

SOCIAL

Sovereign Citizen Alliance – SOCIAL

Information Security for SME and SMO

Low-threshold Information and Introduction to CISIS12 ISMS

Output document of the Erasmus+ project
“SOCIAL – Sovereign Citizen Alliance”



Co-funded by
the European Union



This document was produced as part of the Erasmus+ project:

"Sovereign Citizen Alliance – SOCIAL"

Project Partners:



Betriebswirtschaftliches Forschungszentrum für
Fragen der mittelständischen Wirtschaft e.V.

Betriebswirtschaftliches Forschungszentrum für Fragen
der mittelständischen Wirtschaft e. V. an der Universität
Bayreuth
(*Business Research Center for Small and Medium-Sized
Enterprises e. V. at the University of Bayreuth*),
Germany

<https://www.bfm-bayreuth.de>



IT-Sicherheitscluster e. V.,
Germany

<https://www.it-sicherheitscluster.de>



MYKOLO ROMERIO UNIVERSITETAS,
Lithuania

<https://www.mruni.eu>

This document is licensed under CC BY-SA 4.0.

This document was produced as part of the ERASMUS+ project "Sovereign Citizen Alliance – SOCIAL", Project ID: 2021-2-DE02-KA210-VET-000051512

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Table of contents

The SOCIAL Project – “Sovereign Citizen Alliance”	2
Information Security – Awareness and Low Threshold Information.....	4
Introduction to CISIS12 ISMS.....	5

The SOCIAL Project – “Sovereign Citizen Alliance”

The SOCIAL project was carried out in the period from 01.05.2022 to 31.12.2023 as part of the Erasmus+ Small Scale Partnerships. SOCIAL was an international project with three project partners from Germany (BF/M and IT Security Cluster) and Lithuania (MRU).

The SOCIAL projects strived to facilitate European citizens in responsibly participating in digital environments. The project sets out the steps of awareness rising for security threats, the facilitation to secure compliance of individual rights in the digital space and, finally, the realization of true sovereignty - the execution of ownership, responsibility and independence in the digital world.

The project was implemented through two Activities. “Activity 1 – Roundtables: Information Security in Education” focused on the fact that education and training are the most important angles to unlock competences necessary for digital sovereignty. Therefore, information exchange and knowledge transfer lay at the heart of this project. The first activity establishes common grounds on the status quo of information security awareness among citizens from the member countries. Two roundtables focussed on the information exchange and discussions of security awareness in low-threshold environments were organised with experts in information security and education.

Meanwhile “Activity 2 Internationalization: Information Security Management Systems in SMEs and SMOs” entails the transfer of existing tools, which support especially SMEs and SMOs to develop information security competences. Results were presented on a workshop in Vilnius (Lithuania) to SME and SMO with the topics: “CISIS12 and Information Security in SMEs” and “From theory to practice: Application of Information Security”.



Figure 1: Impression from Workshop in Lithuania on 15.03.2023 “CISIS12 and Information Security in SMEs”.

The project provided important insights necessary for the development of a larger application. By broadening the perspective of information security education and training to the realm of citizenship, the project aims to transfer findings from the education of personnel within SMEs into a wider reality. To the end of establishing new focal points, the exchange and transfer of knowledge and existing tools were conducted and evaluated.

The concrete results were recommendations for information security awareness and corresponding low threshold information were developed (see following chapter) and the information security management system (ISMS) CISIS12 of the IT Security Cluster from Germany was presented (see last chapter of this document). As a result



of the workshop in Lithuania, the CISIS12 derivative (CISA50plus) was developed and published within the frame of SOCIAL.

A significant part of the work in SOCIAL has been driven by the conviction that a comprehensive Information Security Management System (ISMS) is the functionally most effective approach to improving information security in small and medium-sized enterprises (SMEs). However, this thesis must be measured against the means available to organizations. In the context of the SOCIAL project, this thesis was falsified.

As planned in the project outline, the workshop in Lithuania aimed to gather initial experiences with the CISIS12 ISMS. However, the workshop revealed that the bar for implementation was set too high. To bridge the gap between the necessity (implementation of an ISMS) and the actual feasibility for SMEs, a lower-threshold tool was proposed and abstracted. This tool allows SMEs to gain initial experience in information security management. This tool is named CISA50plus.

