TECHNICAL REPORT

ISO/IEC TR 27563

First edition
2023-05

Security and privacy in artificial intelligence use cases — Best practices

Sécurité et respect de la vie privée dans les cas d'usage de l'intelligence artificielle — Bonnes pratiques

Reference number
ISO/IEC TR 27563:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Analysis of security and privacy **3**
5.1 General 3
5.2 Application domains in ISO/IEC TR 24030:2021 use cases 3
5.3 Security in ISO/IEC TR 24030:2021 use cases 3
5.4 Privacy in ISO/IEC TR 24030:2021 use cases 4
6 Templates for analysis **5**
7 Supporting information **6**
7.1 Describe ecosystem 6
7.2 Provide assessment of systems of interest 7
7.3 Identify security and privacy concerns 7
7.4 Identify security and privacy risks 9
7.5 Identify security and privacy controls 11
7.6 Identify security and privacy assurance concerns 15
7.7 Identify security and privacy plan requirements 16
Annex A (informative) **Additional use cases** **18**
Bibliography **28**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information technology, cyber security and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Artificial intelligence (AI) and machine learning (ML) are increasingly being adopted by the digital industry, using algorithms to make decisions that have the potential to negatively impact the privacy of individuals and in some cases can even cause harm to some of them, unless adequate safeguards are deployed. Such safeguards to protect privacy often depend on a variety of factors including the specific type of process, sensitivity of data used, and potential harm likely to be caused.

This concern has been expressed by:

— Practitioners, who identified 23 principles for AI at the 2017 Asilomar conference[1], covering research, ethics and values, as well as longer term issues.

— Standard developers, as evidenced by the report on ethically aligned design published by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems[2].

— Policy makers, as exemplified by the appointment by the European Commission of a high-level expert group on artificial intelligence and the subsequent publication of an assessment list[3].

This document provides an analysis of security and privacy of use cases provided in ISO/IEC TR 24030, which should be used in parallel. A number of additional use cases are provided in Annex A.

This document also uses concepts from ISO/IEC TR 24028, which addresses trustworthiness in AI systems, including approaches to establish trust (e.g. transparency, explainability, controllability), and to achieve trustworthiness properties (e.g. resiliency, reliability, accuracy, safety, security, or privacy).

Security and privacy in artificial intelligence use cases — Best practices

1 Scope

This document outlines best practices on assessing security and privacy in artificial intelligence use cases, covering in particular those published in ISO/IEC TR 24030.

The following aspects are addressed:

— an overall assessment of security and privacy on the AI system of interest;

— security and privacy concerns;

— security and privacy risks;

— security and privacy controls;

— security and privacy assurance; and

— security and privacy plans.

Security and privacy are treated separately as the analysis of security and the analysis of privacy can differ.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.3). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.2
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.1) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.4)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.3
PII principal
natural person to whom the *personally identifiable information (PII)* (3.1) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.4
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.1) on behalf of and in accordance with the instructions of a *PII controller* (3.2)

[SOURCE: ISO/IEC 29100:2011, 2.12]

4 Abbreviated terms

CCTV	closed-circuit television
GDPR	General Data Protection Regulation
HCI	human computing interaction
LINDDUN	linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance
NIST	national institute of standards and technology
OEM	original equipment manufacturer
PIA	privacy impact assessment
PII	personally identifiable information
PoC	proof of concept
SDG	sustainable development goals
STRIDE	spoofing identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege
UC	use case
V2X	vehicle-to-everything

5 Analysis of security and privacy

5.1 General

This document includes a security and privacy analysis of ISO/IEC TR 24030:2021 use cases. Two electronic attachments were used:

— the first is the material used by ISO/IEC TR 24030:2021, available here: https://standards.iso.org/iso-iec/tr/24030/ed-1/en/Use+cases-v05_electronic_attachment_022021.pdf,

— the second is the material used by this document, available here: https://standards.iso.org/iso-iec/tr/27563/ed-1/en/Security-privacy-24030-ed-1-AI-use-cases.pdf.

Annex A provides a list of new use cases.

5.2 Application domains in ISO/IEC TR 24030:2021 use cases

ISO/IEC TR 24030:2021 describes 132 use cases, belonging to 22 application domains as shown in Figure 1.

NOTE 1 134 use cases are listed in this document, as use case 96 from ISO/IEC TR 24030 has been categorized into 3 application domains.

NOTE 2 The number of use cases per domain, e.g. 1 energy use case compared to 29 healthcare use cases is not an indication of the potential deployment of AI capabilities in a domain.

NOTE 3 The assignment of a use case to a domain depends on the viewpoint of experts. For instance, use case 132 (Device control using both cloud AI and embedded AI) is classified as manufacturing instead of home.

