# Security analysis of information systems

## Managing and Sharing of Construction Data

Computing in Construction

Metropolia

Metropolia

# Digitalization, collaboration, and interoperability

The attempts to improve the productivity, quality, and sustainability of construction all increase the

- digitalization of activities and processes
- collaboration between project parties
- interoperability solutions between systems

Resulting problems

- Digitalization: more digital information will be produced and shared
- Collaboration: more information is shared between people
- Interoperability: information is shared so as to be easily used by other systems

→ New vulnerabilities: digital information can be stolen remotely, without leaving any traces

Cyber security

1. the application of technologies, processes, and controls
2. to protect systems, networks, programs, devices and data
3. from cyber attacks

Metropolia

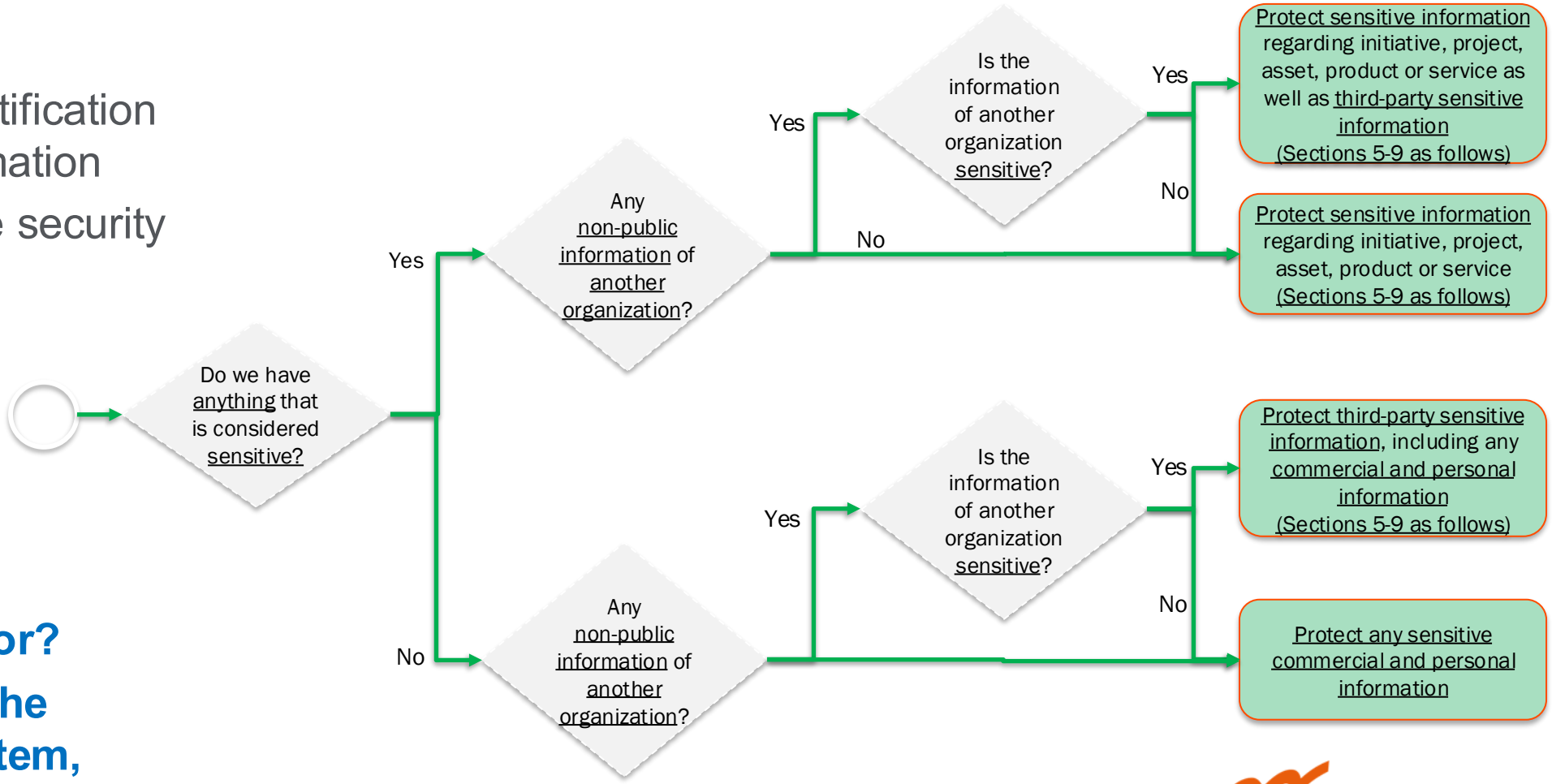
# Analyzing information and systems

Metropolia

# What to look for in information and systems?

## ISO19650-5

- Requires the identification of sensitive information
- The method is the security triage process




- **But what exactly should be look for?**
- **How to analyze the information, system, and agents?**
- **How to decide what is sensitive?**

Metropolia

# Analyzing information from security perspective

ISO 19650-5 Appendix A

Organizations should work to understand

1. the range of **threats** that seek to
   - compromise the value, longevity, and ongoing activities regarding projects, assets, products and services of the organization
   - cause harm, damage, or compromise personnel or users
   - disrupt or corrupt information systems
   - cause reputational damage
   - get personal data, intellectual property or commercially sensitive information

