Methodology for Generative AI privacy Study

Ad hoc group WG 5–42–001 – to advance ISO/IEC 27091
Contribution Antonio Kung

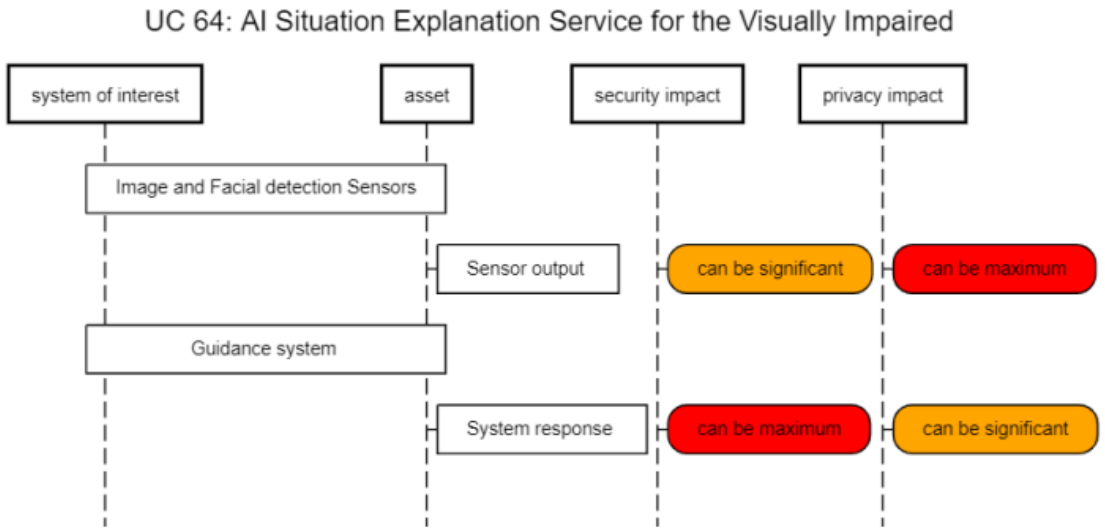
ISO/IEC 27563 Security and privacy in AI use cases – best practices

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> — 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> — 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>
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 that will be validated and reviewed periodically for continual improvement.

Example A.64 AI situation explanation service for the visually impaired

(https://standards.iso.org/iso-iec/tr/27563/ed-1/en/Security-privacy-AI-use-cases.pdf)

ID	64	
Use case name	AI Situation Explanation Service for the Visually Imp	
Ecosystem	Describe the ecosystem: identify the systems of interest, the stakeholders, and the stakeholders' assets that are impacted by AI	- User - Data controller/processes - People in the environment
Assessment of system of interest	Assessment on security and privacy concerns	Impact of AI on privacy can l Impact of AI on security can
Security and privacy concerns	Highlight Security and privacy concerns that are impacted by AI	Privacy and security principl - Consent and choice - Use retention and disclosu - Accuracy and quality - Openness, transparency an - Individual participation an - Accountability - Information security (Conf - Privacy compliance Activities to consider: - Identify-P, - Govern-P, - Control-P, - Communicate-P, - Protect-P - Model will rely on detectin - The UC carries all risks ass machine learning with hun - All of the security objective Availability needs to be co unauthorized access.
Security and privacy risks	Identify security and privacy risks that are impacted by AI	- Unlinkability not well addr - Intervenability not well ad - Transparency not well add - Disclosure of information - Unawareness - All security risks to be considered
Security and privacy controls	Identify security and privacy controls that are impacted by AI	- Information security policies - Asset management - Physical and environmental security - Access control - Cryptography - Operation security - Information security incident management - All control categories from ISO/IEC 27002 (ISMS), ISO/IEC 27701 (PIMS) and ISO/IEC 29100 can be considered for integrating AI components.
Security and privacy assurance	Identify security and privacy assurance aspects that are impacted by AI	The organization operating the system of interest can ensure that the organizational and technical measures applied to ensure privacy and security can be suitably audited (internally or externally), depending on regulations. This includes - Organisational evidence - Technical evidence

	that are impacted by AI	relevant stakeholders and reviewed periodically for continual improvement.
Impact summary	Picture summarizing the impact of the use case on security and privacy	
		Title UC 64: AI Situation Explanation Service for the Visually Impaired participant system of interest

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

Proposal

- Collect use cases
  - e.g. reuse the 27563 template, or a simplified version
- Study use case domain
  - Specify dedicated template for **privacy protection models**
    - Use ISO/IEC DTR 30194 Best practices for use case projects (see next slide)
- Impact on 27091 (AI privacy protection) or on 27564 (Guidance on the use of models for privacy engineering)
  - Publish collection of use case
  - Publish privacy protection models

ISO/IEC DTR 30194 Best practices for use case projects