ETSI TR 104 117 V1.1.1 (2025-12)

TECHNICAL REPORT

Cyber Security (CYBER);
Risk Management Ecosystem

Reference
DTR/CYBER-00141

Keywords
cybersecurity, risk management

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

ICT Risk Management systems have existed since their inception in various forms of telecommunication and computational systems over the centuries as a means of achieving sufficient levels of security or resilience against threats and vulnerabilities.

The risk management ecosystem basically consists of sets of tools or processes that allow an assessment of security or resilience sufficiency for a particular device or system in a particular context followed by the application of corrective measures.

After the digital network technology evolved significantly in 1964 to bring about merger of telecommunication and computer systems, risk management initiatives almost immediately emerged within the U.S. Federal government as sets of processes. As increasingly complex, open, and autonomous ICT infrastructures and products emerged over the decades, a continuing series of risk management initiatives and tools were developed. After 2010, the threats and complexities increased significantly and resulted in major risk management efforts worldwide. Recently, risk management has been manifested as DevSecOps to encompass the complex risk management iterative cycles of software/product development, operational use, threat discovery, and remediation. After 2020, the European Union integrated risk management into multiple legislative instruments and the activities of EU bodies.

Although cyber risk management largely emerged in the USA Federal government, it spread in cycles to all enterprises and worldwide. As the recent seminal SIPRI study on comparative cyber risk management concludes:

- China, Russia, the USA and the EU exhibit a number of terminological and regulatory similarities, but also differences that merit greater exploration for their impacts on cyber risk reduction.

- While their systems of governance differ, China, the USA and the EU each demonstrate cases of interagency and public–private sector coordination in establishing and implementing their regulatory frameworks in cyberspace. However, they each face challenges when it comes to jurisdictional overlap and clarity of roles, which creates tensions and a need to deconflict these cyber risk reduction initiatives. Among their similarities, China, Russia, the USA and the EU are all integrating regulatory measures to secure their supply chains by vetting, limiting or even prohibiting foreign hardware and software, while seeking to mitigate potential misuse of CII, and personal and government data. Furthermore, all four actors are at varying stages of integrating liability and penalties for non-compliance into their evolving regulations [i.42].

1 Scope

The present document provides an overview of the history and facets of the risk management ecosystem. The overview includes the history of this activity, the concepts and specifications that emerged, the diverse venues, use cases, and the contemporary state-of-the-art mechanisms for meeting imposed obligations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance).

[i.2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[i.3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

[i.4] European Commission: "Risk Management in the Commission, Implementation Guide".

[i.5] NIST: Risk Management History.

[i.6] National Bureau of Standards FIPS 31: "Guidelines for Automatic Data Processing Physical Security and Risk Management (1974)".

[i.7] National Bureau of Standards: "FIPS 41, Computer Security Guidelines for Implementing the Privacy Act of 1974 (1975)".

[i.8] National Bureau of Standards FIPS 65: "Guidelines for Automatic Data Processing Risk Analysis (1979)".

[i.9] RAND: "Security Controls for Computer Systems", February 1970.

[i.10] GovernmentAttic: "Five (5) Defense Science Board (DSB) reports, 1974-1978".

[i.11] MITRE: "Proposed Technical Evaluation Criteria for Trusted Computer Systems." (Nibaldi Report).

[i.12] Common Criteria for Information Technology Security Evaluation.

[i.13] RAND Corp: "RM-3420-PR, On Distributed Communications: Introduction to Distributed Communication Networks", August 1964.

[i.14] AFIPS Proceedings: Bernard Peters: "Security considerations in a multi-programmed computer system", April 1967.

[i.15] IEEE Computer Society, Lipner: "The Birth and Death of the Orange Book", 2015.

[i.16] National Computer Security Conferences (1979-2000).

[i.17] FAS: "NSA/NCSC Rainbow Series".

[i.18] NIST NISTIR 90-4262: "Secure Data Network System (SDNS) Key Management Documents", 1990.

[i.19] National Bureau of Standards FIPS 500-153: "Guide to Auditing for Controls and Security", April 1988.

[i.20] NIST SP 800-12: "An Introduction to Computer Security", October 1995.

[i.21] NIST SP 800-12 Rev.1: "An Introduction to Information Security", June 2017.

[i.22] NIST SP 800-39: "Managing Information Security Risk", March 2011.

[i.23] NIST SP 800-160 Vol. 1: "Engineering Trustworthy Secure Systems", November. 2022.

[i.24] NIST SP 800-60 Rev.2: "Guide for Mapping Types of Information and Systems to Security Categories", January 2024.

[i.25] NIST SP 800-53A Rev.5: "Assessing Security and Privacy Controls in Information Systems and Organizations", January 2022.

[i.26] BlackDuck: "Security Risk Assessment Threat Modelling Best Practices.

[i.27] NIST SP800-37 Rev.2: "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy", December 2018.

[i.28] NIST SP800-137A: "Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment", May 2020.

[i.29] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.30] CIS: "Controls Mapping to NIST SP 800-53".

[i.31] ENISA: Risk Management Standards, March 2022.

[i.32] BSI DIN 27076: Cyber RisikoCheck, May 2023.

[i.33] CIS: Risk Assessment Method 2.0.

[i.34] NCSC: Risk Management, 2.0.

[i.35] ANSSI: EBIOS Risk Manager.

[i.36] NIST SP 800-218: "Secure Software Development Framework (SSDF) Version 1.1", February 2022.

[i.37] NIST SP 1800-44A: "Secure Software Development Security, and Operations (DevSecOps) Practices", July 2025.

[i.38] USDOD: "DevSecOps Continuous Authorization Implementation Guide," March 2024.

[i.39] OWASP: "The OWASP Risk Assessment Framework".

[i.40] U.S. Dept. of Defense: "DevSecOps Fundamentals Guidebook: DevSecOps Tools and Activities", March 2021.

[i.41] NIST AI 100-1: "Artificial Intelligence Risk Management Framework", January 2023.

[i.42] SIPRI: "Cyber Risk Reduction in China, Russia, the United States and the European Union" June 2024.

[i.43] Fair Institute: "FAIR Risk Management".

[i.44] USDOD: "DOD Instruction 8510.01, Risk Management Framework for DOD Systems", July 2022.

[i.45] NIST: "NIST Risk Management Framework (RMF)".

[i.46] ReversingLabs: "Assess & Manage Commercial Software Risk".

[i.47] Wikipedia: "Risk Management Framework".

[i.48] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.49] ETSI TR 103 937: "Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management".

[i.50] centraleyes: "7 Best Cyber Risk Management Platforms of 2024".

[i.51] XM Cyber: "Continuous Threat Exposure Management (CTEM)".

[i.52] NTIA: "Cyber Risk Management (CSCRM)".

[i.53] Cyber Risk Institute: "Cyber Profile for the Financial Sector".

