:2018)

Security: State of being free from danger or threat.
(Source: ISO 22300:2018)

Security accreditation: Declaration by the accreditation authority, on the basis of the accreditation file, that the information system in question is appropriate for treating information at a given classification level, in compliance with the stated security objectives, and the induced residual security risks are accepted and controlled The security accreditation remains valid as long as the IS operates under the conditions approved by the accreditation authority.
(Source: IGI 1300)

Security aspect: Characteristic, element, or property that reduces the risk of unintentionally-, intentionally-, and naturally-caused crises and disasters which disrupt and have consequences on the products or services, operation, critical assets and continuity of an organization and its interested parties.
(Source: ISO 22300:2018)

Security criterion: Characteristic of a primary asset used to assess its various need of security.

Security implementation standard: Document specifying authorized ways for realizing security
a document that provides an overview of guidelines and contains plenty of structural components.
(Source: ISO 27000-2018)

Security management: Systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts
(Source: ISO 22300:2018)

Security management objective: Specific outcome or achievement required of security in order to meet the security management policy products, supply or services delivered by the total business to its customers or end users.
(Source: ISO 22300:2018)

Security management policy: Overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with its policy and regulatory requirements.
(Source: ISO 22300:2018)

Security needs: Precise and unambiguous definition of the level of operational needs relating to a primary asset for a given security criterion (availability, integrity, confidentiality, traceability).

Security objective: Expression of the decision to treat a risk in accordance with prescribed methods. The latter are, principally: reduction, transfer (sharing of risk), avoidance (structural change to avoid a risk situation) and retention.

Security personnel: People in an organization in the supply chain who have been assigned security related duties.
(Source: ISO 22300:2018)

Security plan: Planned arrangements for ensuring that security is adequately managed.

(Source: ISO 22300:2018)

Security threat scenario: Means by which a potential security incident can occur.
(Source: ISO 22300:2018)

Sensitive information: Information that is protected from public disclosure only because it would have an adverse effect on an organization, national security or public safety.
(Source: ISO 22300:2018)

Sensitivity: A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Severity: Estimation of the degree of the effects of a feared event or risk. It represents its consequences.
(Source: ISO Guide 73)

Shared resilience requirements: Requirements that are developed for shared organizational assets such as a facility in which more than one high-value service is executed.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Situational awareness: Being aware of and attentive to what is happening in a given environment at a particular time, with particular emphasis on the effect of changes in the environment; in effect, knowing how an incident or event is evolving.
(Source: World Health Organization (2015) Framework for a Public Health Emergency Operations Centre, Public Health Emergency Operations Centre Network (EOC-NET), WHO, Geneva Available at: http://www.who.int/ihr/publications/9789241565134_eng/en/)

Situational prevention: Concept and orientation allowing a methodical approach to the safety problem (dissuade, block, delay and alert).

Social engineering: A general term for trying to deceive people into revealing information or performing certain actions.
(Source: Adapted from FFIEC)

Space management: it's about showing that the sector is busy (for a greater responsiveness.

Spam: Abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
(Source: ISO 27032:2012)

Spyware: Deceptive software that collects private or confidential information from a computer user.
(Source: ISO 27032:2012)

Stakeholder: Person or organization that has a vested interest in the organization or its activities.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Subject of care: One or more persons scheduled to receive, receiving, or having received a health service.
(Source: ISO 27000-2018)

Supporting asset: Asset on which primary (or business) assets depend. IT systems, organizations and premises are distinguished in particular.

Target: Detailed performance requirement, applicable to an organization or parts thereof, that arises from the objectives and that needs to be set and met in order to achieve those objectives.
(Source: ISO 22300:2018)

Target group: Individuals or organizations subject to exercise.
(Source: ISO 22300:2018)

Technology asset: Any hardware, software, or firmware used by the organization in the delivery of services.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Territoriality: Ability to define and materialize the different statuses of the spaces (public / private) and their functions (traffic, parking, etc.).

Threat: Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment or the community.
(Source: ISO 22300:2018)

Threat (or risk) source/Risk source: Any element that, alone or combined with others, has an intrinsic potential to generate a risk.
(Source: ISO Guide 73)

Threat actor: A situation, entity, individual, group, or action with the potential to exploit a threat.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Threat analysis: Process of identifying, qualifying and quantifying the potential cause of an unwanted event, which may result in harm to individuals, assets, a system or organization, the environment, or the community.
(Source: ISO 22300:2018)

Threat assessment: Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat.
(Source: Adapted from NIST)

Threat environment: Set of all types of threats that could affect the current operations of the organization. (See the related term.)
(Source: CERT Resilience Management Model, Version 1.2/2016)

Threat intelligence: Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.
(Source: NIST 800-150)

Threat motive: Reason that a threat actor would exploit a vulnerability or otherwise cause harm.
(Source: CERT Resilience Management Model, Version 1.2/2016)
Threat scenario: Scenario, with a given level, describing operating methods. It combines threat sources that may be the cause, a supporting asset, a security criterion, threats and vulnerabilities that they exploit. Its level corresponds to a estimation of its likelihood.