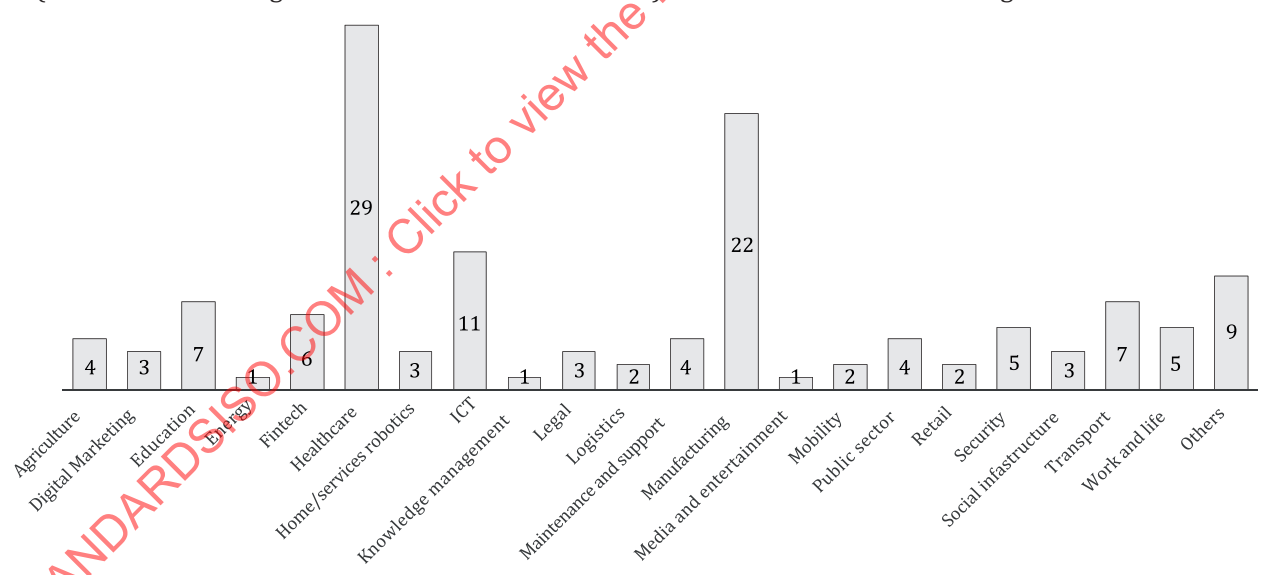


Figure 1 — Distribution of use cases by application domains

5.3 Security in ISO/IEC TR 24030:2021 use cases

Figure 2 summarizes the security analysis of ISO/IEC TR 24030 use cases in the second electronic attachment. It shows for each application domain:

— the number of use cases for which security concerns can be negligible;

— the number of use cases for which security concerns can be limited;

— the number of use cases for which security concerns can be significant; and

— the number of use cases for which security concerns can be maximum.

NOTE 1 The assessment is based on the most critical systems of interest. For instance, use case 1 (Explainable artificial intelligence for genomic medicine) involves two systems of interest, the genomic sequence processing system for which security concerns can be maximum, and the genomic training system for which system concerns can be significant. The resulting assessment is that security concerns can be maximum.

NOTE 2 The assessment result of each domain is not an indication of the potential privacy concern of AI in a domain.

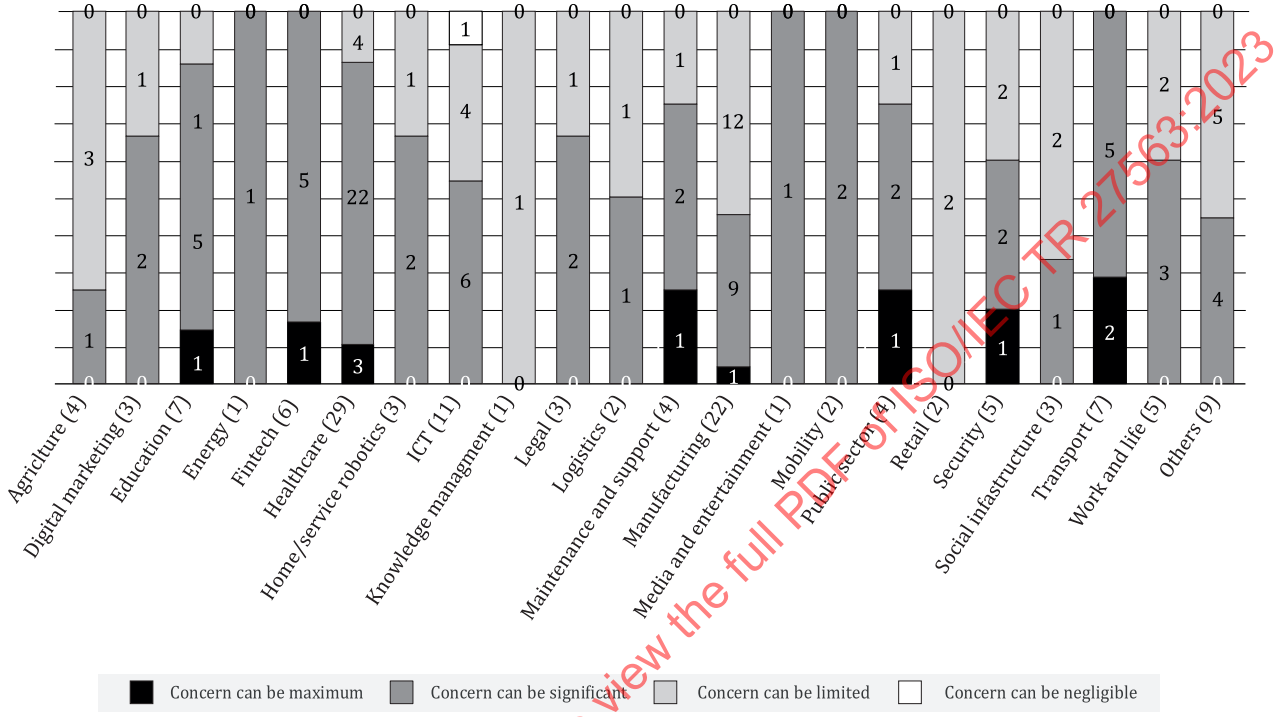


Figure 2 — Security analysis in AI use cases

5.4 Privacy in ISO/IEC TR 24030:2021 use cases

Figure 3 summarizes the privacy analysis of ISO/IEC TR 24030 use cases listed in the attachment. It shows for each application domain:

— the number of use cases for which privacy concerns can be negligible;

— the number of use cases for which privacy concerns can be limited;

— the number of use cases for which privacy concerns can be significant;

— the number of use cases for which privacy concerns can be maximum.

NOTE 1 The assessment is based on the most critical systems of interest. For instance, use case 1 (Explainable artificial intelligence for genomic Medicine) involves two systems of interest, the genomic sequence processing system for which privacy concerns can be maximum, and the genomic training system for which system concerns can be negligible. The resulting assessment is that privacy concerns can be maximum.

NOTE 2 The assessment result of each domain is not an indication of the potential privacy concern of AI in a domain.