[i.54] Sedona Conference: "The Sedona Conference Commentary on a Reasonable Security Test", The Sedona Conference Journal, Vol 22, 2021.

[i.55] NIST: "Software Security in Supply Chains: Software Bill of Materials (SBOM)", November 2024.

[i.56] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[i.57] Consolidated text: Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (Text with EEA relevance).

[i.58] ENISA: "Cyber Resilience Act implementation via EUCC and its applicable technical elements".

[i.59] CEN/CENELEC: "A Risk-Based Approach to Sectoral Cybersecurity: Introducing EN 18037:2025", 16 April 2025.

[i.60] NSA: "The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment", 16 October 2001.

[i.61] NSA: "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set", May 2001.

[i.62] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.63] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance).

[i.64] ETSI TR 104 034: "Cyber Security (CYBER); Software Bill of Materials (SBOM) Compendium".

[i.65] ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection — Guidance on managing information security risks".

[i.66] ISO/IEC 31000:2018: "Risk management — Guidelines".

[i.67] NIST SP 800-128: "Guide for Security-Focused Configuration Management of Information Systems," October 2019.

[i.68] NIST SP 800-61 Rev.3: "Incident Response Recommendations and Considerations for Cybersecurity Risk Management", April 2025.

[i.69] NIST SP 800-34 Rev.1: "Contingency Planning Guide for Federal Information Systems", March 2023.

[i.70] NSA/CSS: "Cybersecurity Advisories & Guidance".

[i.71] ENISA: "Risk Management".

[i.72] ENISA: "Compendium of Risk Management Frameworks with Potential Interoperability", January 2022.

[i.73] ENISA: "Interoperable EU Risk Management Framework", January 2023.

[i.74] ENISA: "Interoperable EU Risk Management Toolbox", February 2023.

[i.75] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.76] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[i.77] BSI TR-03183-2: "Cyber Resilience Requirements for Manufacturers and Products; Software Bill of Materials (SBOM)", October 2024.

[i.78] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[i.79] US DOD: "Chief Information Officer Library".

[i.80] NIST SP 800-161 Rev.1 Upd.1: "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", January 2024.

[i.81] CISA: "National Risk Management Center Cybersecurity Division".

[i.82] CISA: "Guide to Getting Started with a Cybersecurity Risk Assessment", 2022.

[i.83] CISA: "SBOM Resources Library".

[i.84] NIST SP 1305: "NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)", February 2024.

[i.85] CISA: "A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management", 2023.

[i.86] NIST NISTIR 8376: "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry", February 2021.

[i.87] NSA: "Securing the Software Supply Chain: Recommended Practices Guide for Customers", October 2022.

[i.88] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

risk: any event or issue that could occur and adversely impact the achievement of an organisation's operational or strategic objective

risk management: continuous, proactive and systematic process of identifying, assessing and managing risks in line with the accepted risk levels, carried out at every level of an organisation to provide reasonable assurance

EXAMPLE: Making more reasoned decisions (justifying why certain decisions were taken, what risk factors were considered, etc.); improving efficiency (aligning risk levels and resource and control system allocations); reinforcing the reliability of management systems (ensuring key risks have been taken into consideration and that internal control systems have been adequately reinforced) [i.4].

threat surface: total scope of potential threats that could exploit vulnerabilities within a system or network

NOTE: The SIPRI report on comparative cyber risk management regimes provides a use juxtaposition of terminology [i.42].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AFIPS	American Federation of Information Processing Societies
AI	Artificial Intelligence
ANSSI	Agence nationale de la sécurité des systèmes d'information (FR)
ATO	Authorization To Operate
BSI	Bundesamt für Sicherheit in der Informationstechnik (DE)
CAS	Controls Assessment Specification
cATO	Continuous Authorization To Operate
CBOM	Cybersecurity Bill of Materials
CSCRM	Cyber Security Risk Management
CSS	Central Security Service
DAST	Dynamic Application Security Testing
DSB	Defense Science Board (US)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
HBOM	Hardware Bill of Materials
NBS	National Bureau of Standards (US)
NCSC	National Computer Security Conference (US)
NCSC	National Cyber Security Centre (UK)
NIST	National Institute for Standards and Technology (US)
NSA	National Security Agency (US)
RAF	Risk Assessment Framework
RAM	Risk Assessment Method
RMF	Risk Management Framework

SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SDNS	Secure Data Network System
SIPRI	Stockholm International Peace Research Institute
SNAC	Systems and Network Attack Center

4 History

4.1 Timeline of risk management

The long historical arc of risk management across the past 60 years together with highlights described in subsequent clauses is depicted in Figure 4.1-1. The timeline depicts how risk and its management arose at outset of contemporary cybersecurity with the integration of computer systems and digital networks, followed by recurrent initiatives that increased significantly in scope and diversity after 2005 as the threat surfaces and adverse consequences expanded significantly.