Threat situation: Factors such as local, temporal and climatic conditions which affect a given space at a given time and which may give rise to a condition, circumstance or process the action of which may cause damage to a risk element and impairment of a process.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Threat vector: A path or route used by the threat actor to gain access to the target.
(Source: Adapted from ISACA Fundamentals)

Tlpt (threat-led penetration testing) [also known as red team testing]: A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.
(Source: G-7 Fundamental Elements)

Trojan / trojan horse: Malware that appears to perform a desirable function.
(Source: ISO 27032:2012)

Trusted information communication entity: Autonomous organization supporting information exchange within an information sharing community
(Source: ISO 27000-2018)

Ttps (tactics, techniques and procedures): Behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
(Source: Adapted from NIST 800-150)

Unsolicited email: Email that is not welcome, or was not requested, or invited.
(Source: ISO 27032:2012)

Update: Notification category that provides non-urgent emergency management information during all four phases of emergency management.
(Source: ICDRM/GWU 2010)

Virtual asset: Representation of an asset in the Cyberspace / Note 1 to entryIn this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.
(Source: ISO 27032:2012)

Virtual currency: Monetary virtual assets.
(Source: ISO 27032:2012)

Virtual world: Simulated environment accessed by multiple users through an online interface.
(Source: ISO 27032:2012)

Visibility: Objective is to see and to be seen.

Volumetry: Al internal volumes of common interest, air ambulances, reception, waiting room, care areas, stairs, ... and the private areas.

Vulnerability: Weakness of an asset or control that can be exploited by one or more threats. The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.
(Source: ISO 27000-2018)

Vulnerability analysis and resolution: An operations process area in CERT-RMM. The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Vulnerability assessment: Systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.
(Source: Adapted from NIST)

Vulnerability criterion: Conditions for vulnerability assessment.
(Source: Adapted from *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008) Schutz kritischer Infrastrukt: Risikomanagement im Krankenhaus*)

Vulnerability management strategy: Strategy for identifying and reducing exposure to known vulnerabilities.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Vulnerability repository: Organizational inventory of known vulnerabilities.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Vulnerability resolution: Action that the organization takes to reduce or eliminate exposure to vulnerability.
(Source: CERT Resilience Management Model, Version 1.2/2016)

Vulnerable group: Individuals who share one or several characteristics that are the basis of discrimination or adverse social, economic, cultural, political or health circumstances and that cause them to lack the means to achieve their rights or, otherwise, enjoy equal opportunities.
(Source: ISO 22300:2018)

Warning: Dissemination of notification message signaling imminent hazard which may include advice on protective measures. See also "alert." For example, a warning is issued by the National Weather Service to let people know that a severe weather event is already occurring or is imminent, and usually provides direction on protective actions. A "warning" notification for individuals is equivalent to an "activation" notification for response systems.
(Source: ICDRM/GWU 2010)

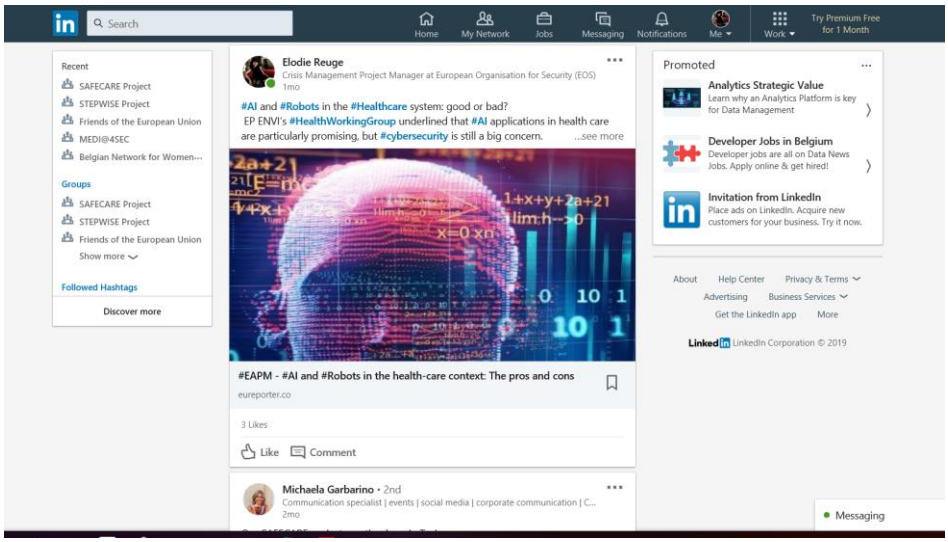
Annex 2 - Internal Reviewers list M07 – M12