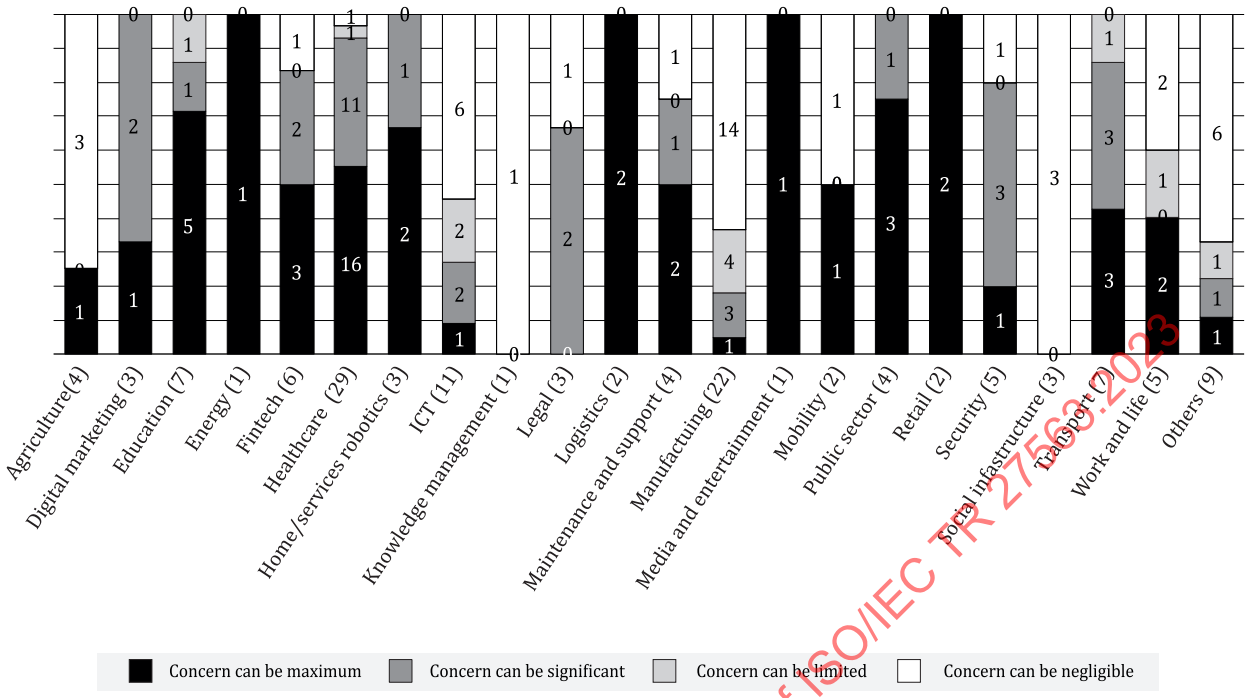


Figure 3 — Privacy analysis in use cases

6 Templates for analysis

The template used to collect material is shown in Table 1. It includes three types of table cells:

— title cell (e.g. use case name);

— instruction cell (e.g. describe the ecosystem);

— example cell (e.g. System of interest: < use case system of interest >).

Example cells can include texts in brackets, e.g. < asset A > . They are intended to be replaced by a specific text related to the use case.

NOTE 1 The proposed texts in example cells use vocabularies and concepts which are aligned with existing security and privacy references (See [7][8][9][10][13][16][17][18][19][24][15][14]).

NOTE 2 A use case can involve several systems of interest.

Table 1 — Template for collecting material

ID	< identification as provided by ISO/IEC TR 24030 >	
Use case name	< use case name as provided by ISO/IEC TR 24030 >	
Ecosystem	Describes the ecosystem: identifies the systems of interest, the stakeholders, and the stakeholders' assets that are impacted by AI	Systems of interest: — < use case system of interest > Stakeholders: — < stakeholder A > Stakeholder assets that are impacted by AI — < asset A >
System of interest: < Use case system of interest >		
Assessment of system of interest	Assessment on security and privacy concerns	— Security and privacy concerns on < use case system of interest > are < negligible, limited, significant, maximum >
Security and privacy concerns	Highlights security and privacy concerns that are impacted by AI	— Protection goals to consider for < asset A > asset are < confidentiality, integrity, availability, unlinkability, transparency, intervenability[8] > — The following privacy principles to consider for a < use case system of interest > integrating a < asset A > asset: < e.g. consent and choice, use retention and disclosure limitation[9] > — The following framework concepts to consider for a < use case system of interest > integrating a < asset A > asset: < e.g. Identify, Protect, Identify-P, Govern-P[21][15] >
Security and privacy risks	Identifies security and privacy risks that are impacted by AI	— Privacy risks related to < asset A > asset (e.g. re-identification of ... while performing AI training and reasoning operations) — Security risks related to < asset A > asset (e.g. alteration of learning data with wrong information, security of training operation, security of reasoning operation, ...)
Security and privacy controls	Identifies security and privacy controls that are impacted by AI	— Security and privacy controls from < reference (see [22][23][24][17][7]) > to be considered for < use case system of interest >
Security and privacy assurance	Identifies security and privacy assurance aspects that are impacted by AI	— Organization operating the < use case system of interest > integrating < asset A > asset to ensure that it can be audited[19][20] This includes organisational and technical evidence.
Security and privacy plan	Identifies security and privacy plan aspects that are impacted by AI	— Organization operating the < use case system of interest > integrating < asset A > asset to establish a security and privacy plan[16] that will be validated and reviewed periodically for continual improvement.

7 Supporting information

7.1 Describe ecosystem

The type of stakeholders and system of interest that can be considered are shown in Table 2.

Table 2 — Points of attention on ecosystem

Points of attention	Description
Type of stakeholders	Supplier (including solution providers and technology providers) Entity that does not process PII at all PII controller PII processor PII principals Third parties
Type of system of interest	AI system of interest (e.g. a reasoning engine) System of interest that includes an asset to protect and uses an AI subsystem

7.2 Provide assessment of systems of interest

The qualifiers that can be used are “can be negligible”, “can be limited”, “can be significant”, “can be maximum”.