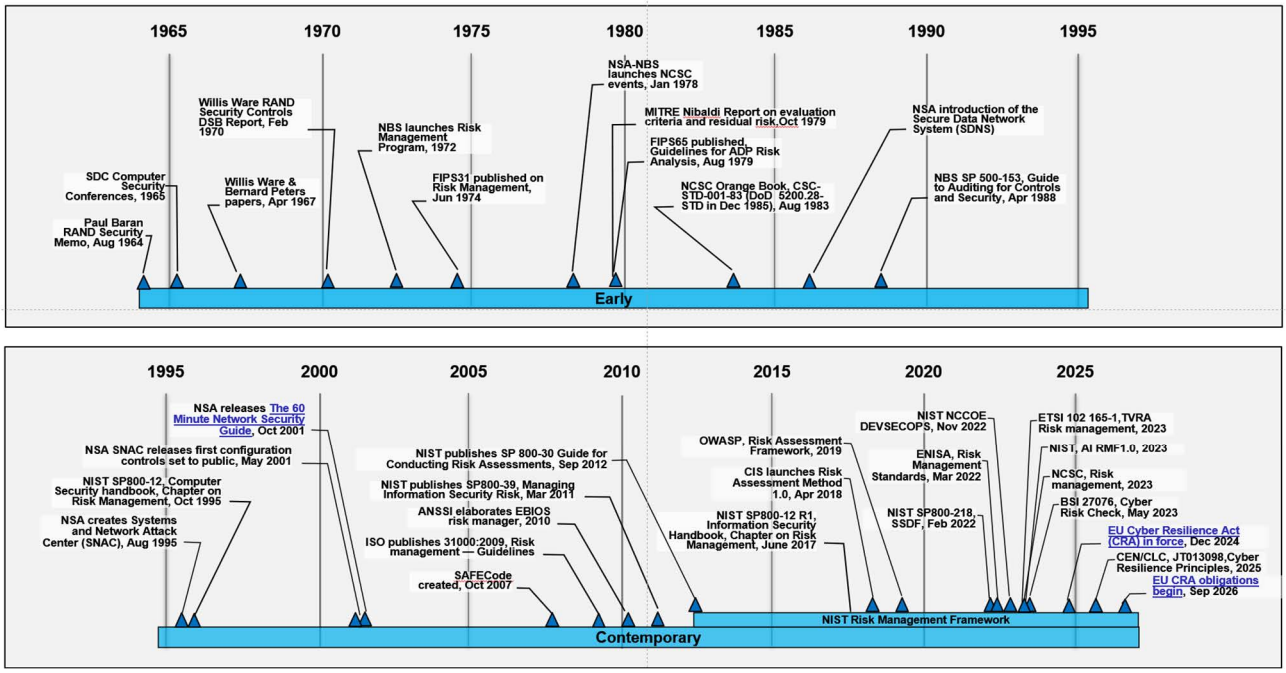

Figure 4.1-1: Risk Management Timeline

It is noted that risk management requires comprehensive risk identification and recent activity in the EU (see CRA [i.1], NIS2 [i.2] and RED [i.63] as examples) require that provision of security measures is "risk based" therefore assumes both risk management and risk identification actions are in place.

4.2 Early period 1940 - 1995

The earliest discussions of risk management in contemporary computer systems and networks appear to have ensued at the RAND Corporation concurrently with its research staff conceptualising packet-based digital networks [i.13]. The next six years witnessed significant studies between RAND and the NSA - resulting in a set of initial papers dealing with risk management at the seminal April 1967 AFIPS [i.14] Atlantic City Conference The five basic tenets were set by NSA's lead computer scientist, Bernard Peters, at the AFIPS Conference:

1) *"security cannot be attained in the absolute sense;*

2) *every security system seeks to attain a probability of loss which is commensurate with the value returned by the operation being secured;*

3) *for each activity which exposes private, valuable, or classified information to possible loss, it is necessary that reasonable steps be taken to reduce the probability of loss;*

4) *any loss which might occur must be detected;*

5) *there are several minimum requirements to establish an adequate security level for the software of a large multi-programmed system with remote terminals."*

The AFIPS Conference was followed by an initial RAND Report to the Defense Science Board in 1970 and underscored Peters basic tenets. That document - often referred to as the Willis Ware Report after its author - identified a set of 29 inherent "computer network vulnerabilities" and set the stage for risk management activities that would follow over subsequent decades [i.9]. The Board served at the time as means for industry collaboration among multiple U.S. national security agencies on evolving risk management challenges [i.10].

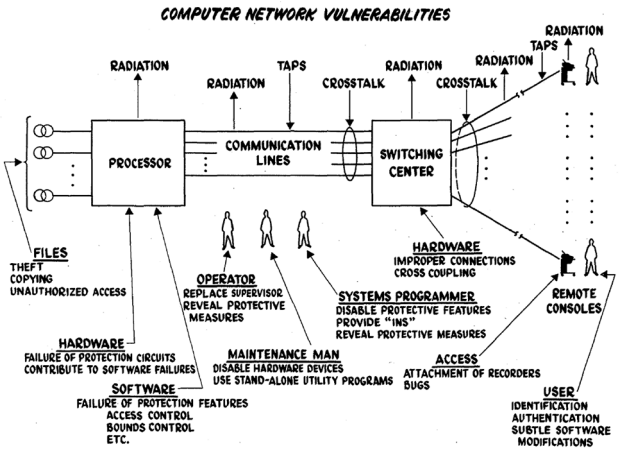

Figure 4.2-1: Ware Computer Network Vulnerabilities [i.9]

In 1972, the US National Bureau of Standards (NBS) launched its Risk Management Program followed by its publication in June 1974 of FIPS 31 guidelines on risk management for computer security [i.6]. FIPS 31 was very comprehensive in addressing most of the identified Ware Report vulnerabilities - consisting of eleven different sets of action ranging from physical security to supporting utilities to envisioning local disasters. It included the conduct of a risk analysis consisting of an estimate of potential losses from different threats, estimating the probability of their occurrence, and remedial measures.

FIPS 41 followed in 1975 and provided a greater level of structure and detailed standards for security risk assessments and safeguard selection, physical security, information management practices, and systems security [i.7]. Security risk assessment included five different categories:

1) accidents, errors, and omissions;

2) risks from uncontrolled system access;

3) risks from authorized users of personal data;

4) risks from the physical environment and from malicious destructive acts;

5) risks from deliberate penetrations.

The next cluster of developments occurred between 1978 and 1983 with the multiple initiatives and increasingly public activities of NSA's National Computer Security Center (NCSC) related to risk management. It published sets of technical reports, guides and standards for secure computer systems that subsequently became known as the Rainbow Series [i.15]. The institution of the National Computer Security Conferences provided a means for broad industry collaboration on risk management initiatives and challenges and vetting a significant number of seminal cybersecurity developments which continue today [i.16].

Among these materials was Grace Hammonds Nibaldi's landmark work in 1979 at MITRE on technical evaluation of trusted computer systems that became known as the Nibaldi Report [i.11]. She proposed a risk management schema with specific measures consisting of six protection levels with the "residual risks" enumerated at every level. In this period, NBS published further guidelines for risk analysis as FIPS 65 in late 1979 [i.8], followed by NSA's NCSC's initial Orange Book [i.17]. The set represents perhaps the most exhaustive set of cybersecurity methods and standards for computer systems and networks ever prepared and remain reflected in almost every cybersecurity activity today.

The subsequent period up until 1995 was marked primarily by NSA undertaking the large-scale Secure Data Network System (SDNS) initiative which has diverse Orange Book risk management methods included in the SDNS standards [i.18], coupled with NBS publication of SP 500-153 [i.19] in 1988 providing detailed risk management auditing and measurement specification [i.19]. SDNS was designed to provide a managed risk public internet infrastructure, protocols and services that became subordinated in the market by TCP/IP based alternatives.

4.3 Contemporary period after 1995

The period from 1995 onwards is primarily marked by extensive introduction of open, autonomous, complex computational systems and networks coupled with an increase of threat surfaces from all manner of vulnerabilities and actors that dramatically increased the challenges of risk management. Perhaps to most seminal event marking this paradigm change was the creation by NSA of the Systems and Network Attack Center (SNAC) in August 1995 known organisationally as C4 [i.60]. SNAC set in motion a considerable array of initiatives and standards that were subsequently explained in 2001 via "The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)" to "better understand how to reduce and manage network security risk" [i.60].

Another action taken via the National Bureau of Standards - newly minted as the National Institute for Standards and Technology (NIST) - was publishing a comprehensive 276-page Computer Security Handbook in 1995 with an entire chapter devoted to risk management [i.20]. SNAC also began addressing threats arising from "Internet-connected systems" together with diverse new practices and mitigations through NSA published critical security control safeguards and configurations [i.61].