   Include
   - terrorism
   - espionage
   - cyber-attacks
   - insider threats
2. the evolving ways of **hostile reconnaissance** where someone is looking for information
   - it can exploit about security
     - physical vulnerabilities, system configuration
   - to identify the modus operandi
   - about the state of security
     - the odds of being detected vs successful
   - of the pattern-of-life of an individual or a group
   - pattern-of-use of an asset
3. the potential for system **contamination**
   - counterfeit or maliciously sub-standard components
4. the potential impact of **malicious acts** (malware, hackers, personnel) to compromise
   - intellectual property or commercially sensitive information
   - personal information
   - metadata or master reference data integrity
5. the potential for insecure systems to permit **unauthorized access** to sensitive information
6. the potential of a **pattern-of-life analysis** for exploitation of habits, routines and preferences
7. the potential for the **information aggregation** to
   - lead to the identification of individuals or groups
   - reveal information about projects, assets, products,...
   - reveal information about the configuration of assets

Aggregation risks can arise from aggregation by

1. **accumulation**: the volume of information increases the impact if compromised
2. **association**: pieces of non-sensitive information have a high impact if put together

# Personnel security

1. Identification of **high-risk functions** within the organization (e.g., in appointments), where high-risk functions include those which
   - have access to the security strategy, or information relating to sensitive assets
   - fulfil an information system administration or information management role
2. Requirements for **security screening and vetting**
   - for persons in contact with sensitive assets
3. Requirements for **security competence**
   - for individuals in specific roles
4. For new persons/organizations a **briefing on the responsibilities**
   - to include security awareness training as part of a project or ongoing operations
   - to cover necessary topics with the required learning outcomes
5. Requirements for **general security awareness training**
   - to promote a security-minded culture
   - including refresher training
6. Requirements for **role-based security training**
7. Requirements for **access control and permissions**
   - to access information or information systems
8. Eventual **demobilization** of organizations and personnel

Metropolia

# Technological security

- Factors to consider
  1. measures related to the cyber security of systems involved with sensitive information
     - regular vulnerability assessment and penetration testing
  2. the security of interconnections and interactions between systems
  3. the security around systems that control physical assets
  4. the permissible interoperability of systems
     - including the resilience of each system to failure
  5. configuration management and change control for the systems processing and storing sensitive information
  6. the secure disposal and/or destruction of information
     - by organizations no longer involved in an appointment
  7. measures to retain information required by regulations and to dispose it when no more needed

By default, maximum security settings should be used in systems containing sensitive information

Metropolia

# Selecting secure software systems

- How the potential systems can deliver
  1. **Confidentiality** — controlling and preventing unauthorized access to information
  2. **Availability** — ensuring that the information and systems are consistently usable,
     - the percentage availability (e.g., 99,999 9 % per annum)
     - the maximum time for restoration of a normal (e.g., 30 minutes)
  3. **Safety** — systems are designed to prevent harmful states which can lead to damage
  4. **Resilience** — the ability of systems to recover in response to adverse events
  5. **Possession** — systems are designed to prevent unauthorized control
  6. **Authenticity** — ensure that information in the system is genuine
  7. **Utility** — ensure that information remain useful over the required period
  8. **Integrity** — maintain the information completeness, accuracy, consistency, and coherence

- Especially regarding any distributed systems such as IoT, organization should
  - understand their security architecture
  - determine to which extent the architecture meets the security requirements
  - assess security risks, including the potential impact of a failure
  - put in place mitigation measures to manage any unacceptable security risks

Metropolia

# Information security

Access to sensitive information should be managed on a **need-to-know basis**: organizations and personnel only having access to the sensitive information that is **relevant and necessary for the completion of their tasks**.

For information security and policies processes, consider

1. the requirements for **inspections or surveys** that can gather sensitive information
2. the **secure storage**
   - management and monitoring
   - secure access to,
   - eventually secure disposal and destruction of information
3. the **maximum amount of information** relating to sensitive assets or systems to be contained
   - in databases,
   - information exchanges and
   - information models
4. the **embedded security requirements** relating to information provided by a third party
5. protection **against the compromise** of
   - information
   - metadata
   - referential master data (permissible property values to be used in models)
6. monitoring **changes to processes** and technologies used for
   - information capture
   - processing (including information synthesis)
   - storage

Metropolia

# Classification of information

Metropolia

# Security classification of information

- Classification is the process of categorizing information based on
  - its level of sensitivity and
  - the impact to the organization if it is disclosed, altered, or destroyed
- No general information classification systems is used in the construction sector
  - Rather, ISO19650-5 proposes a risk-based classification approach
- However, following levels could be used
  - Public information
    - Information intended for public dissemination and does not require protection from disclosure
    - Examples: Press releases, public websites, marketing materials.
  - Internal information
    - Information intended for internal use within an organization, not to be disclosed to the public
    - Examples: Internal communications, organizational policies, internal reports
  - Confidential information
    - Sensitive information requiring protection since its unauthorized disclosure could harm the organization or individuals
    - Applies also to third-party information
    - Examples: Customer data, internal financial information, proprietary business strategies
  - Restricted information
    - Highly sensitive information that, if disclosed, could cause severe damage to the organization or individuals
    - Examples: Trade secrets, intellectual property, strategic plans, and high-level executive communications
  - Top secret/classified information
    - Information that is of the highest sensitivity and is subject to strict access controls
    - Unauthorized disclosure could result in extreme harm, such as threats to national security
    - Examples: Sensitive security details, military buildings, and information relevant for military planning

# Thank you!

Metropolia