Charter of Trust

Guideline on Cybersecurity Risk Assessment

Publication date: 16 February 2024

Charter of Trust – Principle 3
Classification CoT Public

Summary

On February 16, 2018, at the Munich Security Conference, the cornerstone for the Charter of Trust (CoT) was laid to make the digital world more secure. A continuously growing group of multinational companies has signed off on this cybersecurity initiative by endorsing its 10 fundamental principles, which foster three important objectives:

- To protect the data of individuals and companies
- To prevent damage to people, companies, and infrastructures
- To create a reliable foundation on which confidence in a networked, digital world can take root and grow.

The Charter of Trust is a non-profit alliance of leading global companies and organisations working across sectors to make the digital world of tomorrow a safer place. It was founded in 2018 at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape.

A unique initiative underpinned by 10 principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen global cybersecurity posture and provides expertise on topics including AI, security by default, supply chain security, and education. This guideline is a Charter of Trust publication from the principle taskforce on Security by Default.

The Security by Default Taskforce: our activities

One of the key fundamental principles of CoT – Security by Default (Principle 3 Taskforce) –

has worked on the following:

- Phase 1 (Products, Functionalities, Technologies)- baseline security requirements and explanatory document
- Phase 2 (Processes, Operations, Architectures) - baseline security requirements and explanatory document
- Phase 3 (Sharing of Best Practices for Security by Default adoption) - Secure Development Lifecycle: step-by-step guidelines, Risk Assessment guidelines

Objective of the document (O)

This document highlights the significance of caution and due diligence in relation to cyber risks when processes and value chains are supported by digital technology to improve efficiency. As digitalization progresses, such risks exist in products which are combined to systems and networks in the IT but also in the OT world. Though such risks are examined in this document, it should be acknowledged that any kind of risk, if it materializes, will in most cases have a financial and business impact, which can be addressed separately.

The intent of this document is to provide a brief guide to risk assessment. It is not an additional guide, but rather offers practical guidance based on the experience and expertise of the members of the Charter of Trust P3 Task Force.

Charter of Trust

Target audience

The Risk Assessment document aims to provide guidance to current Charter of Trust members, prospective Charter of Trust members and other stakeholders who wish to adopt a cybersecurity Risk Assessment approach in their Security by Default strategies.

Charter of Trust

Content

Introduction

At first glance, Security by Default and Risk Assessment seems to be a contradiction in terms: Why should a Risk Assessment be necessary, if all security by default baseline requirements are fulfilled by appropriate measurements?

There is a good case for conducting a Risk Assessment in many situations, at least at a high-level, and even as a first step:

- An initial risk assessment can confirm that the baseline security measures are sufficient to achieve the intended security level.
- A Risk Assessment can identify areas where these security baseline measures are not sufficient and additional measures are required. These may be areas that are not under the direct control of an organization, such as suppliers or cloud service providers.
- A Risk Assessment should also provide categories of risk levels, so that measurements can be adjusted to the level required making protection more efficient and effective.
- A Risk Assessment can confirm compliance with standards and regulatory requirements.
- A Risk Assessment can provide crucial information on the urgency of action needed, such as in response to newly identified vulnerabilities.

A risk assessment is a necessary step to identify the risks, determine the impact of the considered events on the scope of the risk assessment, and then decide how the risk should be managed.

General benefits of performing a Risk Assessment are listed below:

- Support stakeholders with risk-based decisions
- Create awareness within the organization about the risk exposure
- Reduce cost of data breaches through appropriate risk treatment
- Comply with regulation and avoid legal and regulatory issues
- Prioritize and optimize budgets for cyber security
- Optimize resources based on risk.

This document aims to offer a concise manual for conducting risk assessments. It does not seek to add to the numerous existing guidelines but instead provides pragmatic advice based on the skills and know-how of the Charter of Trust P3 Task Force members.

1. Understanding Risk Assessment Objectives and Scope

1.1 What are the objectives for the risk assessment?

The primary aim of adopting a risk-based strategy is to ascertain the right balance between the cost of protection and the expected loss (also known as 'economic cybersecurity'). The approach may vary depending on whether you are dealing with critical infrastructure, medical devices and pharmaceuticals, nuclear operations, for example, or 'just' day-to-day business.

When performing risk assessments, one must consider several existing dimensions. For instance, when we evaluate risk from a cybersecurity incident concerning an individual asset requires consideration of traditional objectives of protection, namely confidentiality, integrity, and availability, collectively referred to as the CIA-triad. A CVSS (Common Vulnerability Scoring System) score commonly classifies vulnerabilities. The severity score of a vulnerability is determined by factors, such as its impact on the confidentiality, integrity, and availability of the vulnerable system and any subsequent systems that may be affected.

