
# Generative AI  privacy Study

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

# Outline

- Templates
- Workplan
- Use cases
  - Categories
  - Example: IoT+Digital twin+Data spaces

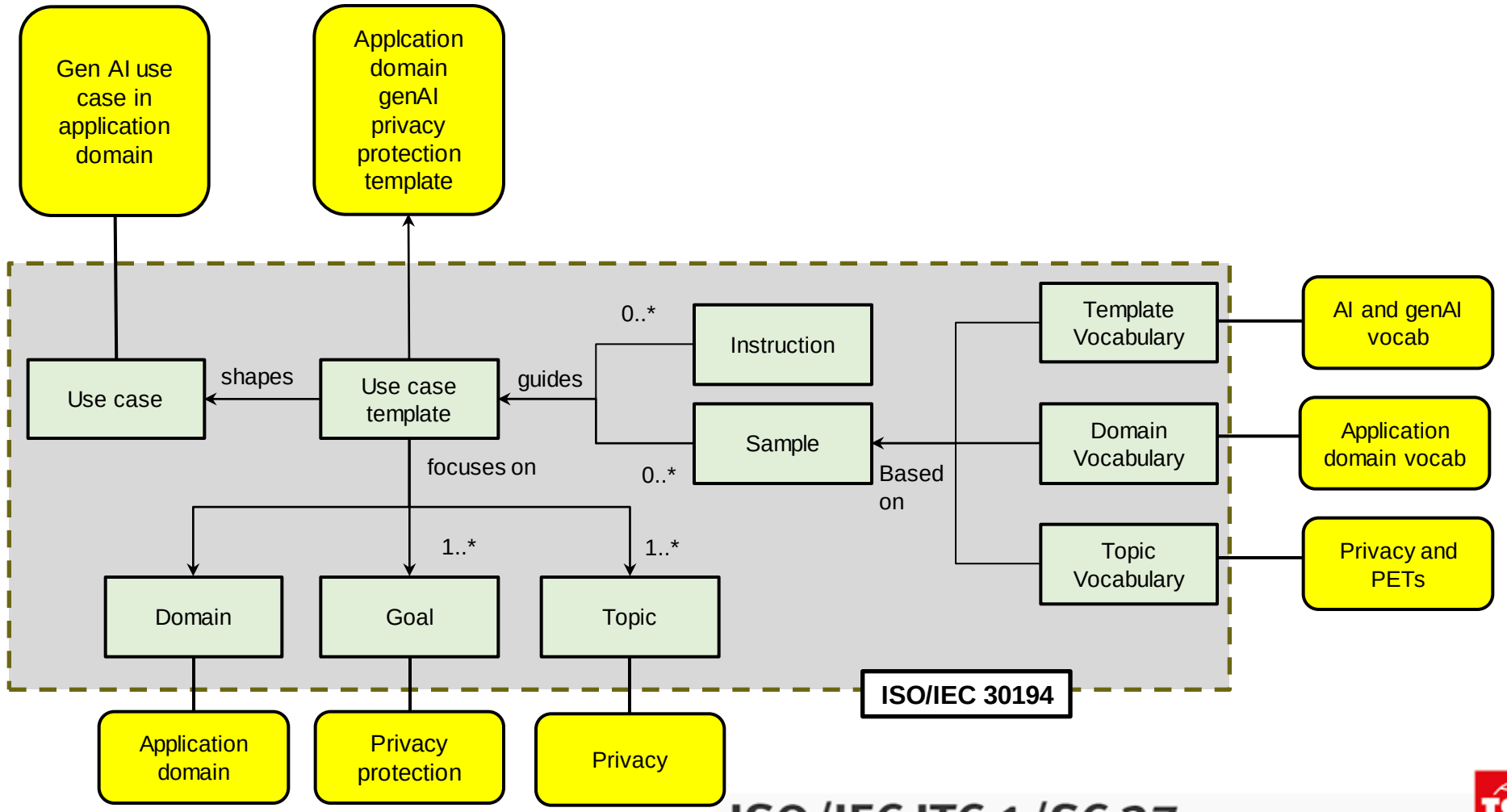
# Template user story

- Value of GenAI
  - As a [stakeholder], I want to be assisted on [task], so that [value]
    - See https://www.atlassian.com/agile/project-management/user-stories
  - As a [writer of a standard] I want to be assisted on [requirements terms (shall, could, may) ], so that [the intent of the standard is clear]
- Value of GenAI for privacy
  - As a [developer of a data exchange capability] I want to be assisted on [de-identification], so that [privacy principles of ISO 29100 are followed]
- GenAI as a threat to privacy
  - As a [hacker], I want to be assisted on [the analysis of a dataset], so that [PII on a specific person is derived]