Risk management is defined in the 1995 Handbook as "the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk". The basic components of risk management were articulated:

1) undertake a risk assessment;
2) mitigate the risks;
3) analyse the uncertainty;
4) understand control interdependencies;
5) know the costs.

See Figure 4.3-1 below.

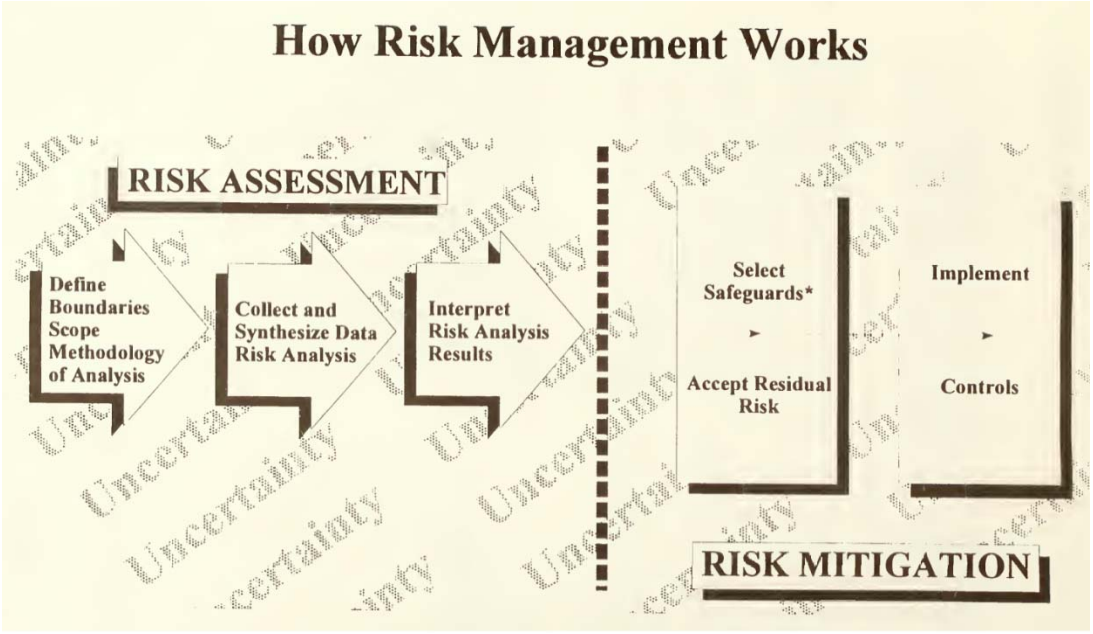

Figure 4.3-1: Risk Management Activities and Processes [i.20]

The comprehensiveness of the SNAC programme and the initial Computer Security Handbook with its articulation of risk management have endured. The Controls were transferred to the Center for Internet Security and transposed into numerous ETSI specifications including the production of a Risk Assessment Method (RAM) with partners [i.29], [i.33], [i.62]. The NIST publication itself was not revised until 2017 and remains the current version with references to multiple, constantly evolving reference materials [i.21]. Over the 1995 - 2010 period, "computer security" terminology transition to "information security."Risk Management was newly articulated as a framework:

1) framing risk;
2) assessing risk;
3) responding to risk; and
4) monitoring risk.

See Figures 4.3-2 and 5.1-1 below.

Figure 4.3-2: NIST SP 800-12 Risk Management Framework [i.21]

The risk management provisions in SP 800-12 Rev 1 [i.20] remain the most comprehensive and exhaustive articulation of risk management today and includes numerous additional publications that are constantly evolving [i.22], [i.28], [i.36], [i.37], [i.41], [i.55], [i.67], [i.68], [i.69], [i.80], [i.84], [i.86] and [i.87]. Noteworthy is that the ETSI Critical Security Controls [i.29] provide an effective set of relevant controls within this framework, and a mapping to NIST SP 800-53A, "Assessing Security and Privacy Controls in Information Systems and Organizations" is available [i.30].

In parallel to much of the above, development of the ISO Common Criteria for Information Technology Security Evaluation [i.12] took steps to unify the security evaluation standards existing at this time: the European ITSEC standard, developed by France, Germany, the Netherlands and the UK; the U.S. TCSEC standard (aka. Orange Book) developed by the United States Department of Defense and the Canadian CTCPEC derived from the TCSEC standard. By unifying security evaluation criteria, the objective was to avoid re-evaluation of products addressing international markets. Common Criteria version 1.0 was issued in 1994. A central theme of Common Criteria is to demonstrate that the security functions deployed adequately meet the risks identified.

In the early 2000s ETSI took its place in the Risk Management arena with a step towards "design for assurance" in which it was identified as necessary to identify risks and to be able to demonstrate that mitigations were adequate. This initiative therefore built on the foundations of SP 800-12, the Critical Security Controls, the Common Criteria and others to develop, first the TVRA method (in ETSI TS 102 165-1 [i.48] in 2003) but to evolve it by application in the development of standards as a framework for risk mitigation.

4.4 Emerging trends: software assurance and expansion of venues

After 2005, the risk management domain became marked by four major trends - a focus on software assurance, the expansion of risk management frameworks in multiple international venues, sector-specific profiles, and diverse legal obligations, especially in EU legislation. As ICT devices became increasingly virtualised with constantly evolving software running on ubiquitous generic networked hardware, software became the principal "threat surface." Sharing the associated risk management burdens became essential.

Multiple national security communities from ranging from NSA and the Rainbow Books in the 1980s to the Common Criteria Control Board in the 1990s, sought to institute improved levels of software assurance as part of risk management frameworks through diverse certification schemes that proved enormously costly and completely ineffective [i.15]. Furthermore, the Common Criteria schemes could not be applied to autonomous, open public information infrastructures where the software was constantly changing.

The establishment of the non-profit SAFECode organisation in 2007 based on the successes of major software vendor initiatives and improvement of increasingly complex code sets marked a turning point in risk management that became the basis for NIST publishing its Secure Software Development Framework (SSDF) [i.36]. The platform has been further integrated into Risk Management via the DevSecOps construct [i.37]. Security is integrated into the core of DevSecOps phases and weaved into the fabric that touches each phase depicted in Figure 4.3-2, above. This integrated and wrapped approach to security facilitates automated risk characterization, monitoring, and risk mitigation across the totality of the application lifecycle. DevSecOps also inherently is entwined with the introduction of emerging Software Bill of Materials requirements [i.38].

The second significant trend was manifested by the increasing globalisation risk management frameworks. NIST instantiated portions of its risk management framework in a set of ISO 31000 series standards in 2009. France's ANSSI published its EBIOS risk manager in 2010 [i.35]. In the past several years, there had been an unending stream of national, regional, and industry cyber risk management guidelines and tools that are treated in clause 5 below. These contemporary risk management materials have also included assessment methods that provide some measurable values to the risk attributes [i.33].