Note It is possible that concerns on security and privacy are not the same.

7.3 Identify security and privacy concerns

For each system of interest, the points of attention are shown in Table 3, Table 4, Table 5, and Table 6.

NOTE 1 Table 3 is based on based on ISO/IEC TR 27550.

NOTE 2 Table 4 is based on ISO/IEC 29100.

NOTE 3 Table 5 is based on ISO/IEC TS 27110 and the NIST privacy framework[15].

Table 3 — Points of attention on protection goals

Points of attention		Description
Security protection goals	Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
	Integrity	Property of accuracy and completeness
	Availability	Property of being accessible and usable upon demand by an authorized entity
Privacy protection goals	Unlinkability	Property that a PII principal can make multiple uses of resources or services without others being able to link these uses together
	Transparency	Property that all privacy-relevant data processing including the legal, technical and organizational settings can be understood and reconstructed
	Intervenability	Property that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing

Table 4 — Points of attention on privacy principles

Points of attention	Description
Consent and choice	Provisions which are made to provide PII principals with the opportunity to choose how their PII is handled and to allow a PII principal to withdraw consent easily and free of charge
Purpose legitimacy and specification	Communicating the purpose and awareness that it is expected to comply with applicable law and rely on a permissible legal basis
Collection limitation	Limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s)

Table 4 *(continued)*

Points of attention	Description
Data minimization	Minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it
Use, retention and disclosure limitation	Limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes
Accuracy and quality	Ensuring that the PII processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use
Openness, transparency and notice	Providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII
Individual participation and access	Giving PII principals the ability to access and review their PII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law
Accountability	Documenting and communicating as appropriate all privacy-related policies, procedures and practices. Assigning to a specified individual within the organization (who can in turn delegate to others in the organization as appropriate) the task of implementing the privacy-related policies, procedures and practices
Information security	Protecting PII under its authority with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and to protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle
Privacy compliance	Verifying and demonstrating that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors

Table 5 — Points of attention on activities

Points of attention		Description
Security	Identify	Ecosystems of stakeholders and threat environment
	Protect	Safeguards
	Detect	Discover cybersecurity events
	Respond	Response to cybersecurity events
	Recover	Restoration and communication after a cybersecurity event
Privacy	Identify-P	Organizational understanding to manage privacy risk for individuals arising from data processing
	Govern-P	Governance controls for privacy
	Control-P	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks
	Communicate-P	Communication capabilities so that organizations and individuals have an understanding on how data are processed
	Protect-P	Data protection safeguards

Table 6 lists points of attention on integration of security and privacy in an ecosystem.

NOTE 4 Table 6 is based on Annex B of ISO/IEC TS 27110.

Table 6 — Points of attention on integration

Points of attention	Example of activities	Example of input	Example of output
Reference architectures	Specify how the cybersecurity framework activities fit with the reference architecture used in the business environment and its ecosystem of internal and external stakeholders	Interview with domain architecture experts Reference architecture documents	Work product specifying the correspondence between the cybersecurity framework and the ecosystem reference architecture
Roles and stakeholders	Specify the mapping between roles and stakeholders in the domain ecosystem and the cybersecurity framework activities	Interview with domain experts List of domain use cases describing roles and stakeholders	Work product specifying the correspondence between the cybersecurity framework and the roles and stakeholders in the domain ecosystem
Security and privacy practices	Specify the relationship with the security and privacy practices in the domain ecosystem	Interview with domain security and privacy experts Reference security and privacy documents	Work product specifying the correspondence between the cybersecurity framework and security and privacy practices in the domain ecosystem
System life cycle processes	Identify how the system life cycle processes integrate the cybersecurity framework	Interview with system life cycle experts Reference system life cycle documents	Work product specifying the correspondence between the cybersecurity framework and the system life cycle processes of the domain ecosystem

Table 7 lists points of attention on AI specific security and privacy vulnerabilities.

NOTE 5 Table 7 is based on ISO/IEC TR 24028.

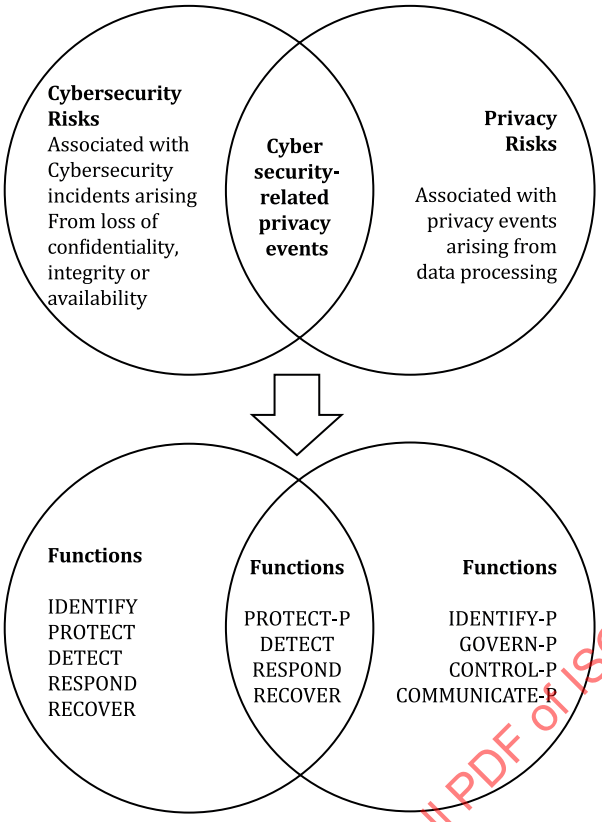
Table 7 — Points of attention on AI trustworthiness vulnerabilities

Points of attention	Vulnerability	Example of threats
AI specific security threats	Data poisoning	Influencing training data to manipulate the results of a predictive model
	Adversarial attacks	Provide perturbed input data to a valid model
	Model stealing	Send to targeted model a high number of prediction queries and use response received (the prediction) to train another model
	Hardware-focused threats to confidentiality and integrity	Affect confidentiality of data Affect integrity of data and computation
AI specific privacy threats	Upon data acquisition	Not following principle of PII minimization Compromising data storage
	Upon data pre-processing and modelling	Using AI to infer PII from data Using AI to re-identify information using multiple data sources
	Upon model query	Using model for non-authorized purpose (e.g. social service screening, credit card scoring)

7.4 Identify security and privacy risks

For each system of interest, security and privacy risks can be identified, and resulting consequences identified. See ISO/IEC 27005 for security and ISO/IEC 29134 for privacy.