# Template use case

| Use case name | |
|---|---|
| Ecosystem | Describes the ecosystem: identifies the systems of interest, the stakeholders, and the stakeholders' assets that are impacted by GenAI |
| System of interest: < Use case system of interest > | |
| Assessment of system of interest | Assessment on security and privacy concerns |
| Security and privacy concerns | Highlights security and privacy concerns that are impacted by GenAI |
| Security and privacy risks | Identifies security and privacy risks that are impacted by GenAI |
| Security and privacy controls | Identifies security and privacy controls that are impacted by GenAI |
| Security and privacy assurance | Identifies security and privacy assurance aspects that are impacted by GenAI |
| Security and privacy plan | Identifies security and privacy plan aspects that are impacted by GenAI |

# Template based on ISO/IEC DTR 30194 Best practices for use case projects



# Workplan

- Collect
  - User stories
    - Call for contributors (SC27, SC42, external?)
    - Collect categories of GenAI user stories
    - Collect user stories
  - Use cases
    - Call for contributors (SC27, SC42, external?)
    - Work A use case the User stories
- Analysis
  - Engineering level (security-by-design, privacy-by-design)
  - Impact assessment level
  - Privacy models (ISO/IEC 27564) (Guidance on the use of models for privacy engineering)
- Outcome
  - Recommendations to 27090, 27091
  - Publish user stories and use cases
  - Publish privacy protection models

March 2024
Validation

April - July 2024
Work on use stories and use cases

August – Oct 2024
Contribution to 27091

Nov 24 – April 25
Publish additional document

# Use case categories

- IT workplace
  - Text translation and productivity
  - Democratize organization data
  - Easy to generate SQL queries
  - Chatbot for dialog and prompt engineering
  - Code migration
  - Easing management meeting
  - Code quality improvement
  - Software coding
  - Generating images with AI
  - Computer programmer and data scientist
  - Security audit will be easy
  - Mock interview
  - Apps creation with generative AI mode
  - Time management
  - Benefits for editing
  - Behaviour prediction and creative writing
  - Fact checking, generating ideas
- Reference
  - Unleashing the Potential: Overcoming Hurdles and Embracing Generative AI in IT Workplaces: Advantages, Guidelines, and Policies. Pan Singh Dhoni

# Use case categories

- Helping cybersecurity
  - Malware detection
  - Anomaly detection
  - Password cracking
  - Threat intelligence
  - Adversarial AI defense
  - Phishing detection
  - Network traffic analysis
  - Automated security response
  - Security training and simulation
- GenAI against cybersecurity
  - Fund raising
  - Ransom email (layman can do it)
  - Generate malicious domains
  - Phishing kits
  - Circulating manipulated photos
  - Fake digital content
  - Fake voice
  - Fake document generation
  - Compromising company intellectual property
- Reference
  - Unleashing the Potential: Overcoming Hurdles and Embracing Generative AI in IT Workplaces: Advantages, Guidelines, and Policies. Pan Singh Dhoni