The third significant trend - sector specific risk management - has been notable in multiple industry sectors where there are substantial liability exposures and driven especially by insurance industry efforts to measure risk. A prominent Artificial Intelligence sector Risk Management Framework (AI RMF) appeared in early 2023 that includes an AI RMF Playbook, Roadmap, and Crosswalk [i.41].

The fourth significant trend - legal obligations - is most prominently exemplified in EU legislation. The use of "risk" and "risk-management in the five principal EU cybersecurity legislative enactments after 2021 is shown in Table 4.4-1, below. The EC maintains a risk-management website [i.4] as does the U.S. NTIA a site for Cyber Risk Management (CSCRM) [i.52]. The U.S. DOD has promulgated cyber-risk related procurement requirements [i.44]. The Sedona Conference which sets legal normative standards for adjudications of burden allocation adopted its "reasonable security test" based on risk-management outcomes [i.54].

Table 4.4-1: Risk and Risk-Management in EU Cybersecurity Legislation

Legislative Instrument	Use of "risk"	Use of risk-management
AI Act [i [i.88]	777	3
DORA [i.3]	344	3
NIS2 [i.2]	145	53
CRA [i.1]	179	1
GDPR [i.76]	75	0
RED [i.63]	14	0
eIDAS [i.75]	11	0
EUCC [i.78]	10	25

5 Risk management ecosystem

5.0 The ecosystem ontology

Figure 5.0-1 provides a high-level view of the contemporary Risk Management ecosystem ontology that emerged from the SNAC programme beginning in 1995 - placing the core standards cluster at the centre with five identified derivative groups that provide different profiles of the core provisions.

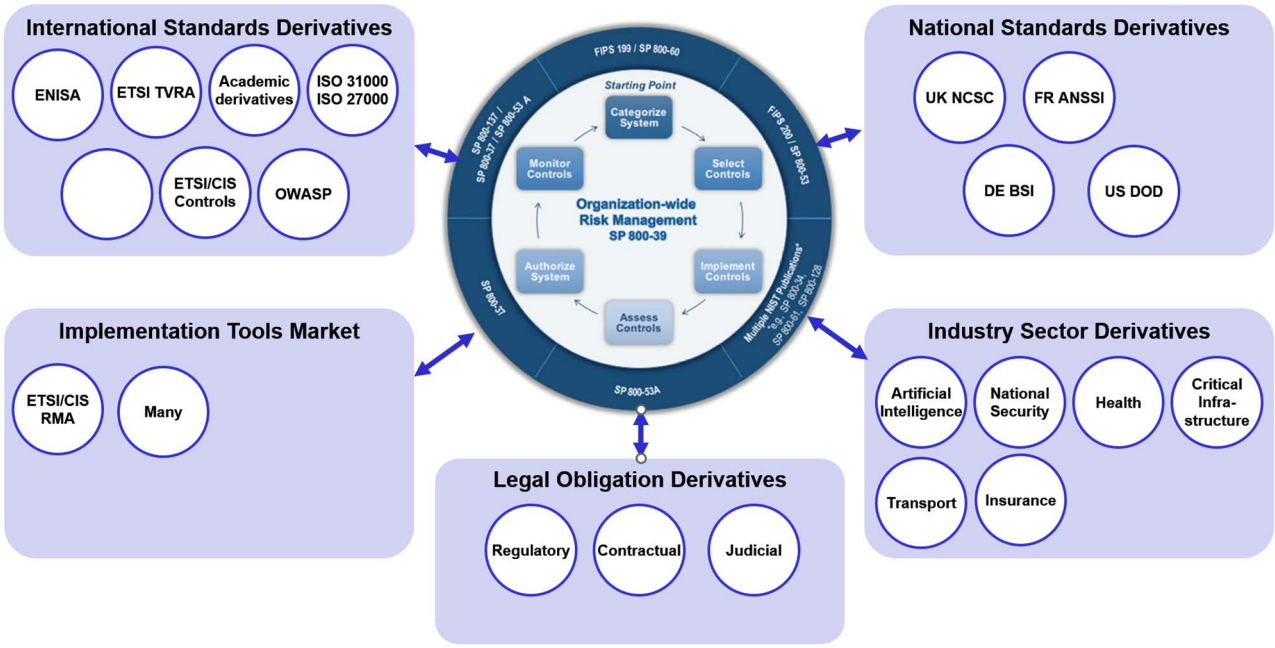

Figure 5.0-1: High-level view of the cyber risk management ecosystem

5.1 Core Risk management process standards

Over several decades, the three basic risk assessment actions and four risk mitigation actions outlined in Figure 4.3-1 above have not changed. All the subsequent treatments by NIST and derivatives in Figure 5.0-1 have simply grouped the actions as processes and then enhanced with treatments of life cycles and bills of material shown in Figure 5.1-1.

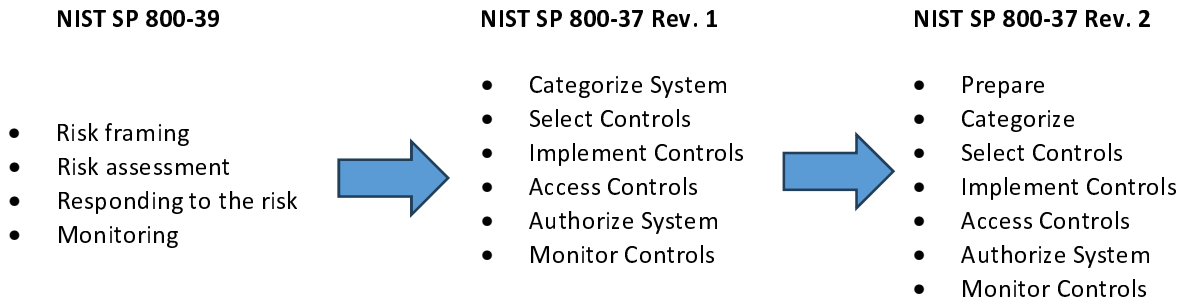

Figure 5.1-1: Core Cyber Risk Management Processes

During the period after 2015, the risk management ecosystem witnessed a focus on a pair of significant idealised dimensions to the core process. One dimension emphasized the cyclical nature of the processes and became known as DevSecOps. The second dimension emphasized in greater detail on identification and analysis of the software components and became known as Software Bill of Materials (SBOM). See Figures 5.1-2 and 5.1-3 below. Actual implementation of SBOM, however, has resulted in several challenges and constraints [i.64].