The technical term for such an instrument is 'Assessment'. An assessment is characterized by bringing together a set of components but not requiring the cyclic practice of certification, audits, surveillance audits, and recertification mechanisms. The assessment serves as a tool for determining the status quo of an organization. However, with CISA50plus, a recurring question-and-answer process can also be initiated and practiced. The assessment consists of 50 questions covering the areas of organization, technology, and legal issues. These questions address the essential information security aspects of small to medium-sized organizations. The answers to the questions can be documented. By repeating the survey cyclically, progress can be assessed based on the scoring. The quality level regarding information security maturity can be inferred from the maturity levels associated with each question relative to the answer.

This mechanism also serves as a means of continuous improvement and the assessment can be continually adapted to new circumstances and different environments. However, it is generic in many approaches, allowing for fairly open areas of application. More specific approaches can be created, for example, by domain-specific extension of the question catalog. Theoretically, the CISA50plus system could also be verified for conformity by an independent auditing authority and equipped with a quality certificate. Experiences with the predecessor model, ISA+ Information Security Analysis by the IT-Sicherheitscluster e. V., provide insights in this regard.

CISA50plus is published in a second SOCIAL output document.



Information Security

– Awareness and Low Threshold Information

Next to technological aspects the most effective way to improve information security in an organisation is to focus on human resources. Employees are often the main gateway for information security incidents. But expert knowledge in information security is faced with the dilemma of an information bubble. It is difficult to reach employees outside of this bubble with low threshold offers.

Based on expert input from the organised Roundtables the SOCIAL project can recommend:

- to improve Information Security Awareness and
- to establish low threshold offers about Information Security.

For successful implementation in practice, it is important to be aware of the following:

- employees are individual and are afraid to ask questions or report problems because of the feeling of shame
- technological developments are progressing very quickly, the main topics change completely every 2-3 years

To overcome these barriers following assistance can be provided:

- offer low-threshold access to information and communication,
- activities should be continuous and updated regularly,
- activities should improve risk awareness and instinct for risk-conscious behaviour,
- use hybrid approaches consisting of awareness measures, learning environments, playful approaches such as gamification, face-to-face meetings and personal exchange,
- related staff for the activities should be authentic and committed to build trust and patience,
- in an organization, the understanding of information security must always be communicated and exemplified by the top management level,
- activities should include the whole staff,
- use storytelling with real incident problems, make personal mistakes visible to overcome shame of employees to open for questions and problems,
- awareness should not be limited on working, private life is also relevant.