The upper part of Figure 4 shows the relationships between security and privacy risks.



SOURCE NIST[15], reproduced with the permission of the authors.

Figure 4 — Security and privacy risks, and related functions

Table 8 and Table 9 show examples of categories of threats that can be used.

NOTE These categories of threats are based on the STRIDE and LINDDUN taxonomy.

Table 8 — Points of attention on threats

Points of attention		Description
Security threat STRIDE taxonomy	Spoofing	The identity of the users is established (or anonymous entities are accepted)
	Tampering	Data and system resources are only changed in appropriate ways by appropriate people
	Repudiation	Users cannot perform an action and later deny performing it
	Information disclosure	Data are only available to the users intended to access it
	Denial of Service	Systems are ready upon request and perform acceptably
	Elevation of privilege	Users are explicitly allowed or denied access to resources

Table 8 *(continued)*

Points of attention		Description
Privacy threat LINDDUN taxonomy	Linkability	Establishing the link between two or more actions, identities, and pieces of information
	Identifiability	Establishing the link between an identity and an action or a piece of information
	Non-repudiation	Inability to deny having performed an action that other parties can neither confirm nor contradict
	Detectability	Detecting the PII principal's activities
	Disclosure of information	Disclosing the data content or controlled release of data content
	Unawareness	PII principals being unaware of what PII about them is being processed Unawareness by PII Controllers of life cycle weaknesses that can exist/develop due to greater awareness of the content of the training model or other ML techniques
	Non-compliance	PII controller fails to inform the data subject about the system's privacy policy, or does not allow the PII principal to specify consents in compliance with legislation

The following categories of issues related to privacy consequences in Table 9 can be used.

Table 9 — Points of attention on issues related to privacy consequences

Points of attention	Description
Discrimination	Unfair, discriminatory or biased outcome that would largely affect the PII principals in any given situations through the processed data about them
Unsolicited Tracking	Automatically identify and eventually track PII principals and their activities without their consent and/or knowledge
Negligence	Failure to act with prudence of PII processors and PII controllers on protecting the information even with knowing the risks represented by the processing
Lack of transparency	Inability to inform or be transparent to PII principals regarding how their PII are processed or handled and its purpose
Lack of proportionality	Amount of PII collected by the system is not proportional to its processing purpose
Loss of Anonymity	Integration of numerous systems and databases which can affect the anonymity of PII principals

7.5 Identify security and privacy controls

For each system of interest, security and privacy controls can be identified.

Table 5, based on ISO/IEC TS 27110 and the NIST privacy framework[15] can be used to guide the identification. The lower part of Figure 4 shows examples of functions that can be used to identify controls.

Table 10 lists control categories as proposed by ISO/IEC 27001, ISO/IEC 27701 and ISO/IEC 29151 for information security. Table 11 lists control categories as proposed by ISO/IEC 27002.

NOTE Table 10 is based on ISO/IEC 27001:2013, Annex A.

Table 10 — Control categories for information security

Category	Sub-categories
Information security policies	Management direction
Organization of information security	Internal organization
	Mobile devices and teleworking
Human resource security	Prior to employment
	During employment
	Termination and change of employment
Asset management	Responsibility for assets
	Information classification
Access control	Business requirements for access control
	User access management
	User responsibilities
	System and application access control
	Media
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas
	Equipment
Operation security	Operational procedures and responsibilities
	Protection from malware
	Backup
	Logging and monitoring
	Control of operational software
	Technical vulnerability management
	Information systems audit considerations
Communication security	Network security management
	Information transfer
System acquisition, development and maintenance	Security requirements of information system
	Security in development and support processes
	Test data
Suppliers relationships	Information security in supplier relationships
	Supplier service delivery management
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity
	Redundancies
Compliance	Compliance with legal and contractual requirements
	Information security reviews

Table 11 — Control categories for information security based on ISO/IEC 27002

Category themes	Controls
Organizational controls	Policies for information security
People controls	Screening
	Terms and conditions of employment
	Information security awareness education and training
	Disciplinary process
	Responsibilities after termination or change of employment
	Confidentiality of non-disclosure agreements
	Remote working
	Information security event reporting
Physical controls	Physical security perimeters
	Physical entry
	Securing offices, rooms and facilities
	Physical security monitoring
	Protecting against physical and environmental threats
	Working in secure areas
	Clear desk and clear screen
	Equipment siting and protection
	Security of assets off-premises
	Storage media
	Supporting utilities
	Cabling security
	Equipment maintenance
	Secure disposal or re-use of equipment
Technological controls	User end point devices
	Privileged access rights
	Information access restriction
	Access to source code
	Secure authentication
	Capacity management
	Protection against malware
	Management of technical vulnerabilities
	Configuration management
	Information deletion
	Data masking
	Data leakage prevention
	Information backup
	Redundancy of information processing facilities
	Logging
	Monitoring activities
	Clock synchronization
	Use of privileged utility programs
	Installation of software on operational systems

Table 11 *(continued)*

Category themes	Controls
	Networks security
	Security of network services
	Segregation of networks
	Web filtering
	Use of cryptography
	Secure development life cycle
	Application security requirements
	Secure system architecture and engineering principle
	Secure coding
	Secure testing in development and acceptance
	Outsourced development
	Separation of development, test and production environments
	Change management
	Test information
	Protection of information systems during audit testing

Table 12 lists control categories as proposed by ISO/IEC 27701 for PII controllers.