Another aspect to consider in Risk Assessment is the broader impact of exploiting vulnerabilities on the entire organization. The disclosure of confidential information or the loss of integrity of an individual asset may well have a greater impact on the organisation than the impact on the individual asset. Likewise, the availability of individual assets may have a significant impact on the continuity of the organisation’s operations.

On an organizational level cyber security risk may impact the following key areas within an organization:

Financial:

- Loss of revenue if major processes to operate the organization are unavailable
- Cost for remediation of a cyber security incident
- Increased insurance cost
- Impact on stock market price
- Contractual penalties
- Quality/reputation loss (followed by lost market shares etc.)

Legal and regulatory

- Fines for not meeting regulatory requirements
- Legislative penalties
- Prosecution of an individual based on reckless exposure to risk

General well-being

- Safety including loss of human life
- Loss of availability of critical infrastructure

Organisations mission

- Impact on business continuity of disruptive cyber security incidents
- Industrial espionage and theft of trade secrets
- Reputational impact is related to perception by customers, suppliers, and the general public

1.2 What are the benefits of a risk assessment?

Data breaches can pose a considerable financial strain on organisations, causing harm to their corporate image and leading to direct financial losses. Consequently, organisations strive to strike a balance between the cost of security measures taken to avert breaches, the potential expenditures linked to a data breach, and insurance. This necessitates conducting risk assessments, which aid in the process of decision-making that is based on risk.

Conducting a Risk Assessment can serve as evidence to regulators that a proper analysis has been carried out before a risk is formally accepted by the responsible stakeholders.

An instance where risk assessments prove integral in the realm of "Security by Default" pertains to vulnerability management. The quantity of identified vulnerabilities is substantial. Year after year, over 20,000 vulnerabilities are detected in open-source components, with more than 60% being of high or critical severity. It is not cost-effective to fix all vulnerabilities, and often not feasible in terms of resources, as tracking and remediation demand significant resources. CISA has developed a Stakeholder-Specific Vulnerability Categorization that takes into consideration additional factors that characterize the risk of an identified vulnerability like:

- the evidence for the exploitation of vulnerabilities
- the possibility that exploitation can be automated
- the technical impact of the vulnerability on an asset
- the impact on the mission of the organization or the well-being

This can enhance vulnerability management, regardless of whether you are a vendor or responsible for securely operating assets in your organisation.

Additionally, conducting cybersecurity risk analyses is a crucial component of recent cybersecurity regulations like the European Cyber Resilience Act (CRA)[1] for product cybersecurity or the NIS2 Directive[2] for cybersecure IT infrastructures.

1.3 What is (typically) in scope for a Risk Assessment?

Currently, the predominant method for determining the risk level in cyber risk assessments is through a qualitative approach whereby subject matter experts provide informed estimations of the risk level. This approach serves as the foundation for subsequent explanations. While there are developments aimed at replacing the expert estimations with quantification, this paper does not explore this avenue any further.

Before you can start a meaningful risk analysis, the following things should be clearly defined:

- Target of evaluation (TOE) that means a system consisting of software, hardware, processes, policies etc. and its boundaries which are the subject of the Risk Assessment (i.e., the WHAT)
- Operational environment of the TOE according to its foreseen use (i.e., the WHERE)
- Security objective(s) i.e., the high-level security needs for the TOE and its cyber-critical assets to protect it against potential cybersecurity threats (i.e., the WHY)

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

A cybersecurity risk assessment includes all things that can have an impact on the security objectives of the target of evaluation within its operational environment i.e.:

- Technology such as system architecture, interfaces, connections, core of trust, system environment, etc.
- Lifecycle processes such as development process & tools, production, (default) setup, maintenance, third-party integration, guidelines, information sharing, phase-out etc.
- Organization/People such as cybersecurity management, secure supply chain, cybersecurity roles, trainings, audits, security intelligence, cybersecurity governance etc.

For a meaningful risk analysis, the following should be identified where possible:

- Potential misuse cases and possible adverse actions at TOE attack surface
- Threat actors (aka attackers) including their potential skills and intentions.