Deliverable No	Deliverable name	Partner in charge	R1	R2	Due Date	Type
D1.3	GEN-Requirement N°7	*AP-HM*	KUL	EOS	12	CO
D2.1	Progress report Y1	*AP-HM*	EOS	KEMEA	12	CO
D2.5	Updated Quality Plan	*EOS*	AP-HM	FMI	8	PU
D3.3	Final SoA about security and known vulnerabilities	*ISEP*	CNAM	ISMB	12	PU
D3.5	Final requirement analysis	*EMAUG*	AMC	CSI	12	RE
D3.6	Definition of the cyber-physical scenarios of threat	*ISEP*	MS	CCS	9	RE
D3.7	Initial cyber-physical risk assessment and impact analysis	*AP-HM*	SPF	ISMSB	11	RE
D4.3	Specification of the intrusion detection system	*MS*	CSI	PEN	12	PU
D5.5	Specification of the advanced file analysis system	*CCS*	FST	BEIA	12	RE
D5.7	Specification of the E-health devices security analytics	*PEN*	AMC	CNAM	12	PU
D6.1	Specification of the global architecture	*CCS*	MS	ENC	12	PU
D6.10	Specification HAMS	*ISMB*	PMS	CSI	12	PU

Annex 2 – SAFECARE Brochure

Annex 3 - SAFECARE Website

Annex 4 - SAFECARE Social Media



Annex 5 - SAFECARE First newsletter

SAFECARE NEWSLETTER

Please find below short updates of SAFECARE's latest developments, discussions, reports and interesting upcoming events.

Management team in a nutshell

The SAFECARE (SAFEguard of Critical heAlth infrastructuRE) project was officially launched in September 2018. After more than 6 months of activity our project has come to life and our teams have rapidly gotten to know and work with each other thanks to our kickoff meeting and to our on-going focus group workshops.

Due to the technical and organizational complexities involved in our project, communications between all project members has been the key to our success thus far.

I would like to acknowledge and thank the dedication of all participants who have contributed in the crucial tasks involved in the building of the overall project (and deliverables).

Although there is still a long way to go, I am happy to report that we are actively moving forward very quickly. The project management must therefore remain highly responsive to the needs of each task force in order to maintain and enhance the quality of our exchanges and innovations.

This initial phase of the project has allowed us to establish a management and organizational system composed of the 8 Work Packages leaders among whom 3 of them assist me in coordinating: Isabel Praça (ISEP) as Scientific Coordinator, Louis Jallet (CSS) as Technical Coordinator and Elodie Reuge (EOS) as Communications and Organizational Coordinator. This team offered major support in the preparation of the overall project from its inception.

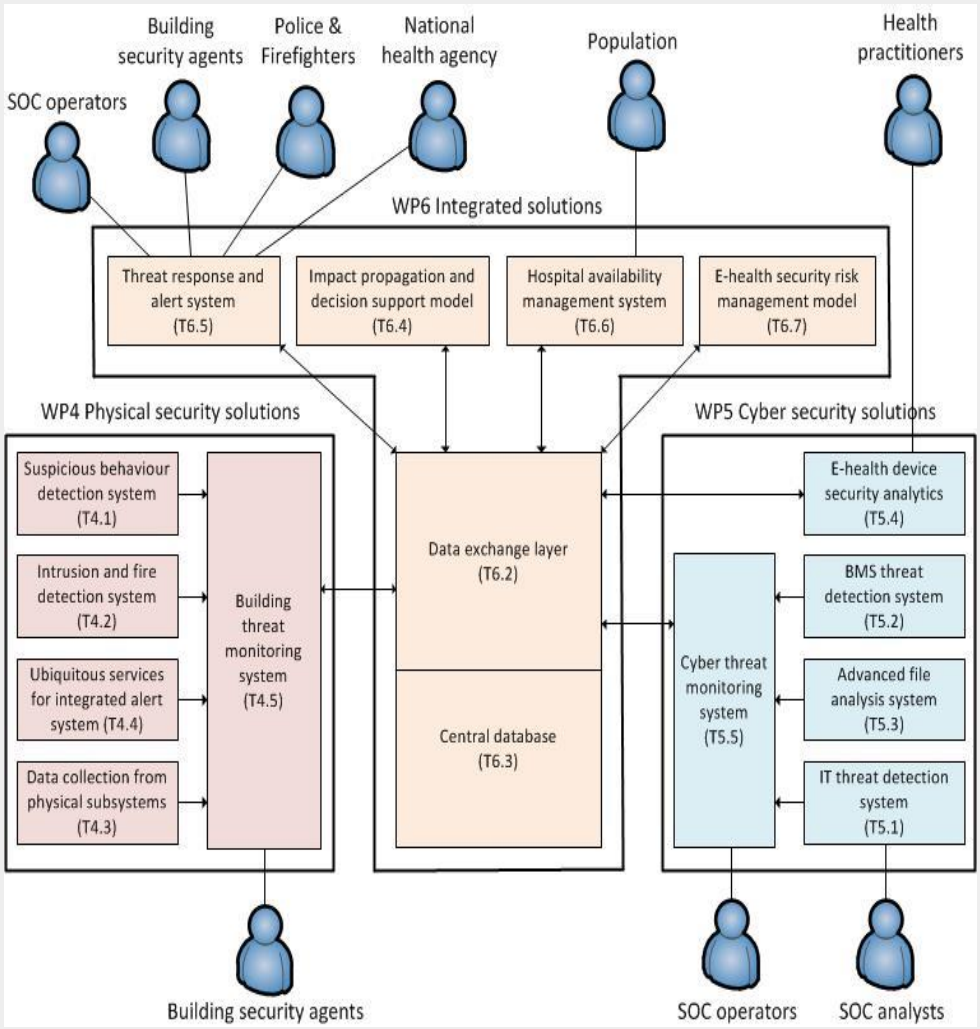
SafeCare coordinator

Philippe Tourron

Project Status

Below is an illustration of the main outcomes of SAFECARE for each Work package. The list of Work Packages and the Global architecture and interconnections are described in the following figures as a reminder.

WP Number	WP Title	Lead beneficiary	Start month	End month
WP1	Ethic requirements	1- AP-HM	1	36
WP2	Project Management	1 – AP-HM	1	36
WP3	Risk assessment and requirements	6 – ISEP	1	36
WP4	Physical security solutions	14 - Milestone	6	26
WP5	Cyber security solutions	2- CCS	6	26
WP6	Integrated cyber-physical security solutions	9 – ISMB	6	26
WP7	Tests and demonstrations	10 – CSI	18	33
WP8	Dissemination, exploitation and standardization	12 – EOS	1	36



Work Package 1

The WP on Ethics requirements was requested by the European Commission in the development phase, before signing the Grant Agreement. With such themes related to the healthcare, it is legitimate and fundamental to raise questions relating to ethics while at the same time, carrying out a risk analysis on privacy for the patients. It aims to consolidate information into deliverables originally planned for another WPs (including consents, responding to GDPR concerns). The consortium has been able to produce the first 3 deliverables of this period. Nevertheless, the partners will have to improve the coordination between themselves in order to facilitate the work to be done under the WP1.

The first approach to the analysis of privacy has been made. The latter is to be completed over the following months in order to take into account the particularities of the tool under construction within the framework of the SAFECARE project. Significant work on authorizations has been done by the entire consortium but the final approval before

demonstration on-site still needs to be obtained. The next deliverable will be the annual report of the Ethics board which is to be prepared by all the partners.

Work Package 2

The Work Package dedicated to Project Management organizes WP Leaders meetings every two weeks to review the status of each WP. At this time, the difficulties and the possible needs for arbitration by the coordinator are reported. In general, it is mainly a question of allowing each WP Leader to access the necessary information in order to best organize the planning of her/his WP and to define interfaces with other WPs. These meetings allow the organization to submit the deliverables as per DoA at the right level of quality and in keeping with the deadlines. They also contribute in the planning of the focus groups and events. 2 deliverables were completed on time (The initial Quality plan and the Financial Report). Some difficulties were experienced for the Financial Report, in terms of recovering the needed information. This point will be taken into consideration for the next financial deliverables.