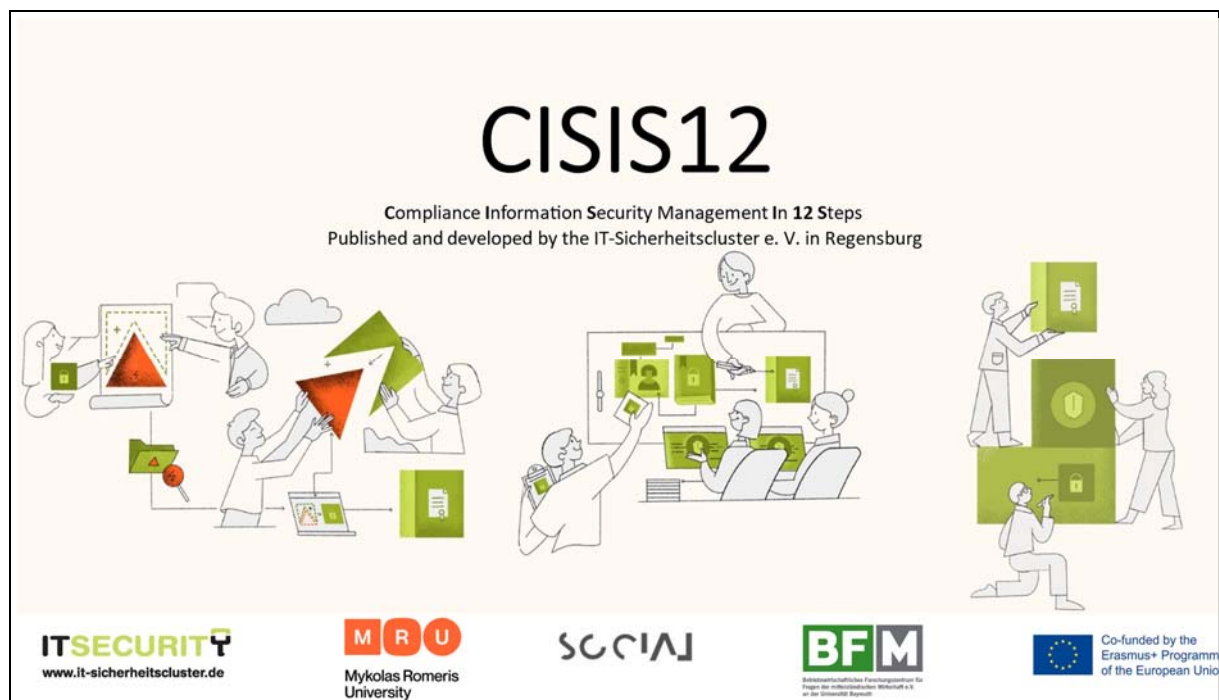
Introduction to CISIS12 ISMS

To gain digital sovereignty, it seemed to be necessary to practice information security, which includes IT security, in a managed way. Using a circular practiced system with clear steps is a considered solution to increase all the goals described above. An ISMS is a structured, recurring, certifiable and thus legally based procedure in which awareness is conveyed and an entire organization (and not just IT) is integrated into a steering procedure/process through recurring actions and far-reaching documentation. This must be planned carefully. Through the practices taught/developed in this process, an organization achieves sovereignty over all its information-relevant areas. Therefore, it fits directly into the project objectives of SOCIAL.

On the workshop in Lithuania the SOCIAL project team introduced in the first lecture “CISIS12 and Information Security in SMEs” the Information Security Management System (ISMS) “CISIS12 - **C**ompliance **I**nformation **S**ecurity Management **I**n **12** **S**teps“ developed by the German project partner IT-Sicherheitscluster e.V. with insights in:

1. Some thoughts about Cybersecurity, Information Security, IT-Security
2. CISIS12: An overview of the structure, design and steps of implementation

The following slides are from the first presentation on the workshop.



The slide features the title "CISIS12" in large black font, with the subtitle "Compliance Information Security Management In 12 Steps" and "Published and developed by the IT-Sicherheitscluster e. V. in Regensburg" below it. The central illustration shows three groups of people interacting with various digital and physical security-related icons like a warning triangle, a laptop, a smartphone, and a server rack. At the bottom, there are five logos: ITSECURITY (www.it-sicherheitscluster.de), MRU (Mykolas Romeris University), SOCIAL, BFM (Bismarck-Forschungsinstitut für Management und Wirtschaft), and the European Union logo with the text "Co-funded by the Erasmus+ Programm of the European Union".



Overview

1. Some thoughts about Cybersecurity, Information Security, IT-Security
2. CISIS12: An overview of the structure, design and steps of implementation



Information Security

Why we not (only) talk about IT- and/or Cybersecurity

Information security covers both IT-/Cybersecurity as well as all aspects of information in an organisation.

Examples: Papers on your desktop, name plates on doors, dumpsters and their content... They are in need of protection.



Information security affects all parts of an organisation.





How about Security?

Drowning by Numbers – What is happening out there?
And what more to say?

116,6 million more software «products» which where malware appeared in Germany in between 2021 to 2022.

An attack on satellites caused a failure of a central wind turbine control system.



Q3 of 2021: 322.168 Dollar ransom money was paid.

The first digital disaster case lasted 207 days (regional administration/authority) was affected.

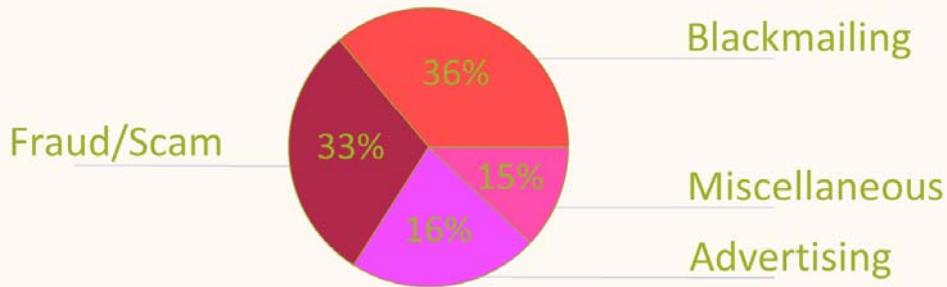
20.174 vulnerabilities in software products were found in 2021. Share of critical vulnerabilities 13 per cent.

Reference: BSI Annual report 2022 <https://www.bsi.bund.de/>



Sad, sad E-Mail Systems

The proportion of various types of spam in 2021-2022



Reference: BSI Annual report 2022



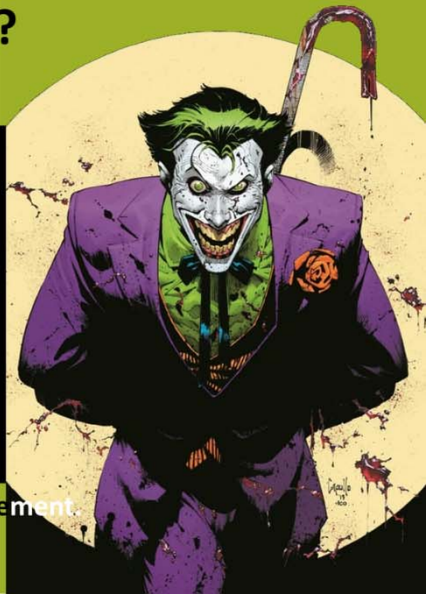


Q: What makes the Joker laughing?