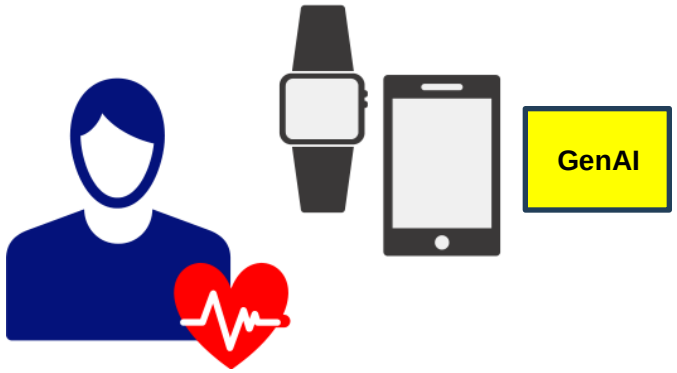
# Use case categories

- Enhance data quality
  - Data imputation and completion (Completing missing data, Time series forecasting)
  - Data validation and cleasing (Data anomaly detection, data quality validation, data standardization)
  - Data augmentation (Enhancing datasets, Feature engineering – privacy?)
  - Data simulation and testing (Realistic test case, stress testing)
  - Data governance and compliance (Data masking, auditing and monitoring)
- Reference
  - Exploring the Synergy between Generative AI, Data and Analytics in the Modern Age. Pan Singh Dhoni