1.4 What is (typically) out of scope for a Risk Assessment?

- All things that have no or negligible impacts (if directly assessable) on the cybersecurity of the target of evaluation (e.g., temperature, not part of any damage scenarios)
- All components that already come with a (trustworthy) risk assessment (e.g., cybersecurity certificate)
- All components and procedures that come with given assumptions about their cybersecurity risks (e.g., “trusted third party”)

**Note: not an exhaustive list of topics in- and out of scope but rather an illustrative list*

2. Conducting Comprehensive Risk Assessments: Roles, Timing, Methods, and Standards

2.1 Who is involved in a Risk Assessment?

Cybersecurity risk arises not only by the operation and maintenance of the asset owner (own organization), but also by the development process of the integrator commissioned by asset owner. Management vulnerabilities by process owners can also be a cybersecurity risk.

Cybersecurity risk can also be created by organisations that cannot be directly controlled, such as product suppliers, cloud service providers, and open source foundations.

Thus, Risk Assessment is important for organisations to proactively conduct risk assessments, recognize cybersecurity risks, and implement "Security by Default". And Risk Assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders with cybersecurity experts.

A Risk Assessment is the first step in meeting stakeholders' expectations and gaining their trust.

Who performs this activity?

- Cybersecurity experts: knowing the methodology and procedures to execute a cybersecurity risk analysis combined with comprehensive knowledge about the (asset-specific) threat and vulnerability landscape (e.g., recent attacks, attackers, attack paths, weaknesses, vulnerabilities etc.).
- Asset owner: understanding the values and potential impacts of owned products and systems if they become affected by a cybersecurity incident. If necessary, the Risk Assessment results should be drawn up in cooperation with the relevant regulatory authorities.
- System integrator: understanding the cybersecurity risks involved in the lifecycle processes of the systems delivered to the customer. If necessary, the assessment results are explained to the customer and approved.
- Service provider, product supplier: understanding cybersecurity risks as a component from a supply chain perspective.
- Process Owner: Understanding every risk, including cybersecurity, and comprehending the purpose of the business to enhance their own business processes related to IT operations and product development.

Who will the stakeholders be?

- Enterprise Executives (business owner): It is necessary to make good management decisions as the leader of an organization.
- Regulatory authorities, Incident Response Organization: It is necessary to promote measures to maintain the safety and security of society.
- Operators of Customer: It is necessary to isolate and address whether the system failure is a failure or a cyberattack.

- Consumer: It is necessary to properly update their software to avoid becoming victims and perpetrators of cyberattacks.
- Other Risk Assessment departments such as Health, Safety, and Environment: It is necessary to integrate cybersecurity and HSE risks and promote measures to reduce risks to levels acceptable to the organization.

2.2 When is it appropriate to consider a risk assessment?

If the initial risk assessment identifies a “Security by Default” approach and confirms that the intended level of security can be achieved based on standards and regulatory requirements, the initial assessment may change as development and operations progress through the lifecycle. Moreover, external modifications, including the sudden discovery of a critical vulnerability in applications, can also impact the assessment. Therefore, the Risk Assessment should continuously verify compliance with Security by Default protocols, industry standards and regulatory requirements under the following circumstances:

- Design of new systems/products development
- Final implementation/release of new systems/products development (esp. if where have been changes/updates towards the original design)
- (Obligatory) conformity assessment
- Updating, change or retrofitting of the systems/products/operating environment/intended or foreseeable use/underlying assumptions etc.
- Phase-out of the systems/products
- Upon discovery of a security incident or vulnerability
- Periodically in the operation and maintenance phase (ex. once a year)

2.3 Examples of risk assessments and when to choose which one?

There are several risk assessment approaches available, including quantitative, qualitative, asset-based, vulnerability-based, and threat-based methods. Each method evaluates an organization's risk posture with specific trade-offs:

- Quantitative
  Quantitative methods provide a rigorous analytical approach to risk assessment, assigning dollar values to assets and risks. Nevertheless, some risks may prove to be challenging to quantify fully, and imposing a numerical structure on them can jeopardize the objectivity of the evaluation.
- Qualitative
  Qualitative methods involve the “educated guess” from employees across the organization to understand the potential impact on respective processes if a system where to go offline. The information gathered is used to categorize risks into broad categories such as High, Medium, or Low.
- Asset-Based
  Asset-based approaches to risk assessment are preferred as they are aligned with the structure, operations, and culture of IT departments. The risks and controls of assets like firewalls are relatively straightforward to comprehend. However, these approaches may not yield comprehensive risk assessments as certain risks that are not part of the information infrastructure, such as policies, processes and other 'soft' factors, are not captured.
- Vulnerability-Based
  Vulnerability-based methodologies broaden the scope of risk assessments beyond just the

organization's assets. They begin with an analysis of known weaknesses and deficiencies in organizational systems or their operating environments. Potential threats that could exploit these vulnerabilities and the possible consequences of such exploits are identified. While this approach captures a wider range of risks than an asset-based assessment, it is based on known vulnerabilities and may not encompass all threats an organization may face.

- Threat-Based

  Threat-based methodologies provide a more comprehensive assessment of an organisation's overall risk posture by evaluating the conditions that create risk based on known threats, including an audit of assets and their controls. These approaches take into account the techniques used by threat actors.

All methods have their own strengths and weaknesses, and none is perfect. Yet, they are not mutually exclusive and can be combined in risk assessments. The techniques selected for the Risk Assessment procedure will be based on the specific objectives and the nature of the organisation.

2.4 How to perform a risk assessment?

A comprehensive risk assessment must comply with applicable legal and regulatory requirements or industry-specific guidelines. Firstly, it is crucial to determine if any limitations or parameters need to be observed. If such guidelines exist, establish the relevant standards and protocols. If there are no guiding frameworks, it is advisable to consider general recommendations:

- Currently, the prevalent method of assessing cyber risks involves a qualitative approach. This entails subject matter experts offering an informed estimation of the level of risk. According to this approach, "cyber risk" is defined as:
  - Risk = Probability of Occurrence *x* Impact
  - The Probability of Occurrence depends on the severity of Threat and Vulnerability, in other words:
  - Probability of Occurrence = Threat *x* Vulnerability
- These “input values” are defined within the respective Risk Assessment approaches in a detailed way. For further reference please see “Best Practice Industry Standards and Guidelines” below.
- But generally spoken, any Risk Assessment follows the approach below:

1. Define target of evaluation
2. Define security environment (e.g., based on intended/foreseeable use)
3. Define security objectives (e.g., based on misuse cases)
4. Build attack tree (e.g., based on potential attackers and attack paths)
5. For each leaf of the attack tree:
   a. Estimate attack potential (aka ‘probability of occurrence’) based on necessary skills, tools etc.
   b. Estimate damage potential (aka ‘impact’) on finance, operation, safety etc. (cf. ‘Objectives’ section)
   c. Calculate (and classify) resulting cybersecurity risk = AP x DP

2.5 Next steps after Risk Assessment

When assessing risks, it is essential in the risk management process to respond proactively to any identified risks; this constitutes the risk treatment phase.

Risk treatment involves choosing and applying measures to mitigate risk to a level deemed acceptable by the organization. It is crucial to engage the management team in reviewing remaining risks. It should be noted that risk treatment, as a component of risk management, falls under the purview of the management team rather than risk managers.

Risk mitigation measures can comprise various methods that are not necessarily exclusive. The treatment of risks may involve one or more of the following:

- Avoiding the risk
- Taking the risk
- Risk remediation
    - Removing the risk source
    - Changing the likelihood
    - Changing the consequences
- Sharing the risks
- Retaining the risk

Even when risk treatments are carefully planned and executed, they must be reviewed, monitored, and recorded on a regular basis to ensure that they are effective.

2.6 Best Practice Industry Standards and Guidelines

- ISO 310xx series – e.g.
    - ISO 31000 - Risk management — Guidelines
    - IEC 31010 - Risk management – Risk Assessment techniques
- ISO 27005 - Information security risk management
- ISO/IEC 27557 - Application of ISO 31000:2018 for organizational privacy risk management
- ISO/IEC 29134 - Guidelines for privacy impact assessment
- ISO/IEC/IEEE 24765:2017 - Systems and software engineering — Vocabulary
- ISO 23894 – Artificial intelligence — Guidance on risk management
- ISO/IEC9798-3:2019 - IT Security techniques — Entity authentication
- ISO/IEC 24392:2023 Cybersecurity — Security reference model for industrial internet platform (SRM- IIP)
- IEC 62443-1-1:2009 - Terminology, concepts and models
- IEC62443-2-1:2010 - Establishing an industrial automation and control system security program
- IEC62443-2-4:2015 - Security program requirements for IACS service providers
- IEC62443-3-3:2013 - System security requirements and security levels
- IEC 62443-3-2 - Security Risk Assessment for system design – for industrial IT
- ISA-TR84.00.09 - Cybersecurity Related to the Functional Safety Lifecycle – for industrial IT
- SAE/ISO 21434 — Road vehicles — Cybersecurity engineering