A: The Horror of the Triple «P»

PPP

Missing or bad Password policies,
Phishing in all "flavours",
Poor or non-existent Patch management



How about Awareness?

What are Germany's SME's are doing to prevent cybercrime?

Last year, 22 per cent of German companies laid off staff from the IT security department.

Only a mere third of German companies see cyber attacks as the most important challenge for 2023.

→ 53 per cent of German companies have experienced one serious incident in the past year.

Reference: ArcticWolf 2022
<https://arcticwolf.com>





So what are We Talking About?

Reference: ArcticWolf 2022
<https://arcticwolf.com>


 Mykolas Romeris University
 

 Co-funded by the Erasmus+ Programme of the European Union



Information Security






And how we think we can improve it

Where to start?
Think of your organisation as a **whole entity**. Buzz word: **holistic!**
Every employer counts.

In every direction: From top to bottom and back

The human factor **[i. e. your employees]** is not the enemy.
The enemies are **persons who commit cybercrime**.
Learning is not only understanding but also training.
There are **many regulatory frameworks** outside on market.
Take the one which **fits into your needs**.

 Follow KISS: Keep it simple and stupid!


 Mykolas Romeris University
 

 Co-funded by the Erasmus+ Programme of the European Union



CISIS12 – A Systematic Approach to Increase Security

Information Security Management System (ISMS)

A management system (like for instance the ISO-9001 but for IT- and information security).

Follows a circular principle: PDCA – Plan Do Check Act

Follows the principle of continuous improvement

Step-by-step procedure model



CISIS12 – Documents plus Software

The Components



Manual



Standard (definitions, rules, descriptions)



Measures





Compliance The "C" in CISIS12

CISIS12 follows processes not devices to be compliant

- Compliance should regard internal and external guidelines
- The perspective takes leadership as well as technologies and buildings into account to increase the degree of information security
- CISIS12 integrates process levels with system levels
- All requirements follow PDCA cycle and should be documented (Plan-Do-Check-Act)



About CISIS12

10 years on the market.

Version 3 was published 2021/1/6

CISIS12 places the focus on

- Risk-management,
- Compliance and pending processes.
- CISIS12 has a structured set up: standard, measures plus audit scheme.
- Is upgradable and transparent to higher standards such as the ISO/IEC 27001 family.
- Integrates into domain specific standards and catalogues, such as vTISAX, B3S-KRITIS.
- Ready to implement in small and medium enterprises and administrations!
- Supplemented with a manual, and a training concept for users and consultants.
- Different software products exist to accompany the implementation process, which include GDPR module or a DMS.





Project planning: Kick off

Thoughts before you start with CISIS12

- CISIS12 needs project management.
- Plannings in detail must be factual and limited to the departments affected and should always be based on contexts of the organisation.
- It is recommended to be supported by a software tool.
- Calculate not only in terms of revenue or return on invest.
- An ISMS costs money and seems not to appear with a positive value in your books. As long as nothing happens.
- There's wisdom in the phrase that it is not a question of if, but when your organisation will become a victim of cybercrime.
- **An ISMS does not guarantee that you will not be affected by cyber criminals!**



Preliminaries

Start with a statement of work/terms of reference written by the contracting authority (consultant) and the project leader. It should comprise:

- Project's contracting authority,
- Project leader, Members of the project team,
- Project coach (external advisor),
- Project start and project finish date,
- Project objectives,
- Demarcation concerning non-project objectives,
- Project phases,
- Project resources and costs,
- Signatures of the project's contracting authority and of the project leader.

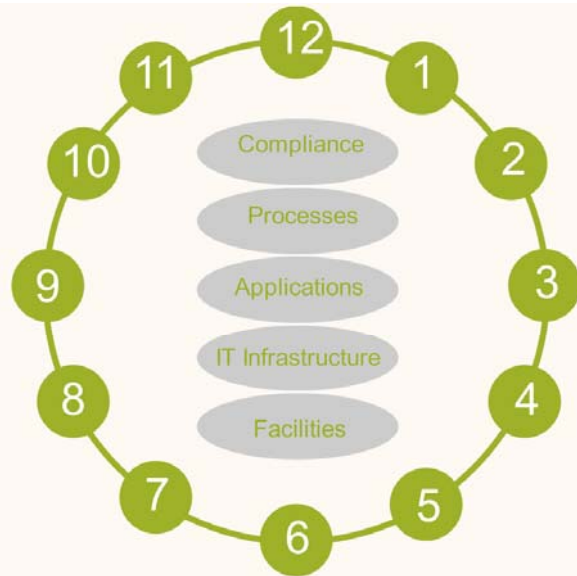




Before you start

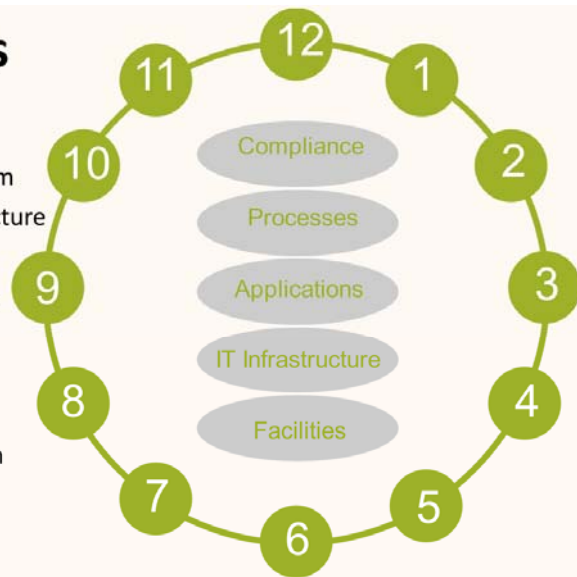
You should have determined and recorded

- The persons and roles:
 - Information security officer (ISO),
 - Data protection officer (DPO),
- Members of the ISMS project core team and of the extended ISMS project team.
- The objectives are (examples)
 - Developing and establishing of an ISMS with CISIS12 within X months,
 - Sustainable training and awareness raising of the employees and senior management,
 - Identifying of IT service management processes and their sustainable safeguarding,
 - Passing the certification audit.



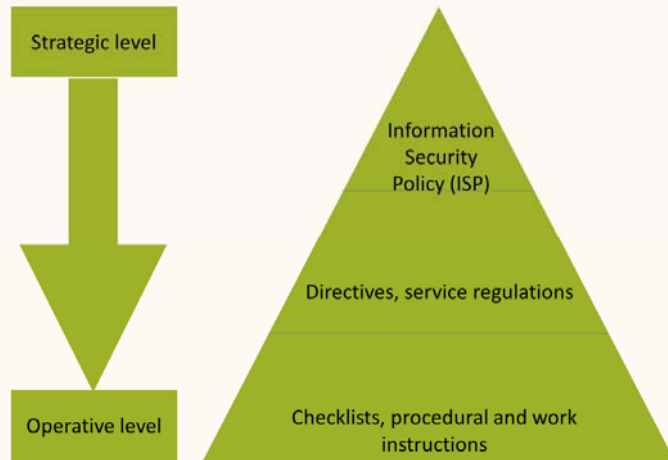
Lift off: The Twelve Steps

- Step 1 – Drawing up a Policy
- Step 2 – Raising Awareness of Employees
- Step 3 – Establishing an Information Security Team
- Step 4 – Determining the IT Documentation Structure
- Step 5 – IT-Service Management Processes
- Step 6 – Compliance, Processes and Applications
- Step 7 – Analysing the IT Structure
- Step 8 – Risk Management
- Step 9 – Target Actual Comparison
- Step 10 – Planning and Executing Implementation
- Step 11 – Internal Audit
- Step 12 – Review



Step 1 – Drawing up a Policy

- The commitment of the organisation's management as to adopt the full responsibility for information security,
- The definition of scope,
- The link between business objectives and information security objectives,
- The significance of information security,
- A guiding principle for implementing and monitoring success,
- The organisational structure for implementing the ISMS process.



Step 2 – Awareness

- Within SOCIAL we tried to find out how awareness works.
- Without active participation plus intrinsic motivation and identification awareness will not be successful.
- All employees within the scope must be addressed.
- This also entails that
 - all relevant stakeholders (senior staff, employees, external partners) are familiar with the essential documents on information security (policy and further relevant directives, service regulations, checklists, procedural and work instructions),
 - impacts of non-compliance of information security regulations are known, including possible sanctioning,
 - training and awareness-raising activities are prepared in a target-group-oriented manner, while considering risk potentials specific to the organisation,
 - the contribution of each individual employee within the scope to the effectiveness of the information security regulations is made clear and possibly evidenced via tests, regular exercises on information security are executed.



Step 3 – Documentation

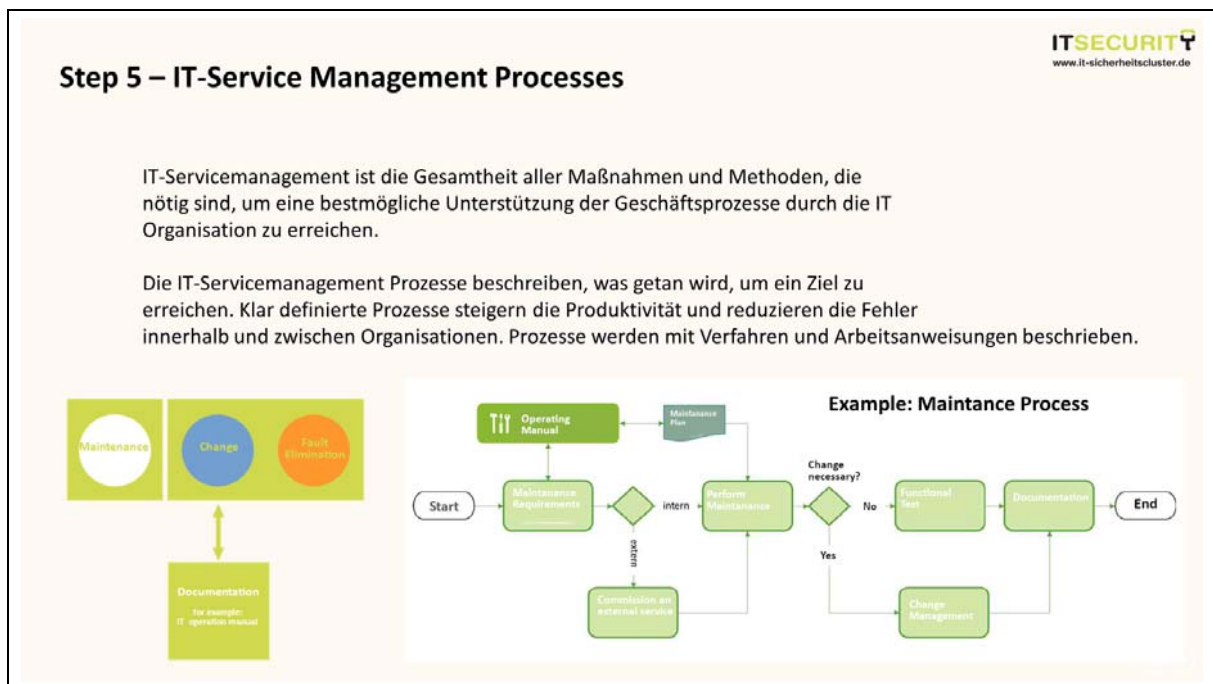
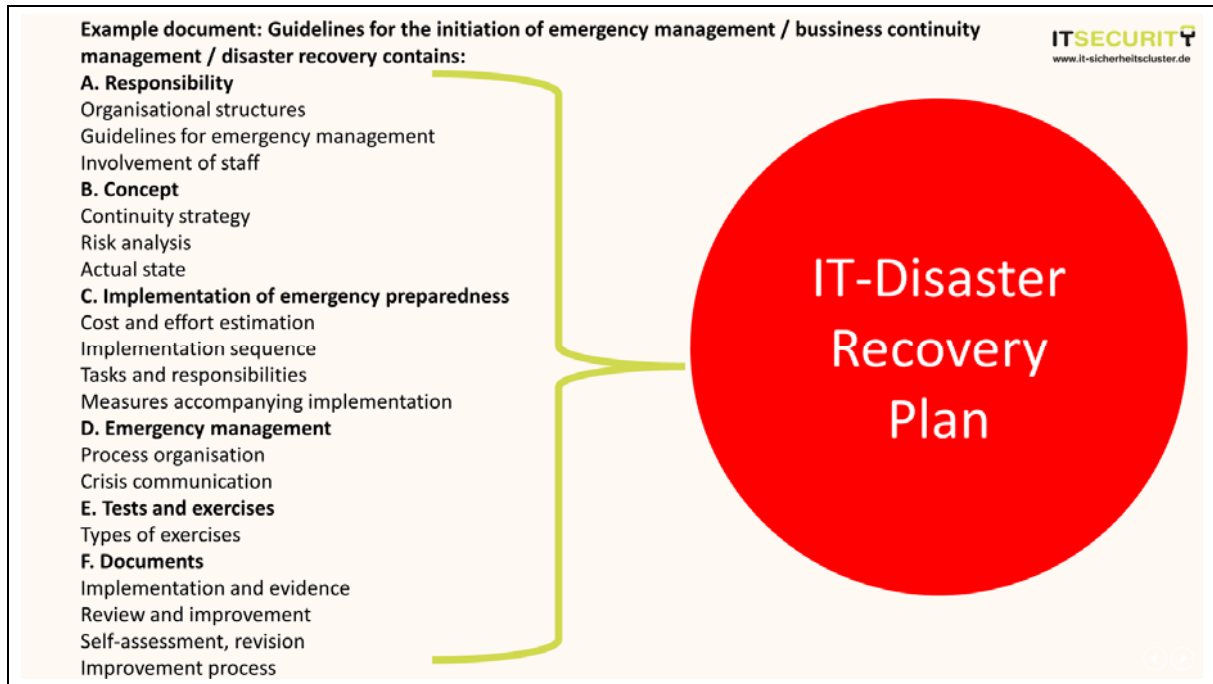
- Information Security Policy (ISP),
- Training and awareness-raising concept,
- Appointing ISO, DPO and IS team,
- Operations Manual (OM),
- Precedence diagram (adjusted),
- Business Continuity Manual (BCM),
- IT Service Management Manual (IT SMM),
- Process profiles, Security Requirement Analysis (SRA),
- Security concept, Implementation plan,
- Management report,
- Revision including internal audit report and perhaps external audit report,
- Guideline on risk management and Risk response plan.



Step 4: Determining the IT Documentation Structure

1. information security guideline,
2. training and awareness-raising concept,
3. documents regarding role designation and ISMS team,
4. IT operations manual (core document for all processes, confidential, assets, system files, infrastructure, cleansed network plan, documentation of all faults, etc., documentation of licences, rights, configurations, hardware, OS),
5. IT emergency manual, (BCM, all names, processes, responsibilities to restore operations as quickly as possible; confidential, paper and digital).
6. IT service management manual,
7. process descriptions,
8. protection needs assessment,
9. system specifications regarding the infrastructures,
10. security concept,
11. implementation plan (measures, costs, scheduling, goals, training, implementation, opportunities and risks),
12. management report including the audit report of the internal audit. 13,
13. audit (if applicable with audit report of the certification audit).

Documents should be provided with metadata so that their status is clear. This includes name, date, version number, revision number, status (draft, release, etc.), class (protection requirement, confidential, secret, public, etc.), person responsible, releasing authority in the organisation).





Step 6 – Compliance, Processes and Applications

Levels of Protection

CISIS12 defines three levels of protection requirements:

- A: Limited/manageable damage impact,
- B: Significant damage impact,
- C: Existential, threatening or catastrophic damage impact.

Concretisation of the damage impact in protection requirement scenarios:

- Violation of applicable law and concluded contracts.
- Data protection: Impairment of the right to informational self-determination.
- Financial effects.
- Negative internal and external effects.
- Restriction of room for manoeuvre, impairment of task fulfilment.

Protection requirements are identified (interviews), documented, formalised (templates), then determined by organisational management.

Example: How high is the protection need of an e-mail application in a farming business in relation to a helpdesk?

How high may the MTDL (maximum tolerable data loss) be? Or MTD (maximum tolerable downtime)? Backup/emergency management!

Governance, Compliance

Governance means something like "organisational constitution" and Compliance, on the other hand, means roughly "observance, adherence, compliance, observance".

When talking about governance and compliance, the boundaries are often blurred in terms of content, because there are no uniform definitions.

The area of compliance also deals with laws and regulations that govern the course of all organisational processes.

For this reason, it is difficult to distinguish between compliance and corporate governance. terms are often used synonymously.



Step 7 – Analysing the IT Structure

List of all IT systems, network connections, and buildings.

Recording of networked as well as non-networked IT systems and non-IT systems: IT assets, hardware/software and building assets: buildings, rooms.

An asset includes:

- Name,
- Description,
- Platform (hardware, OS etc.),
- Person responsible,
- Quantity,
- level of protection,
- building blocks, critical applications.

Derivation of the protection requirement (S)

Maximum principle: S is derived from the maximum of running applications.

Accumulation effect: S can be higher than the highest application, if several applications are run on one server.

Distribution effect: S can be lower than Max. if redundancy is given. Only with regard to availability.



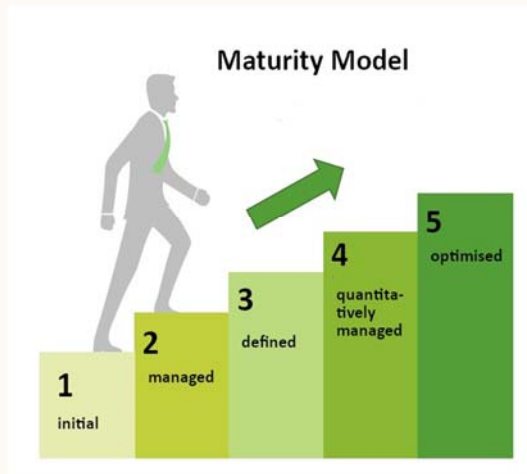
Step 9 – Risk Management

- **Introduction of a risk management process because**
- with structured ISMS processes, comprehensible results can be achieved in risk assessment and
- comprehensible results can be achieved in risk assessment and evaluation,
- the starting point can simplify "mission-critical core processes" and their downstream "critical applications",
- the risk treatment and associated measures are to be developed and implemented on the basis of solid, comprehensible decision-making criteria,
- to provide the information basis for necessary documentation of results (management reports, internal audits, auditing, certification).

A risk is the possibility of deviating from planned target values resulting from an unforeseeable future caused by random disturbances.



Step 9 – Target-Actual Comparison



Compliance/Conformity

Effectiveness

Degree of target achievement, Maturity level

Efficiency

Profitability

Define KPI. Develop metrics appropriately. What are key success factors (KSF)? To be honest? Does the state with the plans and the objectives in the project planning?

Step 10 – Planning and Executing Implementation

Measures are analysed in terms of costs for their realisation.

Measures are prioritised and presented to the management for release of the required resources as a basis for decision-making.

Preparation of an implementation plan.



Step 11 – Internal Audit

- Audits are an important instrument for proving or checking conformity, i.e. compliance with the specifications contained in the standard or defined in internal guidelines.
- According to ISO 19011, an audit is a systematic, independent and documented process. Audit evidence and its objective evaluation allow to determine whether previously defined audit criteria are fulfilled or not.
- The internal audit serves as a tool for identifying potential for improvement. In an internal audit, the responsibility lies with the organisation itself.
- In practice, this means that an auditor or a team of auditors uses various techniques, mainly audit discussions (interviews with ISMS stakeholders) and review of documents and records.
- stakeholders) and reviewing documents and records to verify that the ISMS is designed and effectively implemented in accordance with the requirements of CISIS12.
- Nomen est omen: The team conducts the audit itself.
- Objectives: Are the internal requirements for the ISMS met? Are there quality deviations? What can be improved?
- There must be a programme for this.
- Standards/guidelines are taken into account.
- Organisational management directs, guides and is responsible for the objectives.
- Scope is determined by organisational size.
- Scope is determined by the type, complexity, maturity ... of the ISMS.

Step 12 – Revision

- Through the regular audits, statements can be made about their effective implementation, completeness, adequacy and the current state of information security.
- The audit is thus a necessary tool for determining, achieving and maintaining an appropriate level of security in an organisation and is to be presented in the annual report.
- An audit can only provide a snapshot of the degree/maturity level of the implemented information security management system and assesses the ISMS at a specific point in time.



Step 13 – Audit

Audit and certificate

- A successful Certification is proof that the implementation has been carried out successfully.
- Auditing of implementation of CISIS12 is always done externally: independently, impartially. Prevents operational blindness.

Advantages

- Customers look at an organisation that is learning to deal with hazards.
- Liability risks are reduced.
- Compliance requirements are met.
- Legislative requirements are met.
- Customer requirements are met.
- In the case of incidents, the burden of proof can be shifted.
- Insurance or loans may be possible at better conditions.
- Acquisition of fundings is facilitated.

Process

- Organisation submits application.
- Approved auditor checks on site according to certification scheme.
- Certification body examines the audit report and issues the CISIS12 certificate after a positive result.



Thank you very much for your attention

Contact

IT-Sicherheitscluster e. V.
Dr. Matthias Kampmann
Franz-Mayer-Strasse 1
D-93053 Regensburg

matthias.kampmann@it-sicherheitscluster.de
<https://cisis12.de>
<https://www.it-sicherheitscluster.de>



We thank the co-authors from:

BF/M-Bayreuth

IT-Security Cluster

Mykolas Romeris University

Sovereign Citizen Alliance - SOCIAL

Co-funded by the European Union



**Co-funded by
the European Union**



SOCIAL