Table 12 — Additional supporting information for PII controllers (for information systems)

Category	Supporting information
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Joint PII controller
	Records related to processing PII
Obligations to PII principals	Determining and fulfilling obligations to PII principals
	Determining information for PII principals
	Providing information to PII principals
	Providing mechanism to modify or withdraw consent
	Providing mechanism to object to PII processing
	Access, correction and/or erasure
	PII controllers' obligation to inform third parties
	Handling requests
	Automated decision making

Table 12 *(continued)*

Category	Supporting information
Privacy by design and privacy by default	Limit collection
	Limit processing
	Accuracy and quality
	PII minimization objectives
	PII de-identification and deletion at the end of processing
	Temporary files
	Retention
	Disposal
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer between jurisdictions
	Countries and international organizations to which PII can be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties

Table 13 below lists control categories as proposed by ISO/IEC 27701 for PII processors.

Table 13 — Additional supporting information for PII processors (for information systems)

Category	Supporting information
Conditions for collection and processing	Customer agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	Customer obligations
	Records related to processing PII
Obligations to PII principals	Obligations to PII principals
Privacy by design and privacy by default	Temporary files
	Return, transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for PII transfer between jurisdictions
	Countries and international organizations to which PII can be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

7.6 Identify security and privacy assurance concerns

For each system of interest, security and privacy assurance points of attention can be identified. Examples are shown in Table 14.

Table 14 — Points of attention on assurance

Points of attention	Comment
Evidence for security and privacy assurance	Assurance focuses on verifying that requirements concerning security privacy for AI system are met. Evidence are defined for each requirement EXAMPLE 1 A design report explains how explainability is done EXAMPLE 2 The AI system has an HCI for explainability EXAMPLE 3 A privacy impact assessment report is provided
Organizational and technical evidence	Organisational evidence EXAMPLE 4 A periodic review of risks is made Technical evidence EXAMPLE 5 Demonstrating that a specific de-identification mechanism is used
Assurance approach and metrics for assurance	Audits can focus on system assurance or on process assurance EXAMPLE 6 A system assurance can be the security and privacy certification of a Machine learning (ML) capability EXAMPLE 7 A process assurance can be the audit that an AI system life cycle process is at a given integrity level NOTE Ecosystem assurance can depend on the underlying governance approach
Competence and ecosystem for assurance	To be effective assurance is based on the requirements EXAMPLE 8 ISO/IEC 27001 is supported by ISO/IEC 27006 EXAMPLE 9 ISO/IEC 27701 and ISO/IEC 27002 is supported by ISO/IEC TS 27006-2

7.7 Identify security and privacy plan requirements

For each system of interest, points of attention on security and privacy plan can be identified. Examples are shown in Table 15 and Table 16.

NOTE Table 5 is based on ISO/IEC TS 27570.

Table 15 — Points of attention on security and privacy ecosystem plan

Points of attention	Comment
Governance process	The governance process focuses on the establishment of security and privacy policies, and the continuous monitoring of their proper implementation in the ecosystem. These activities are carried out by the governing bodies of the ecosystem, as well as by the organizations in the ecosystem which implement the security and privacy policies.
Data management process	The data management process focuses on the management of security and privacy in the creating, capturing, collecting, transforming, publishing, accessing, transferring, and archiving of data within an ecosystem. These activities are carried out by the governing bodies of an ecosystem, as well as by the organizations in the ecosystem.
Risk management process	The risk management process deals with the analysis and the treatment of security and privacy risks in an ecosystem. The activities are carried out by the governing bodies of the ecosystem, as well as by the organizations in the ecosystem.
Engineering process	The engineering process is a set of activities related to the life cycle of a service in an ecosystem. These activities are carried out by the governing bodies of the ecosystem, as well as by the organizations in the ecosystem concerned with the delivery, and the use of the availability of the ecosystem service. It elaborates the conceptual principles such as privacy by design and privacy by default and other important design goals in applicable jurisdictions. It also considers the requirements specified in ISO/IEC TR 27550.

Table 15 *(continued)*

Points of attention	Comment
Citizen engagement process	The citizen engagement process focuses on consultation with citizens on security and privacy rules and policies at governance level, and on the support on the enforcement of these rules and policies concerning the security and privacy of an ecosystem service.

Table 16 — Points of attention on security and privacy plan

Points of attention	Comment
Continuous determination of roles	There are specific responsibilities that are associated with the certain stakeholders (e.g. PII controllers, PII processors). It is important to have a continuous assessment of whether a stakeholder is changing its role. For instance, it is possible that an operator of an AI system deployed it with the understanding that no PII is collected, but further operations can lead to a status where the AI system is collecting PII. Here are examples of factors that can lead to this situation: — Governance capabilities (the AI system dynamically decides to collect some type of data), — Re-identified data (some data that is initially categorized at non-PII is now a PII) — Error in data sharing agreements.
Organizational measures in the ecosystem	Virtually all use cases of ISO/IEC TR 24030 are part of an ecosystem. Organizational measures are implemented when there it is expected that stakeholders to synchronise their actions. For instance, when data sets include privacy leaks, all the stakeholders using the data sets can be informed and take appropriate actions.
Accountability	Organizations (both processors and controllers) demonstrate accountability and responsibility when processing personal information e.g. by having a data protection officer or data protection team/office dedicated in catering the compliance of the organization
Compliance	To ensure that organizations are compliant with data processing and data protection requirements to their respective and applicable jurisdictions including their adherence to data privacy principles
Ethics principles	The digital economy is built on massive streams of data being processed. Through the application of AI, the traditional governance frameworks and strategies can be insufficient. Having a set of principles of data ethics in building programs and AI solutions can reinforce its processes, such as decision-making, ethical controls that can mitigate new risks and challenges that AI encounters.
Data breach and security incident management	As we have entered digital economy and the rise of data processing, there are increasing incidents of personal data breaches that impact both public and private entities, entailing significant economic and legal costs for those involved in processing of personal data. This also puts at risk data subjects for identity theft, crimes and other harm. In order to afford protection of personal data, reasonable and appropriate measures are implemented to ensure that organizations are ready for data breaches and security incidents when it happens.