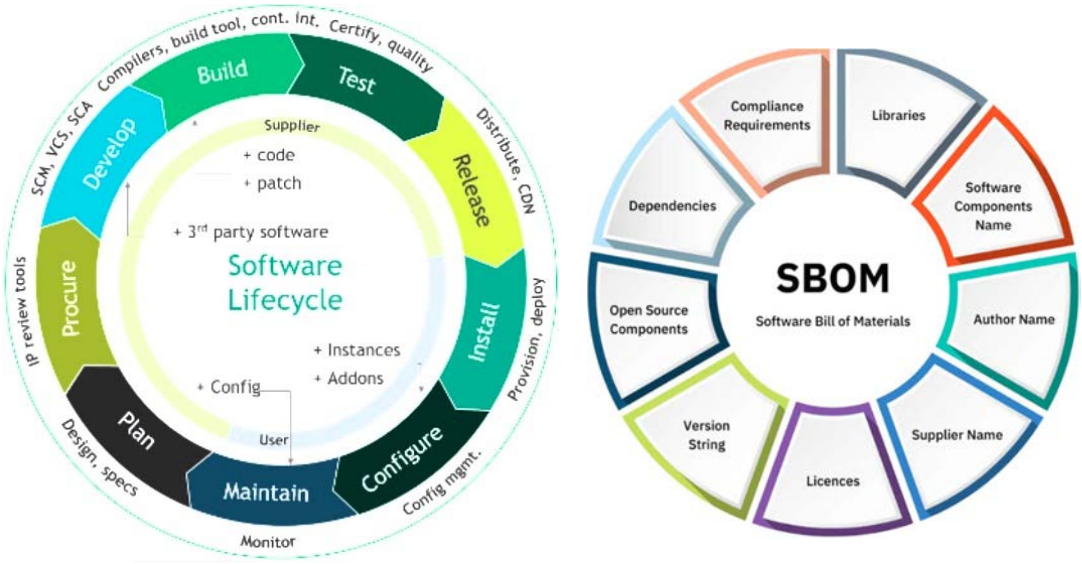

Figure 5.1-2: Additional risk management process dimensions [i.55]

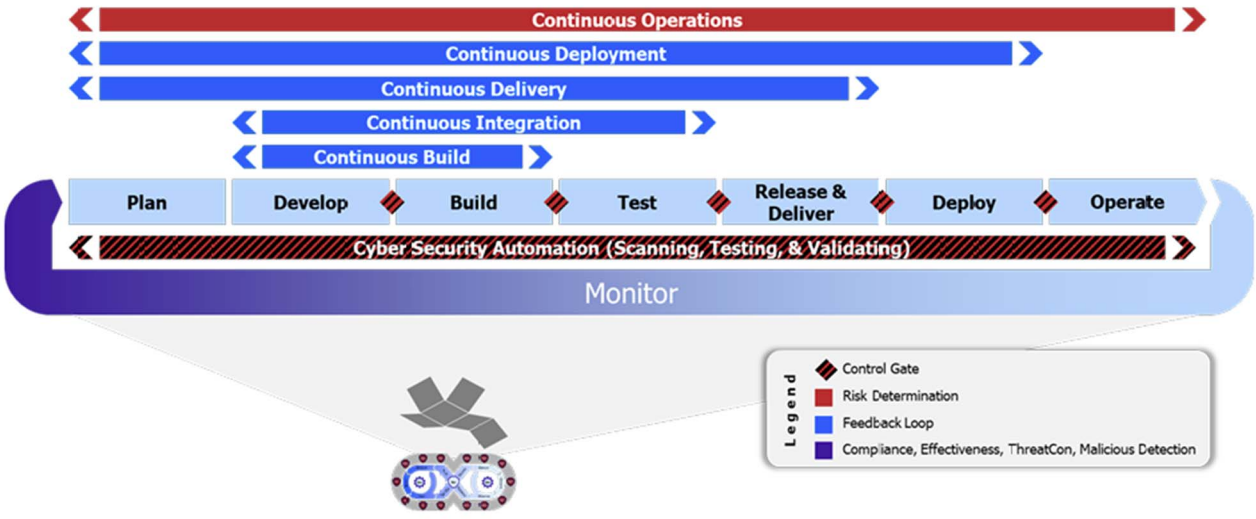

Figure 5.1-3: DevSecOps Phases and Continuous Feedback Loops [i.37]

5.2 Risk management derivative standards clusters

5.2.1 International standards

A considerable array of international standards for risk management have emerged and examples are enumerated below.

NIST/NSA Risk Management Standards, SP 800-39 family [i.22]

The NIST family of *de facto* international risk management standards represent the continuum of NSA SNAC programme joint activity that provide the foundation of all the derivatives and collectively constitute the state of the art. Published in 2011 as a successor to the 1995 risk management handbook, SP-39 consists of a family of specifications that have been continuously updated and expanded and include:

- "NIST Risk Management Framework (RMF)", August 2025 [i.45]. The RMF site provides continuing notice of recent updates.
- NIST SP 800-60 Rev. 2: "Guide for Mapping Types of Information and Systems to Security Categories", January 2024 [i.24].
- NIST SP 800-53A Rev. 5: "Assessing Security and Privacy Controls in Information Systems and Organizations", January 2022 [i.25].
- NIST SP 800-34 Rev.1: "Contingency Planning Guide for Federal Information Systems", March 2023 [i.69].
- NIST SP 800-61 Rev.3: "Incident Response Recommendations and Considerations for Cybersecurity Risk Management", April 2025 [i.68].
- NIST SP 800-128: "Guide for Security-Focused Configuration Management of Information Systems, October 2019 [i.67].
- NIST SP 800-37 Rev.2: "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy", December 2018 [i.27].
- NIST SP 800-137A: "Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment", May 2020 [i.28].
- NIST SP 800-218: "Secure Software Development Framework (SSDF) Version 1.1", February 2022 [i.36].
- NIST SP 1800-44A: "Secure Software Development, Security, and Operations (DevSecOps) Practices", July 2025 [i.37].
- NIST AI 100-1: "Artificial Intelligence Risk Management Framework", January 2023 [i.41].
- NIST SP 800-160 Vol.1: "Engineering Trustworthy Secure Systems", Nov. 2022 [i.23].
- NIST SP 800-161 Rev.1 Upd.1: "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", January 2024 [i.80].
- NIST SP 1800-44A: "Software Security in Supply Chains: Software Bill of Materials (SBOM)", November 2024 [i.55].
- NIST SP 1305: "NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)", February 2024 [i.84].
- NIST NISTIR 8376: "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry", February 2021 [i.86].
- NSA: "Securing the Software Supply Chain: Recommended Practices Guide for Customers", October 2022 [i.87].

The NIST published risk management standards are continuously enhanced and facilitated by NSA/CSS advisories, information sheets, operational risk notices and recommended configurations that are referenced and used by national security agencies globally [i.70].

ETSI TVRA (ETSI TS 102 165-1 [i.48]

This specification newly updated in 2025 in a stepwise evolution since its first publication in 2003 defines a method primarily for use in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system to identify applicable countermeasures. The method described has been tailored to apply to pre-production but can be applied to production devices with due attention given to the possibility that the application of countermeasures may be unachievable for a re-design strategy. The method also builds from the Common Criteria for security assurance and evaluation and may be used to form part of the documentation set for the Target Of Evaluation.

ETSI Cyber Resiliency and Supply Chain Management (ETSI TR 103 937 [i.49]

This technical report was published in 2024 to address the increasing significant attacks on ICT infrastructure that has led to a return to cybersecurity fundamentals developed after the conceptualization of packet data networks to provide access to computer resources. It was a realization that persistent vulnerabilities in every digital element and system will always exist, that "ex ante" trust certifications were minimally useful, and that a different set of tools was necessary. The development of these tools for cyber resiliency proceeded under a broad "Zero Trust Model" aegis that includes Supply chain Bill Of Materials (SBOM), community exchange of vulnerability and remediation code, Continuous Monitoring for threat anomalies, and application of Critical Security Controls. The report is also applicable to the implementation of EU Cyber Resilience Act.

ENISA Risk Management [i.71]

The family of international risk management reports, specifications, and tools are significant components of ENISA's EU cybersecurity mission. The materials are continuously updated and expanded and include:

- ENISA: "Compendium of Risk Management Frameworks with Potential Interoperability", Jan 2022 [i.72]. This report presents the results of desktop research and the analysis of currently used cybersecurity Risk Management (RM) frameworks and methodologies with the potential for interoperability.
- ENISA: "Risk Management Standards", January 2022 [i.31]. The report provides an overview of EU legislation that increasingly refers to risk management, enumerates primarily ISO risk management standards, describes methodologies and tools that can be used to conform with or implement those standards, and makes 15 recommendations directed at EU policy makers, European SDOs, and ENISA itself.
- ENISA: "Interoperable EU Risk Management Framework", January 2023 [i.73]. This report proposes a methodology for assessing the potential interoperability of Risk Management (RM) frameworks and methodologies and presents related results.
- ENISA: "Interoperable EU Risk Management Toolbox", February 2023 [i.74]. This document presents the EU RM toolbox, a solution proposed by ENISA to address interoperability concerns related to the use of information security RM methods.

ISO Risk Management Standards 27005 and 31000 [i.65] and [i.66]

Published in 2022, ISO/IEC 27005 [i.65] provides guidance on managing information security risks to support the implementation of an Information Security Management System (ISMS) based on other ISO/IEC standards. Derived from the NIST standards, it offers a structured approach for identifying, assessing and treating information security risks across all types of organisations. Published in 2018, ISO/IEC 31000 [i.66] also derived from the NIST standards, provides generic principles and guidelines for risk management.

CEN/CENELEC EN 18037:2025 [i.59]

The 2025 specification describes a risk-based approach based on ISO 27000 series standards that could be used in conjunction with the EU Cyber Resilience Act across multiple stakeholder organisations. The utility for CRA requirements per se, however, is unclear because ICT risks related to threats to the availability of the ICT system can typically only be mitigated at ICT system level, not by requirements to dedicated ICT products which is the scope of the CRA. If EN 18037 assessments were carried out for the majority market sectors and application areas of ICT products, the results could be documented, and some of the documentation obligations could be undertaken.

CIS/ETSI Risk Management Controls family

The CIS Critical Security Controls and configuration guides were part of the original NSA/NIST risk management family of specifications and have been subsequently amplified to include platforms for assessing actual control implementations and quantitatively measuring risk. These publications have been directly and indirectly transposed into ETSI Technical Specifications and Reports and include:

- ETSI TS 103 305-1 [i.29]: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence" .
- ETSI TR 103 305-4 [i.62]: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".
- CIS: "Controls Mapping to NIST SP 800-53" [i.30].
- CIS: Risk Assessment Method (RAM) 2.0 [i.33] was developed to provide a structured approach for organizations to identify, analyse, and prioritize risks related to the Critical Security Controls. The latest versions introduced different approaches to support organizations at various implementation levels (IG1, IG2, and IG3). The Controls and RAM are continuously updated and refined through a consensus-based process involving experts from government, industry, and academia that ensures the methods remain relevant and effective in addressing evolving cyber threats.

OWASP Risk Assessment Framework (RAF) [i.39]

The OWASP Risk Assessment Framework (RAF) consists of tools for Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). The OWASP Risk Assessment Framework is a structured methodology for evaluating and prioritizing risks associated with web application vulnerabilities. It uses a two-dimensional approach, assessing both the likelihood of a vulnerability being exploited and the potential impact of such an event. This framework helps organizations understand and address security weaknesses in their web applications by providing a systematic way to analyse and prioritize risks. The Framework consists of five steps:

1) Identify Risks;
2) Assess Likelihood;
3) Assess Impact;
4) Calculate Risk; and
5) Prioritize and Mitigate.

SIPRI Risk Management Report [i.42]

The 2024 report provides an overview of cyber risk reduction terminology and regulatory measures within China, Russia, the United States and the European Union (EU), based on primary source official documents. Cyber risk reduction may be defined as a combination of risk assessment, risk management and mitigation processes, through which risks in cyberspace are identified, evaluated and addressed to reduce harm and negative impacts. This paper offers a foundation to enhance engagement among the four actors on cyber risk reduction.

5.2.2 National standards

A considerable array of national standards for risk management have emerged. Prominent examples are enumerated below.

UK NCSC Risk Management Guidance [i.34]

The 2023 guidance website provides a comprehensive 14-part compendium of topics and actions for cyber security risk practitioners to help their organisations understand and make decisions in this area. It is also helpful to those setting up a cyber security risk management functions in their organisation for the first time or looking to improve existing functions.

Germany BSI Risk Management Publications

Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI) has produced a set of risk management publications:

- BSI DIN 27076: "CyberRisikoCheck", May 2023 [i.32].
- BSI Standard 200-3: "Risk Analysis based on IT-Grundschutz", Version. 1, Oct 2017 [i.78]. The standard provides a structured approach for organizations to identify, assess, and manage information security risks. The IT-Grundschutz framework is a comprehensive methodology for establishing and maintaining an Information Security Management System (ISMS). The updated version is based on a simplified hazard model that combines the former 450 specific hazards into 46 elementary, product and technology-neutral hazards.
- BSI TR-0318 3-2: "Cyber Resilience Requirements for Manufacturers and Products; Software Bill of Materials (SBOM)", October 2024 [i.77]. TR-0318 3-2 facilitates risk assessments encompassing knowledge of software components.

France Agence nationale de la sécurité des systèmes d'information ANSSI Risk Management Tools [i.35]

In November 2019, ANSSI published the web site based EBIOS Risk Manager as method for assessing and treating digital risks. It provides a toolbox that can be adapted, of which the use varies according to the objective of the project. EBIOS Risk Manager is compatible with the reference standards in effect, in terms of risk management as well as in terms of cybersecurity. In addition to the EBIOS Risk Manager guide, "method sheets" have been created to help users conduct each workshop described in the guide. The platform is evolved with the assistance of the Club EBIOS organisation.

US Department of Defense Risk Management Framework

The US DOD has initiated a number of Risk Management related programmes together with implementing specifications [i.79]. In July 2022, it published "DOD Instruction 8510.01, Risk Management Framework for DOD Systems" [i.44]. The 2022 publication updated a 2014 version and established a life-cycle approach with 7 steps found in NIST SP 800-37 Revision. 2 [i.27].

In March 2021, the DOD further published "DevSecOps Fundamentals Guidebook: DevSecOps Tools and Activities" [i.40] that further implements the SP 800-37 Revision. 2 discussing risk tolerance levels and including the establishment of a software lifecycle within the pipeline that uses management processes that meets the unique needs of the mission environment, system complexity, system architecture, software design choices, risk tolerance level, and system maturity level.

The Guidebook was further updated in March 2024 with the "DevSecOps Continuous Authorization Implementation Guide" [i.38] which introduced the DevSecOps cATO (continuous Authorization to Operate) evaluation criteria [i.79]. Risk Management Frameworks (RMF) establish the continuous management of system cybersecurity risk. Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached. cATO attempts to emphasize the continuous monitoring step of RMF. It embraces real-time or near real-time data analytics for reporting security events essential to achieve the level of cybersecurity required to combat contemporary cyber threats and operate in contested spaces.

US Dept of Commerce NTIA Cyber Risk Management [i.52]

NTIA began significant cyber risk management public outreach initiatives beginning in 2017 to work with the private sector to develop an array of risk management platforms that are instantiated on a dedicated Cyber Risk Management (CSCRM) web site that include NIST and CISA enumerated above and include the following topics.

- Cyber Supply Chain Risk Management for the Public.
- Software Bill of Materials (SBOM) Resources Library.

US DHS Cybersecurity and Information Security Agency (CISA) Cyber Risk Management [i.81]

CISA has undertaken significant cyber risk management programs - especially relating to supply chain risk management - that overlap with those of NSA, NIST, and NTIA and include the following:

- CISA: "Guide to Getting Started with a Cybersecurity Risk Assessment" 2022 [i.82].
- CISA: "SBOM Resources Library" [i.83].

- CISA: "A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management" 2023 [i.85].

5.2.3 Industry sector guidelines

Almost every significant industry sector has some form of cybersecurity risk management guidelines. Within the EU, as noted above, the DORA financial services sector enabling legislation uses the term "risk" no less than 344 times. It is beyond the scope of the present Technical Report to treat all the different industry sector guidelines. A representative example of how cyber risk management is effected for the financial sector can be found in the non-profit Cyber Risk Institute publication "Cyber Profile for the Financial Sector" [i.53]. A generic model for different sectors can be found in the Fair Institute model "FAIR Risk Management" [i.43].

5.2.4 Implementation tools market

The significant demand for cyber risk management tools has resulted in a large market for implementation tools. Some of the more prominent surveys and tools include:

- centraleyes: "7 Best Cyber Risk Management Platforms of 2024" [i.50].
- ReversingLabs: "Assess & Manage Commercial Software Risk" [i.46].
- xmcyber: "Continuous Threat Exposure Management (CTEM)" [i.51].
- BlackDuck: "Security Risk Assessment, Threat Midelling Best Practices [i.26].

5.2.5 Legal obligations

Regulatory requirements

The only risk management regulatory obligations are those of the European Union as shown in Table 4.4-1 which is effectively experimenting with the concepts as the only governmental authority promulgating risk management requirements. The challenge, however, is achieving a reasonable and proportional outcome given that risk management requires knowledge of factors spread across a constantly changing ICT system and under the autonomous control of many different parties. For example, CRA product manufacturers have very limited knowledge of the implementations of their products and no real control over them and thus cannot undertake a risk assessment. Risk assessments are typically what an end user undertakes, not a product manufacturer. Ultimately, regulatory requirements that lack proportionality and reasonableness will be determined through judicial decisions described in the judicial decisions below [i.54].

Judicial decisions

Court cases related to risk management often arise from situations where a failure in risk management practices has led to harm or loss. Here's a breakdown of relevant information:

1) Risk Management Failures and Legal Liability:

   - Duty of Care: Organizations have a legal and ethical obligation to protect employees, customers, and others from foreseeable harm. This duty of care is a core concept in risk management.
   - Negligence: When an organization fails to meet its duty of care, it can be found negligent and held liable for the resulting harm. Negligence is often the basis of many risk management related lawsuits.
   - Risk Management Liability: Companies can be held liable for risk management failures that lead to financial losses, reputational damage, or even criminal charges.

EXAMPLE: The Wells Fargo fake accounts scandal and Boeing's 737 Max incidents are examples where failures in risk management led to significant legal and financial consequences.

2) Court Cases in Specific Industries:

   - Technology: With the increasing reliance on technology, companies face risks related to cybersecurity, data privacy, and intellectual property.

3) Examples of Risk Management Cases:

- State v. Loomis (Wisconsin, 2016): This case involved the use of a risk assessment tool (COMPAS) in sentencing, raising questions about due process and algorithmic bias.
- Southwest Airlines Co. v. Liberty Ins. Underwriters, Inc. (5th Cir. 2024): This case dealt with whether losses incurred due to an airline's business decisions to mitigate damages from a computer disruption were covered under a cyber insurance policy.
- Cases involving duty of care: There are numerous cases related to duty of care in various sectors, highlighting the importance of organizations taking reasonable steps to prevent harm.

4) Best Practices for Risk Management:

- Proactive Risk Identification and Assessment: Organizations should regularly identify and assess potential risks to their operations, employees, and stakeholders.
- Robust Policies and Procedures: Implementing clear policies and procedures to address identified risks is essential.
- Employee Training and Awareness: Training employees on risk management practices and fostering a culture of safety is crucial.
- Continuous Monitoring and Improvement: Risk management is an ongoing process that requires continuous monitoring and improvement.

In conclusion, court cases related to risk management demonstrate the legal and financial consequences of inadequate risk management practices. Organizations need to prioritize risk management, adhere to their duty of care, and take proactive steps to prevent foreseeable harm.

Annex A: Bibliography

- Eling, McShane, & Nguyen: "Cyber risk management: History and future research directions" Risk Management Insur Rev. 2021; 24:93-125.
- IBM: "What is cyber risk management".
- SAFECode: "NIST Publishes Important New Framework for Secure Software Development", June 2020.
- BlackDuck: "Open Source Security and Risk Analysis Report", 25 February 2025.
- BlackDuck: "Navigating the EU Cyber Resilience Act", 7 July 2025.

History

Document history		
V1.1.1	December 2025	Publication