Work Package 3

WP3 deals with risk analysis and requirements. This WP started working on the first day of project execution with the Kick-off of tasks 3.1 (Identification of critical assets in health infrastructure), 3.3 (Requirement analysis) and 3.6 (Study of ethical and privacy constraints related to the health environment). Up to now, work about critical assets, requirements analysis, SoA of security and know vulnerabilities and ethics, privacy and confidentiality constraints has been delivered. All these tasks are crucial to achieving the SAFECARE project goal to provide solutions that will improve physical and cyber security to prevent attacks, to promote incident responses and mitigate the impacts.

Work Package 4

WP4 concerns physical security solutions and kicked off in February 2019. Current tasks address the specification of functionalities for suspicious behavior detection, intrusion and fire detection, and the mobile service for integrated alerting. The process of collecting information of current provision of, and historical data, from cameras, fire detection devices and access control system is being carried out. The participants are also working on mapping out how the systems will interact, both within the physical security systems scope, and within the larger integration (WP6), in collaboration with WP5 on cybersecurity. A task on the building threat monitoring system, which is the basis of interaction with the rest of the architecture, will start in April 2019, and data collection from ICS, SCADA and smart building sensors will start in May 2019.

Work Package 5

The WP5 about Cyber security solutions has officially started in February 2019 during the Focus Group in Turin in January 2019.

The task T5.4 started in February 2019, with the objectives to provide a device security analytics solution. The task is led by Philips and its main contributors are CSI, Enovacom, AMC, Airbus and KU Leuven. First a specification of the e-health devices security analytics will be delivered, then the prototype will be achieved.

All other WP5 tasks will start in May 2019

Work Package 6

The WP6 about Integrated cyber-physical security solutions has just started at M6. The contributors of this WP will meet every 2 weeks for periodic calls in order to contribute to the development and achievement of the main objectives of this WP as the realization of :

- The central database
- A communication system between modules developed in other WPs
- Models for impact propagation and cascading effects
- Software modules for improving the availability and security of health services

Work Package 7

N/A (The WP7 about Tests and demonstrations will start at M18)

Work Package 8

The WP8 (Dissemination, exploitation and standardization D8.1) started at M1. The first deliverable of the project, the Dissemination and Communication strategy, has been submitted at M3 (and will be updated at M13). The implementation of the strategy will be carried out under the T8.2 and several activities are already in place :

- Web presence (SAFECARE Website)
- Social media presence (SAFECARE Project LinkedIn and SAFECARE Twitter)
- Material design for flyers
- Events participation (see below)
- Events organization (such as the Focus Groups and the first awareness event)
- Newsletters

Past and Upcoming Events

- 19/10/2018 : Presentation of SAFECARE at the conference *Forum biomedical « l'Avenir de l'e-sante »,* in Marseille (France) by AP-HM
- 24-25/10/2018 : Networking for SAFECARE at the *,Internet of things security conference*, in The Haag (The Netherlands) by BEIA
- 24/10/2018 : Networking for SAFECARE at the *European Brokerage Event on Resilience from disaster*, in Paris (France) by BEIA
- 11/2018: Presentation of SAFECARE at the *European Cyber Week (ECW),* in Rennes (France) by Airbus
- 14/11/2018: Networking for SAFECARE at the *4th eHealth Security Workshop,* in Rotterdam (The Netherlands) by ISEP
- 5-6/12/2018: Networking at the *Security Research Event,* in Brussels (Belgium) by EOS and ISEP
- 6/12/2018 : Presentation of SAFECARE at the SAYSO 2nd Public Workshop, in Brussels (Belgium) by EOS and KEMEA
- 15-16/01/2019: First Focus Group, in Marseille (France) with all the partners
- 23/01/2019 : Presentation of SAFECARE at the *International Security forum (FIC) :* « Are SCADAs and cyber-physical systems 'unsecure' by design ? » in Lille (France) by AP-HM (Please see the link of the conference)
- 29-30/01/2019 : Second Focus Group, in Turin (Italy) with all the partners
- 25-24/02/2019 : Presentation of SAFECARE at the *Milestone Integration Platform Sysmposium* (MIPS), in Nashville (US) by Milestone
- 18/03/2019: Presentation of SAFECARE at the *Evènement national H2020 Sécurité des Infrastructures Critiques* in Paris (France) by AP-HM and Airbus
- 25-27/03/2019 : Presentation of SAFECARE at MIPS EMEA, Copenhagen, (Denmark) by Milestone
- 2-5/04/2019: Presentation of SAFECARE at MIPS APAC, in Bali (Indonesia) by Milestone

Twitter Website

Annex 6 – References

Deliverable 2.4 – Submitted at M3

EU Grants: H2020 AGA — Annotated Model Grant Agreement – ARTICLE 19 – Submission of Deliverables

Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fifth Edition