Annex A
(informative)

Additional use cases

A.1 General

This annex provides additional new examples of use cases elaborated by experts in the scope of this document, which are not listed in ISO/IEC TR 24030.

A.2 Abnormal transaction

The use case in Table A.1 follows the template described in Clause 6. Figure A.1 summarizes the impact of the use case on security and privacy.

Table A.1 — Abnormal transaction use case

ID	SC27–1	
Use case name	Abnormal transactions of internal control and compliance employees in bank system	
Ecosystem	Describe the ecosystem: Identify the systems of-interest, the stakeholders, and the stakeholders' assets that are impacted by AI	Systems of interest: — Abnormal transactions monitoring system Stakeholders: — Bank — Bank regulator Stakeholder assets that are impacted by AI — Core banking system — Internal control and compliance data
System of interest: Abnormal transactions monitoring system		
Assessment of system of interest	Assessment on security and privacy concerns	— Security concerns on abnormal transactions monitoring system are significant — Privacy concerns on abnormal transactions monitoring system are significant
Security and privacy concerns	Highlight security and privacy concerns that are impacted by AI	— All security and privacy protection goals to consider for abnormal transactions monitoring system (confidentiality, integrity, availability, unlinkability, transparency, intervenability) — All security framework concepts to consider for abnormal transactions monitoring system (Identify, Protect, Detect, Respond, Recover) — All privacy framework concepts to consider for abnormal transactions monitoring system (Identify-P, Govern-P, Control-P, Communicate-P, Protect-P)

Table A.1 *(continued)*

Security and privacy risks	Identify security and privacy risks that are impacted by AI	— Privacy risks related to abnormal transactions monitoring system (e.g. disclosure of identity information and sensitive legal information etc. while performing AI training and reasoning operations) — Security risks related to abnormal transactions monitoring system (e.g. alteration of learning data with wrong information, security of training operation, security of reasoning operation)
Security and privacy controls	Identify security and privacy controls that are impacted by AI	— Security controls from ISO/IEC 27001 or ISO/IEC 27002 to be considered for abnormal transactions monitoring system (e.g. information security policies, asset management, physical and environmental security, access control, operation security, information security incident management) — Privacy controls from ISO/IEC 27701 to be considered for abnormal transactions monitoring system
Security and privacy assurance	Identify security and privacy assurance aspects that are impacted by AI	— Organization using abnormal transactions monitoring system to ensure that system can be audited (see ISO/IEC 27006-1 and ISO/IEC 27006-2). This includes organizational and technical evidence.
Security and privacy plan	Identify security and privacy plan aspects that are impacted by AI	— Organization using abnormal transactions monitoring system to establish a security plan, that will be validated and reviewed periodically for continual improvement.
Impact summary	Picture summarizing the impact of the use case on security and privacy	Figure A.1 shows the impact of the use case on security and privacy.
	Picture source code Sequencediagram.org	participant system of interest participant asset participant security impact participant privacy impact box over system of interest,asset:abnormal transactions monitoring system box right of asset:Core banking system parallel box right of asset:internal control and compliance data rbox right of security impact #lightgrey:significant rbox right of privacy impact #lightgrey:significant parallel off

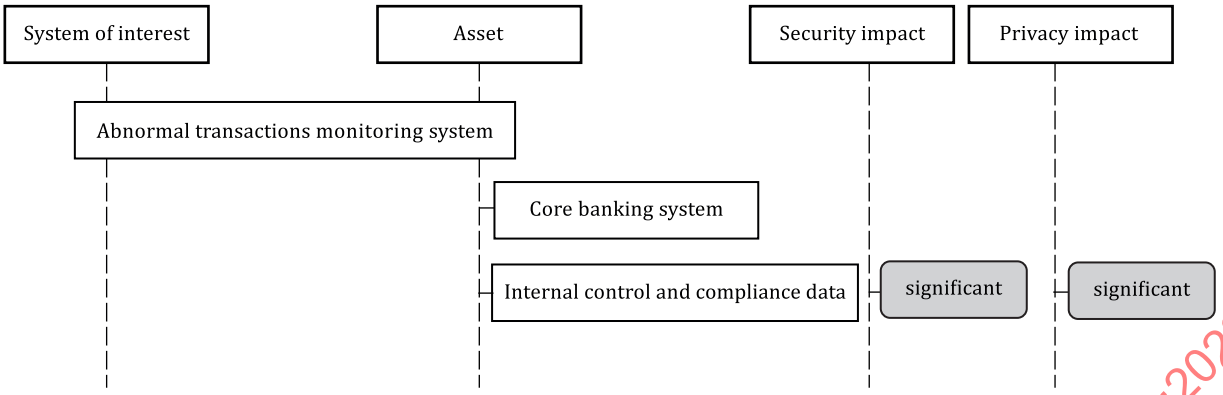


Figure A.1 — UC SC27–1 Abnormal transactions of internal control and compliance employees in bank system

A.3 Financial risk control

The use case in Table A.2 follows the template described in Clause 6. Figure A.2 summarizes the impact of the use case on security and privacy.

Table A.2 — Finance risk control

ID	SC27–2	
Use case name	Financial risk control	
Ecosystem	Describe the ecosystem: Identify the systems of interest, the stakeholders, and the stakeholders' assets that are impacted by AI	Systems of interest: — Financial risk management system Stakeholders: — Financial institution (such as bank) — Financial regulator Stakeholder assets that are impacted by AI — Financial business management system — Financial performance data
System of interest: Financial risk management system		
Assessment of system of interest	Assessment on security and privacy concerns	— Security concerns on financial risk management system are significant — Privacy concerns on financial risk management system are significant
Security and privacy concerns	Highlight security and privacy concerns that are impacted by AI	— All security and privacy protection goals to consider for financial risk management system (confidentiality, integrity, availability, unlinkability, transparency, intervenability) — All security framework concepts to consider for financial risk management system (identify, protect, detect, respond, recover) — All privacy framework concepts to consider for financial risk management system (Identify-P, Govern-P, Control-P, Communicate-P, Protect-P)

Table A.2 *(continued)*

Security and privacy risks	Identify security and privacy risks that are impacted by AI	— Privacy risks related to financial risk management system (e.g. disclosure of identity information and sensitive legal information while performing AI training and reasoning operations) — Security risks related to financial risk management system (e.g. alteration of learning data with wrong information, security of training operation, security of reasoning operation)
Security and privacy controls	Identify security and privacy controls that are impacted by AI	— Security controls from ISO/IEC 27002 to be considered for financial risk management system (e.g. information security policies, asset management, physical and environmental security, access control, operation security, information security incident management) — Privacy controls from ISO/IEC 27701 to be considered for financial risk management system
Security and privacy assurance	Identify security and privacy assurance aspects that are impacted by AI	— Organization using financial risk management system to ensure that system can be audited (see ISO/IEC 27006-1 and ISO/IEC TS 27006-2). This includes organizational and technical evidence.
Security and privacy plan	Identify security and privacy plan aspects that are impacted by AI	— Organization using financial risk management system to establish a security plan, that will be validated and reviewed periodically for continual improvement.
Impact summary	Picture summarizing the impact of the use case on security and privacy	Figure A.2 illustrates the impact of the use case on security and privacy.
	Picture source code Sequencediagram.org	participant system of interest participant asset participant security impact participant privacy impact box over system of interest,asset:Financial risk management system box right of asset:Financial business management system parallel box right of asset:Financial performance data rbox right of privacy impact#lightgrey:significant rbox right of security impact#lightgray:significant parallel off

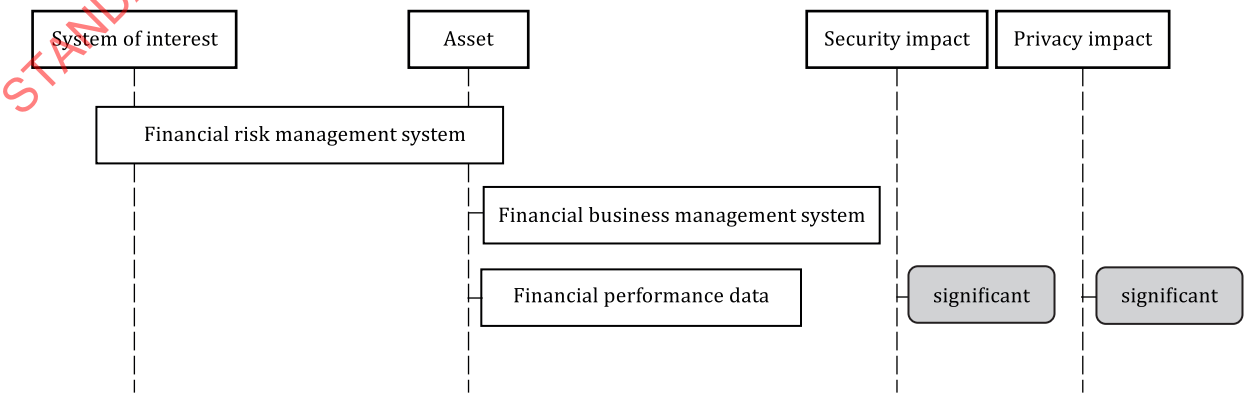


Figure A.2 — UC SC27-2 Financial risk control

A.4 AI webcam employee monitoring

The use case in Table A.3 follows the template described in Clause 6.

Table A.3 — AI webcam employee monitoring

ID	SC27–5	
Use Case Name	AI webcam employee monitoring	
Ecosystem	Describe the ecosystem: Identify the systems of interest, the stakeholders, and the stakeholders' assets that are impacted by AI	Systems of interest: — AI webcam employee monitoring Stakeholders: — Business processing outsourcing companies Stakeholder assets that are impacted by AI: — Employees — Productivity of employees — ICT resources
System of interest: AI webcam employee monitoring		
Assessment of system of interest	Assessment on security and privacy concerns	— Privacy concerns for employees are significant as they are monitored while working especially those that are in telecommute setup.
Security and privacy concerns	Highlight security and privacy concerns that are impacted by AI	Security concerns: — Confidentiality and integrity Privacy concerns: — Unlinkability, transparency, purpose legitimacy and proportionality. All privacy concepts to consider for monitoring productivity of employees and ensure that they are aware of the processing and data being processed are proportional to the declared purpose. (Identify-P, Govern-P, Control-P, Communicate-P, Protect-P)
Security and privacy risks	Identify security and privacy risks that are impacted by AI	Security risks: — Repudiation, information disclosure, spoofing Privacy risks: — Identifiability, detectability, disclosure of information, unawareness, non-compliance, lack of transparency, unsolicited tracking
Security and privacy controls	Identify security and privacy controls that are impacted by AI	— Controls from ISO/IEC 27001 applies (e.g. mobile devices and teleworking, logging and monitoring, user responsibilities, compliance with legal and contractual requirements) — Controls from ISO/IEC 27701 applies (e.g. identify and document purpose, identify lawful basis, privacy impact assessment, obligations to PII principals, privacy by design and privacy by default, records of PII disclosure to third parties)
Security and privacy assurance	Identify security and privacy assurance aspects that are impacted by AI	Assurance approach and metrics for assurance
Security and privacy plan	Identify security and privacy plan aspects that are impacted by AI	All security and privacy plan requirements applies (governance process, data management process, risk management process, engineering process, citizen engagement process).

A.5 Training with privacy-sensitive data

The use case in Table A.4 follows the template contained in ISO/IEC TR 24030.