- TOGAF 10.0 – Risk Management
- COBIT 2019 – Risk Assessment
- NISTIR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM) with
  - NIST Cybersecurity Framework (CSF)
- NIS2 Directive
- NIST SP 800-30 Rev.1-Guide for Conducting Risk Assessments
- Australian Cyber Security Centre: Guidance on the IRAP assessment process
- Cyber Security Agency of Singapore: GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE
- Information-technology Promotion Agency of Japan: Security Risk Assessment Guide for Industrial Control Systems (Quick Guide)
- European Cyber Resilience Act (CRA)

Selected Charter of Trust documents

- CoT P3 Baseline Requirements (Phase 1 & Phase 2)
- CoT P3 Explanatory documents for Phase 1 & Phase 2
- SDLC Document (Secure Development Lifecycle)
- CoT P2 baseline requirements
- CoT P3 baseline requirements

Glossary

Asset:	Anything that is valuable to an organization or consumer that requires protection against cyber threats. **Relevant Asset Categories:** **Examples of assets that are relevant:** • Digital information • Physical device (networked or standalone) • Supporting software and applications **Examples of assets that are irrelevant:** • Paper-based information • Building without technology
Asset Owner:	Individual or organization responsible for one or more Assets
Baseline Requirements:	Mandatory set of requirements to reach an acceptable level of cybersecurity.
Confidentiality, Integrity, Availability:	**Confidentiality:** • Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information **Integrity:** • Property of protecting the accuracy and completeness of assets **Availability:** • Property of ensuring timely and reliable access to and use of control system information and functionality
Cyber Risk:	"Cyber Risk " includes " Risk"
Disaster:	"Disaster" includes "cybersecurity incidents"
Guidance:	"The act or process of guiding. Direction/Advice/Controlling course."
Guidelines:	"a line by which one is guided à an indication or outline of policy or conduct."
HSE:	**Health, Safety and Environment:** Responsibility for protecting the health and safety of workers and the surrounding community and maintaining high environmental stewardship

Process owner:	Person (or team) responsible for defining and maintaining a process
Risk:	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence
Safety:	Freedom from unacceptable risk
Security Incident/Event:	Event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system
Service Provider:	Individual or organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner
Stakeholder:	Individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services. Stakeholders include the manager of the cyber security program as well as the cross-functional team of individuals from all of the departments affected by the cyber security program.
System Integrator:	person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications.
Testable:	“Capable of being tested.”
Tested:	“Subjected to or qualified through testing.”
Threat & Vulnerability:	**Threat:** • Circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service. **Vulnerability:** • flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise
Trusted Third Party:	Security authority or its agent, trusted by other entities with respect to security related activities
Trustworthiness:	Ability to meet stakeholders’ expectations in a verifiable way
Verifiable:	“Capable of being verified.”

Charter of Trust

The Charter of Trust

Protecting the digital world of tomorrow

About the Charter of Trust

The Charter of Trust is a non-profit alliance of leading global companies and organisations working across sectors to make the digital world of tomorrow a safer place. It was founded in 2018 at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape.

A unique initiative underpinned by 10 principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen global cybersecurity posture and provides expertise on topics including AI, security by default, supply chain security, and education

Objectives

The Charter of Trust seeks to harmonize cybersecurity approaches and address cybersecurity challenges from a holistic, ethical and fair perspective. The alliance is collaborating across industries to cultivate, advocate, and enhance global cybersecurity standards. By fostering widespread awareness and sharing expertise, it ensures a cohesive approach to security that enables seamless global interoperability.

Key principles

The work of the Charter of Trust is underpinned by 10 principles fundamental to a secure digital world:

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Cyber-resilience through conformity and certification
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Contact

contact@charteroftrust.info

Contributors

Frank Semmler, Jill Jenkins - **ATOS SE**

Michael Moore - **Eviden**

Angelika Steinacker - **IBM Corporation**

Daniel Schmitt - **Infineon Technologies AG**

Patricia Eke - **Microsoft Corporation**

Fumikado Anzai, Ki Hyun Park, Dilshod Gulamov - **Mitsubishi Heavy Industries, Ltd.**

Thomas Ben, Christoph Bouly - **NXP Semiconductors N.V.**

Marko Wolf, - **Robert Bosch GmbH**

Oliver Kaiser, Stefan Jost-Dummer - **Siemens AG**

Josef Güntner, Joe Lomako, Sudhir Ethiraj - **TÜV SÜD AG**