# Use case example IoT

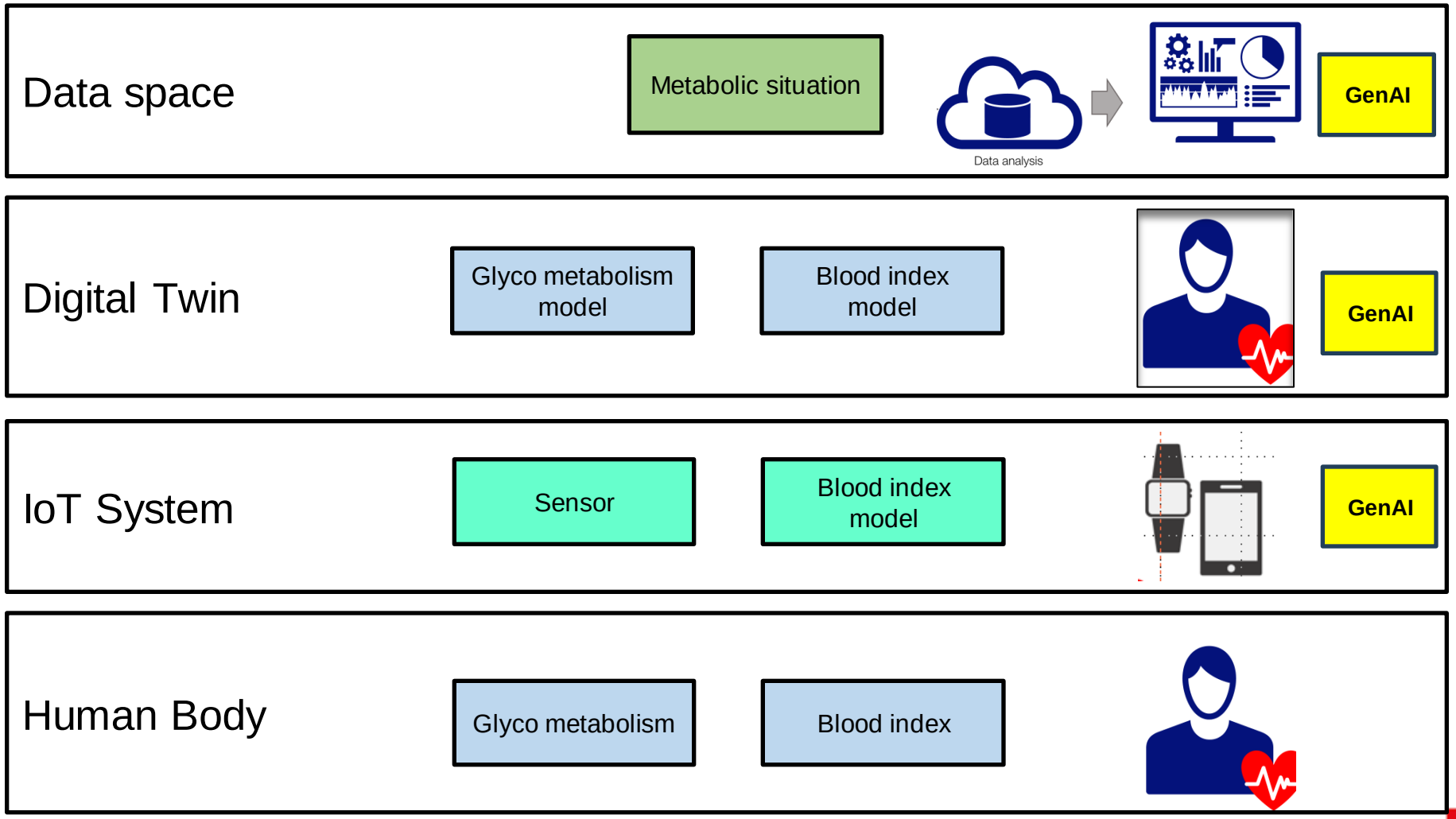
Data space


Data sources
Health




https://www.iec.ch/basecamp/virtual-sensors

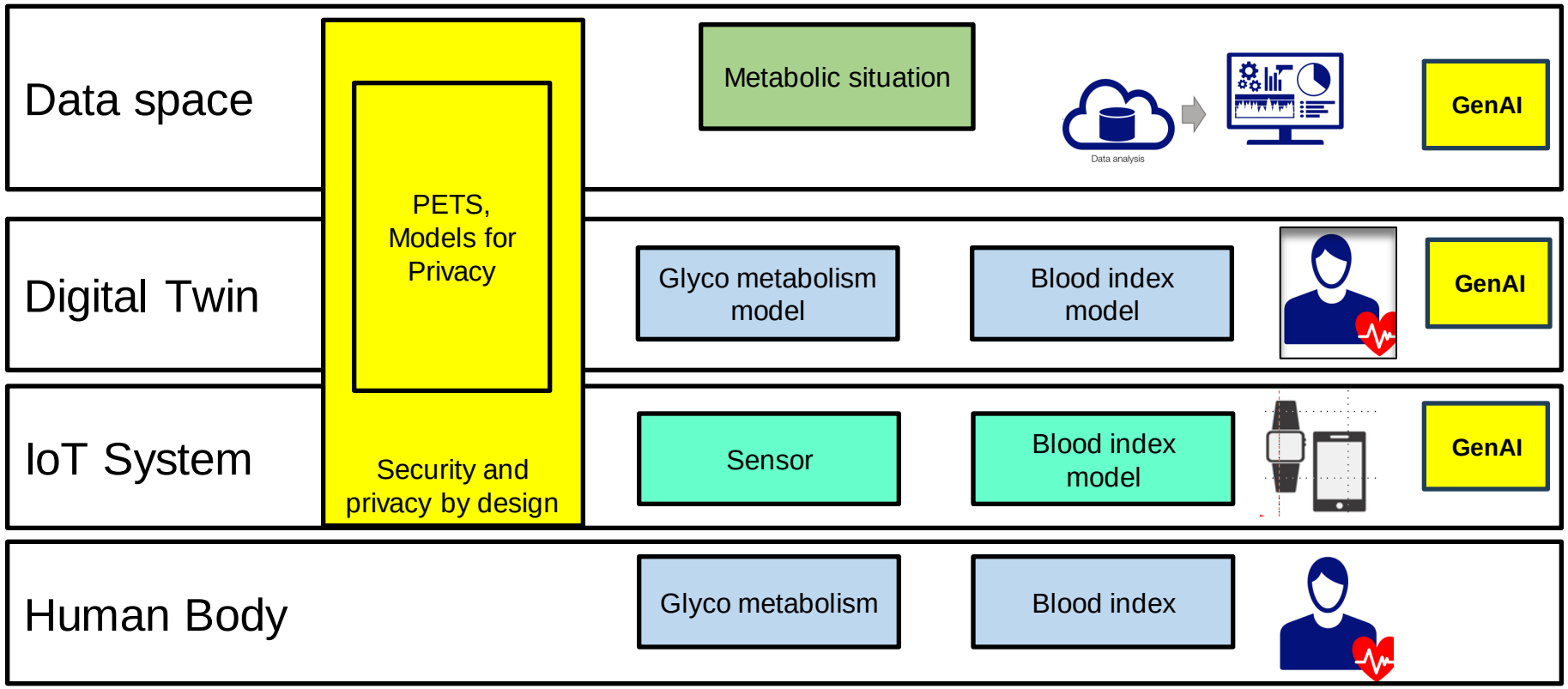
# Digital Twin Integration






ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

# Security and Privacy Integration






ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection