ISO19650-5 Security-minded approach

Managing and Sharing Construction Data

Computing in Construction

Metropolia

Metropolia

ISO 19650 – Security issues

ISO 19650-1 – Part 1: **Concepts and principles** (2018)

- The concepts and principles of the information management process.

ISO 19650-2 – Part 2: **Delivery phase of assets** (2018)

- The process for the management and collaborative production of information during the delivery phase of assets.

ISO 19650-3 – Part 3: **Operational phase of assets** (2020)

- The process for the management and collaborative production of information during the operational phase of assets.

ISO 19650-4 – Part 4: **Information exchange** (2022)

- Recommended concepts and principles for the exchange of information between parties throughout the lifecycle of an asset.

Across project consortium

ISO 19650-5 – Part 5: **Security-minded approach to IM** (2020)

- A framework for a security-minded approach to managing information relating to sensitive assets.

ISO 19650-6 – Part 6: **Health and safety** (work in progress)

- Expected to concern the production and management of health and safety information on built environment projects.

Within single organization

ISO/IEC 27001 – Information security, cybersecurity and privacy protection - **Information security management systems** - Requirements (2022)

- Information security requirements for an individual organization, organizational department or system.

Security-minded approach (SMA)

- *"A security-minded approach encompasses*
  - *personnel,*
  - *physical and*
  - *cyber security*
- *as well as a*
  - *clear governance structure with*
  - *good accountability and responsibility*
- *to mitigate security risks"*

Motivations

Sharing information securely without inhibiting collaboration

Appropriate and proportionate approach to security across the project lifecycle

Metropolia

threat
potential cause of an incident which may result in harm

vulnerability
weakness that can be exploited to cause harm

safety
state of relative freedom from *threat* or harm caused by random, unintentional acts or events

security
state of relative freedom from *threat* or harm caused by deliberate, unwanted, hostile or malicious acts

security incident
suspicious act or circumstance threatening *security*

security breach
infraction or violation of *security*

Metropolia

sensitive information

information, the loss, misuse or modification of which, or unauthorized access to, can:

- adversely affect the privacy, *security* or *safety* of an individual or individuals
- compromise intellectual property or trade secrets of an organization;
- cause commercial or economic harm to an organization or country; and/or
- jeopardize the security, internal and foreign affairs of a nation

security-minded

understanding and routinely applying appropriate and proportionate *security* measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities

Metropolia

ISO/IEC 27001 Information security management systems – Requirements (2005 – 2022)

Metropolia

ISO/IEC 27001 Information security controls

ISO/IEC 27001 Appendix 1

- Organizational controls (37)
- People controls (8)
- Physical controls (14)
- Technological controls (34)

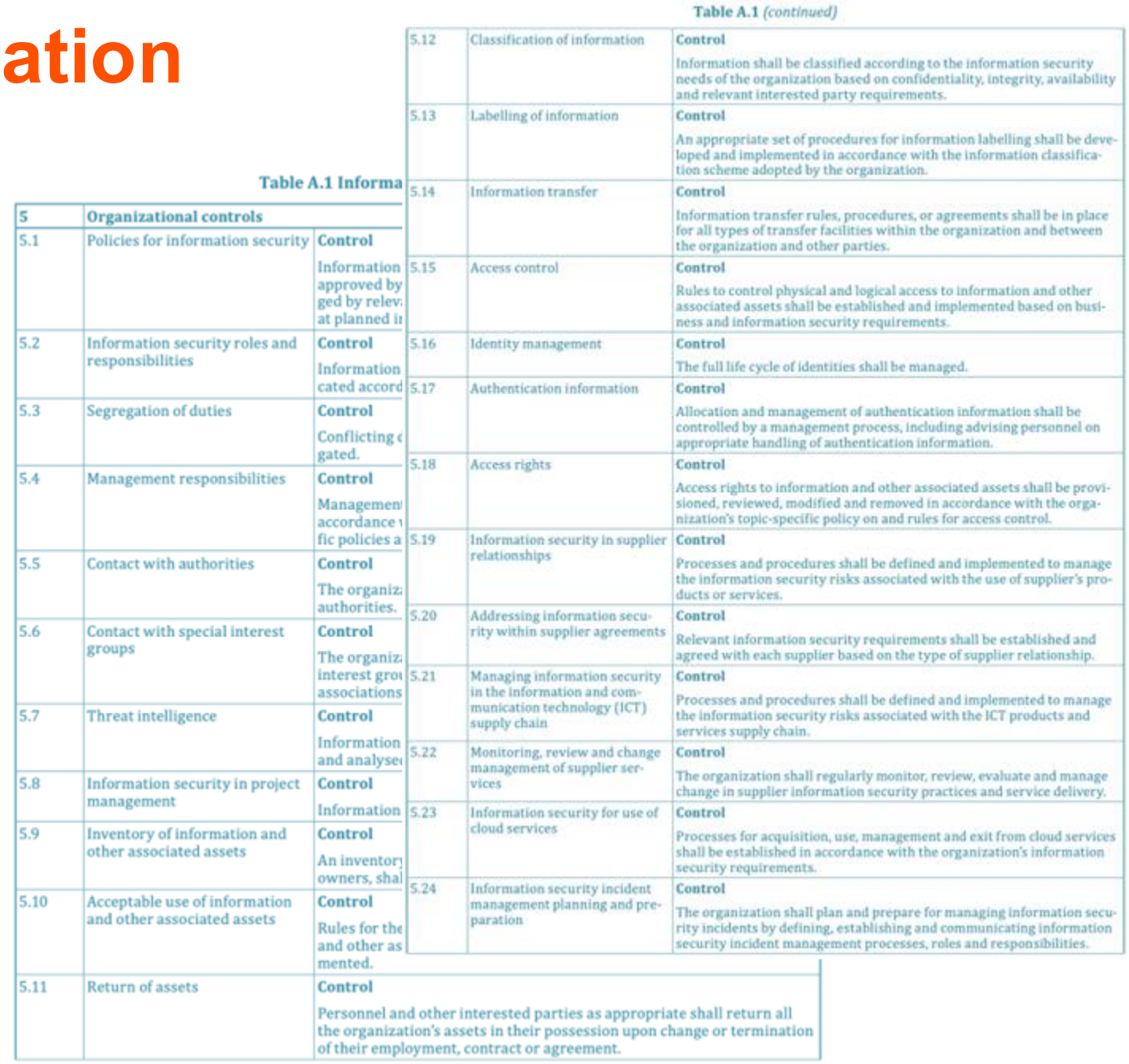


Table A.1 Informa

5	Organizational controls	
5.1	Policies for information security	**Control** Information approved by ged by relev at planned i
5.2	Information security roles and responsibilities	**Control** Information cated accord
5.3	Segregation of duties	**Control** Conflicting gated.
5.4	Management responsibilities	**Control** Managemen accordance fic policies a
5.5	Contact with authorities	**Control** The organiz authorities.
5.6	Contact with special interest groups	**Control** The organiz interest gro associations
5.7	Threat intelligence	**Control** Information and analyse
5.8	Information security in project management	**Control** Information
5.9	Inventory of information and other associated assets	**Control** An inventor owners, sha
5.10	Acceptable use of information and other associated assets	**Control** Rules for the and other as mented.
5.11	Return of assets	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Table A.1 *(continued)*

5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
5.13	Labelling of information	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
5.15	Access control	**Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.18	Access rights	**Control** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
5.19	Information security in supplier relationships	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
5.20	Addressing information security within supplier agreements	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review and change management of supplier services	**Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Metropolia

ISO/IEC 27001 Information Security Management System

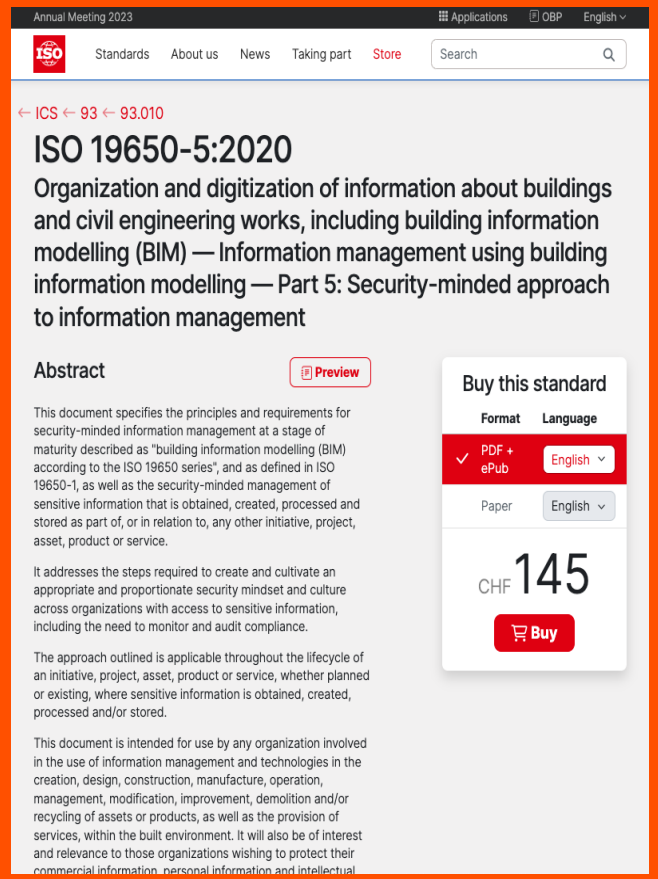
- Comprehensive list of security controls (93)

- Systematic approach to
  - examine security risks (threats, vulnerabilities, impacts)
  - design and implement coherent set of security controls to mitigate the risks
  - document security policies
  - involve the top management to the process
  - implement continuous improvement process to ensure ongoing security

- ISO/IEC 27001 Certification
  - also adds compliance with GDPR

- Widely recognized internationally
  - first version published 2005
  - can be integrated with other standards (e.g., ISO 9001, ISO 14001)

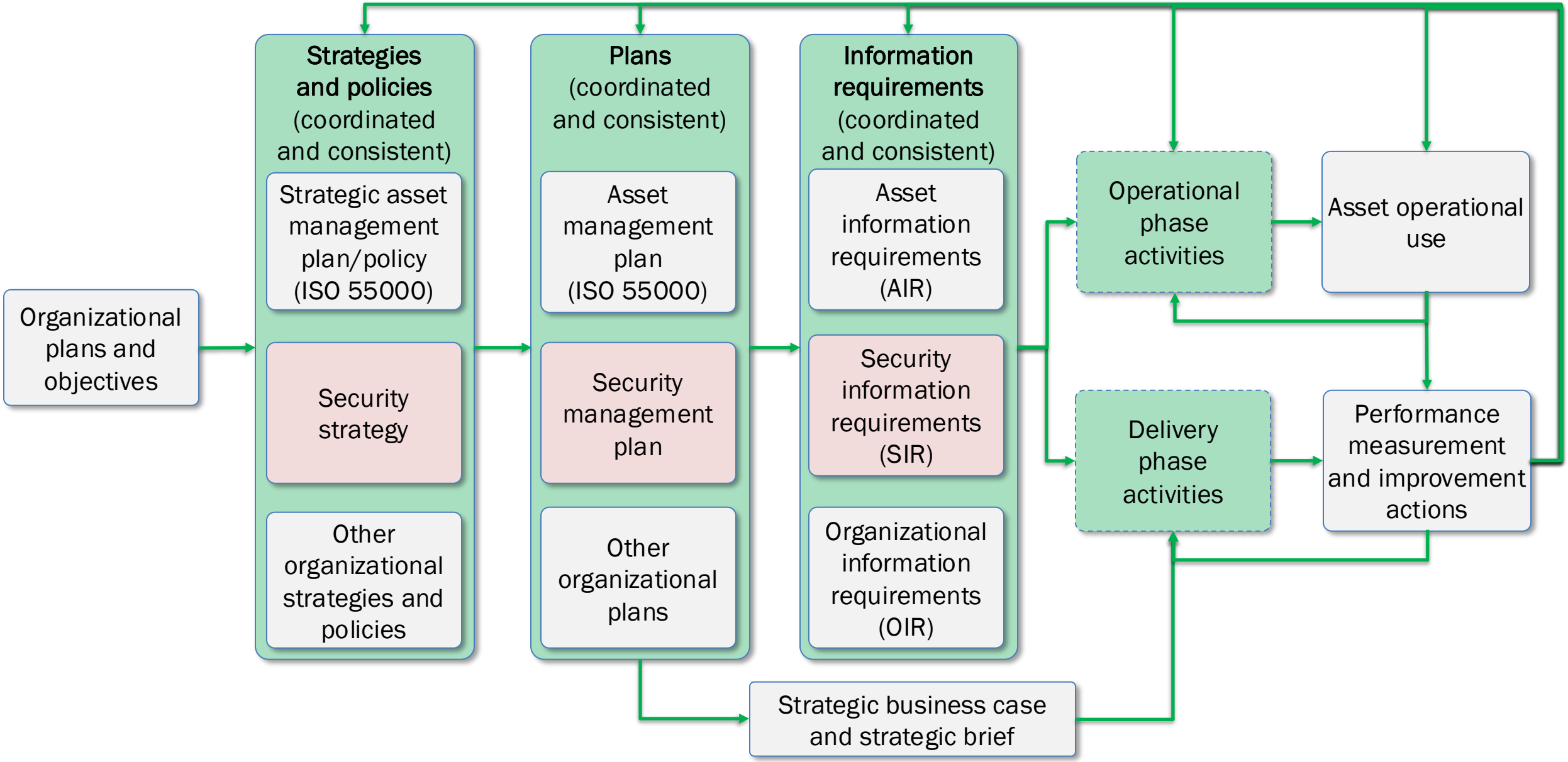
Metropolia



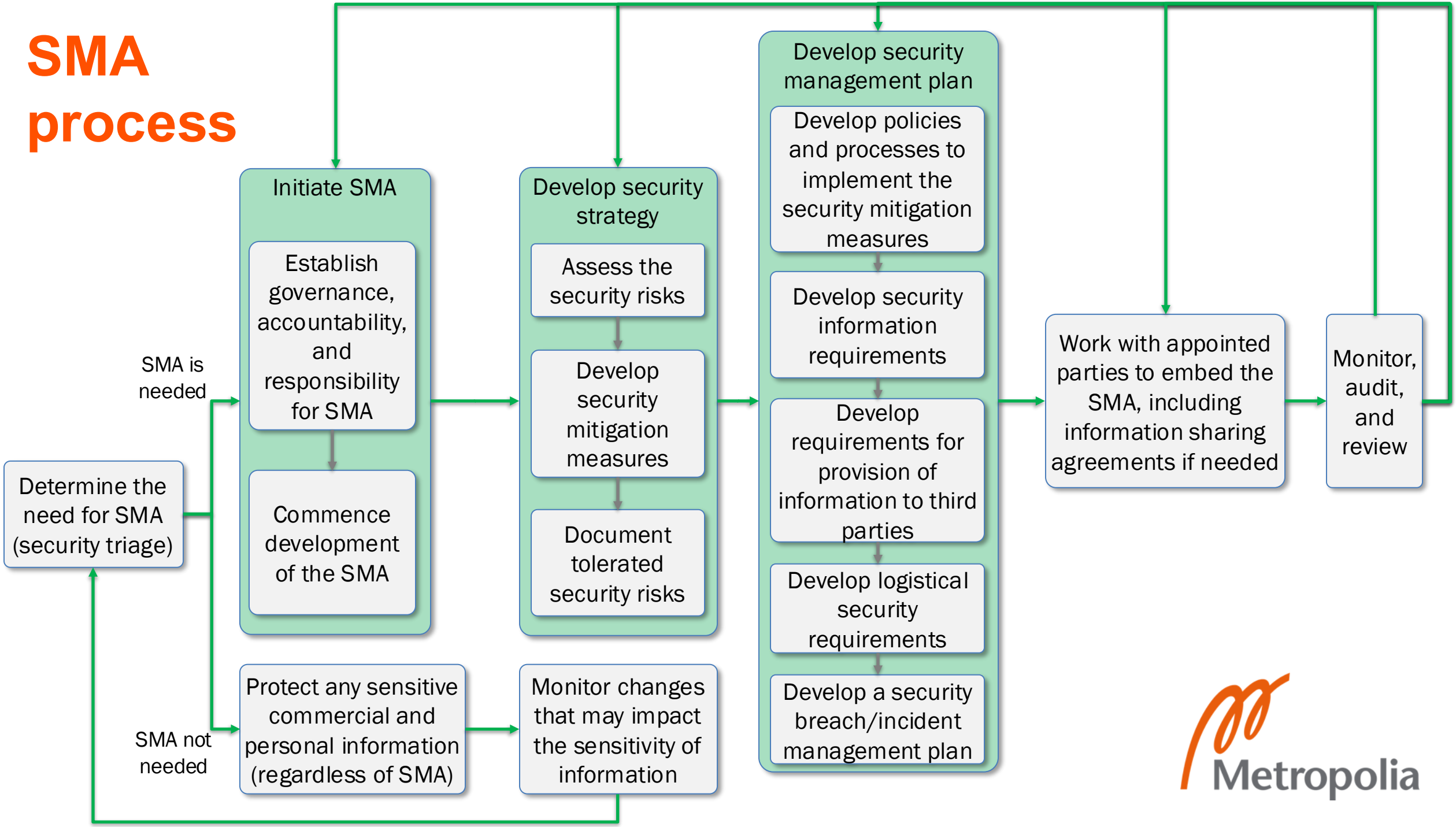
ISO 19650-5 Information management using building information modelling — Part 5: Security-minded approach to information management (2020)

Metropolia

Integrating the SMA within the BIM process

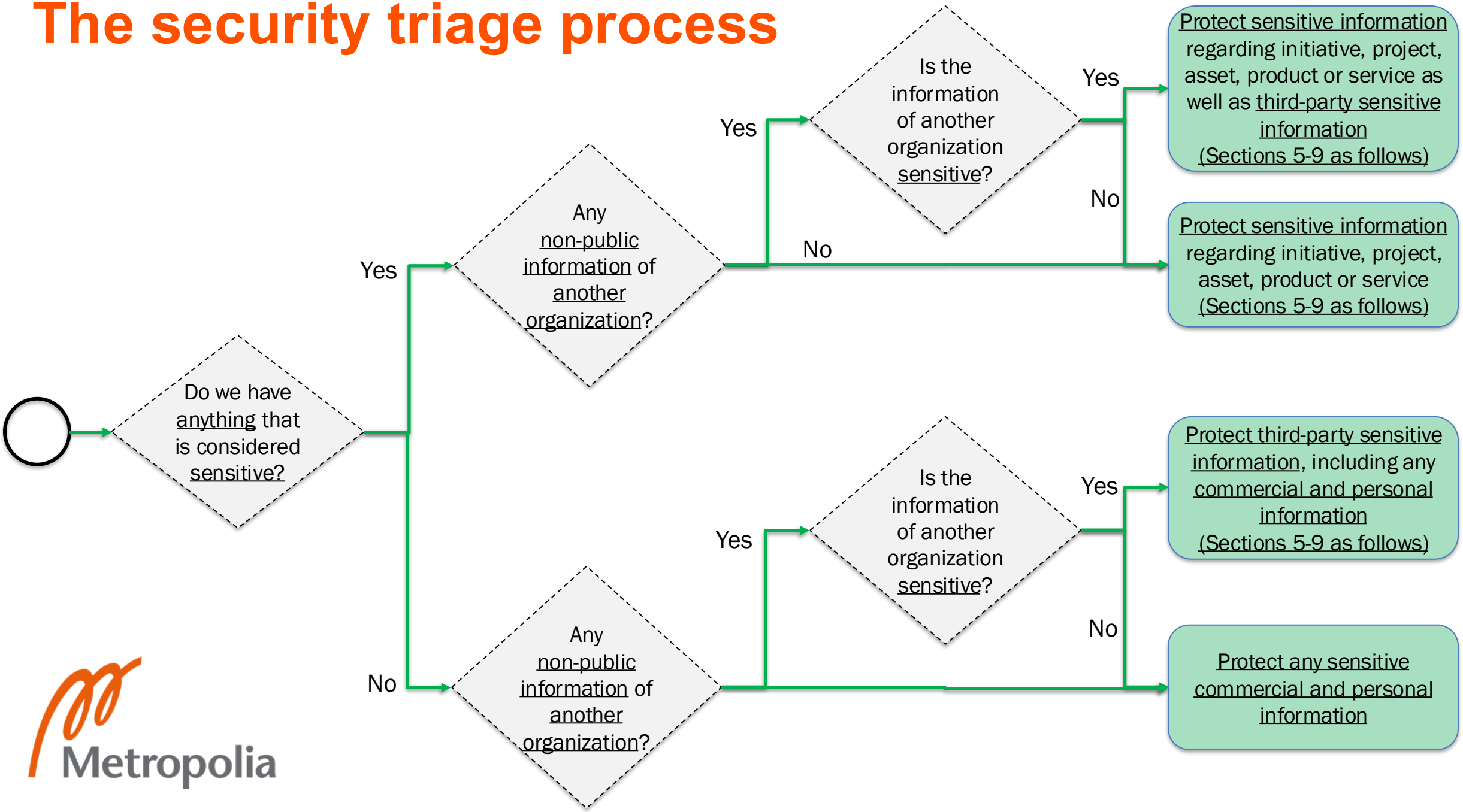


SMA process



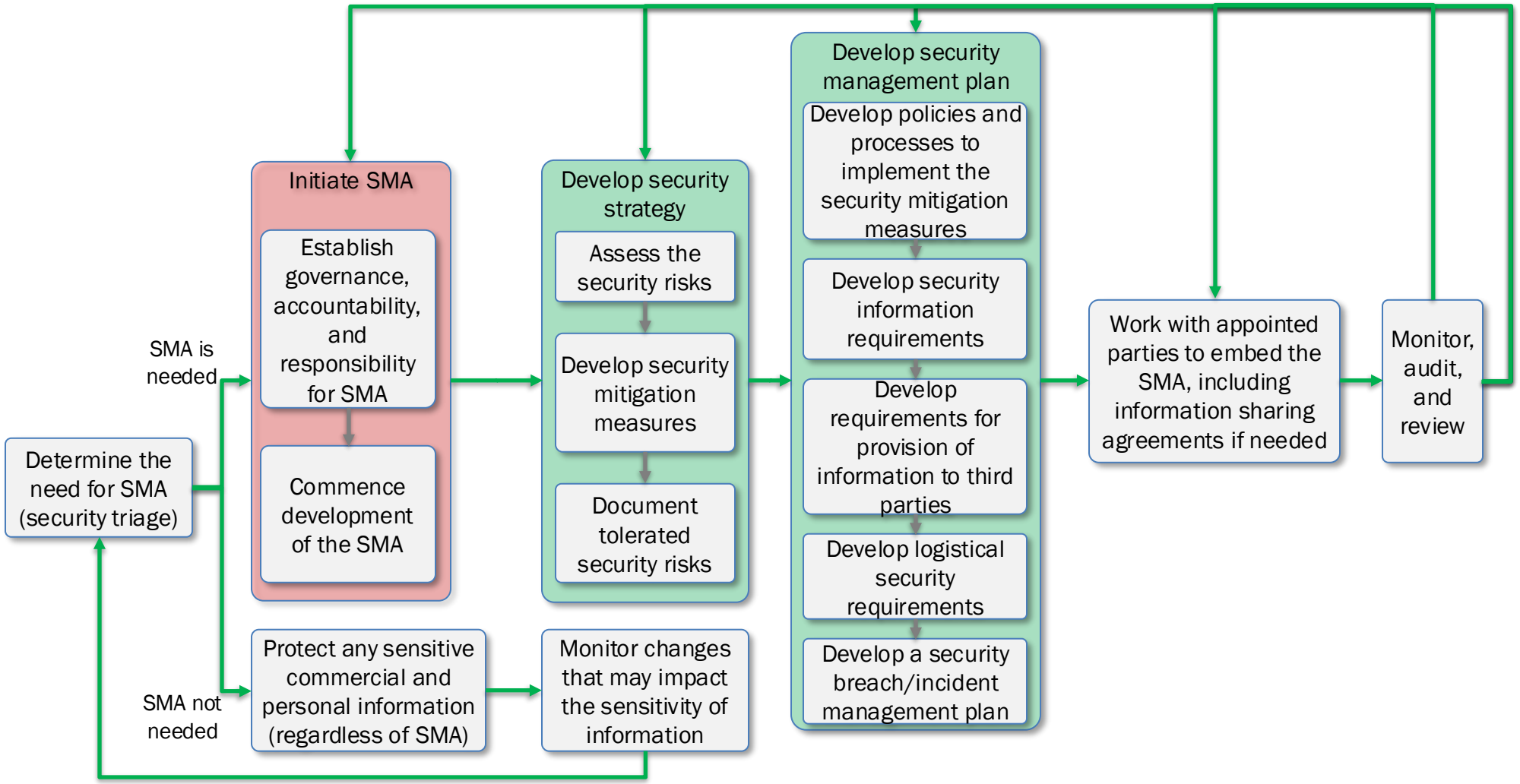
Metropolia

The security triage process



Metropolia

Section 5: Initiating the security-minded approach



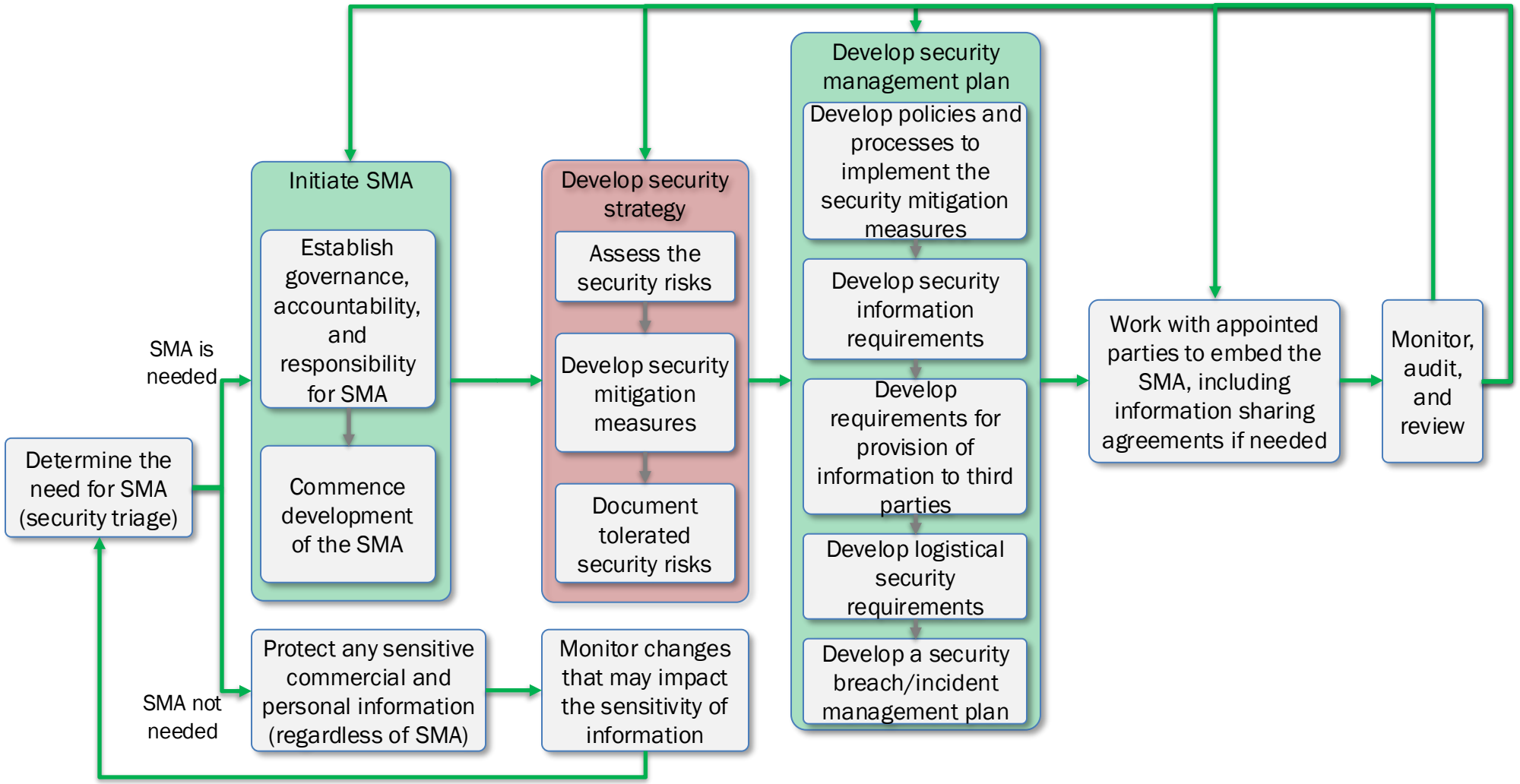
Metropolia

Section 5: Initiating the security-minded approach

- Establishing governance, accountability and responsibility for the SMA
  - accountable individual at top management
  - when collaboration with other organizations, for each
    - create the governance structure
    - agree on how to split the leadership
    - appoint the accountable individuals
    - review and update the governance structure when needed
  - appoint individuals to
    - providing a holistic view of the security threats and vulnerabilities
    - guide the handling of the resultant security risks;
    - develop a security strategy
    - develop and implement a security management plan
    - embed the security requirements into any procurement/appointment;
    - promote the security-minded culture
    - brief third parties about security policies
    - oversee the development and testing of security policies and processes
    - contact security experts, if needed
- Commencing the development of the security-minded approach
  - SMA should be developed as early as possible
    - in each planning stage
    - alongside with other requirements (OIR, AIR, PIR, EIR)

Metropolia

Section 6: Developing a security strategy



Metropolia

Section 6: Developing a security strategy

- A security strategy should include
  - the outcome of the security triage process
  - the governance, accountability and responsibility arrangements for the SMA
  - the assessment of the security risks from
    - the greater availability of information,
    - integration of services and systems, and
    - the increased dependency on technology-based systems
  - the potential risk mitigation measures to address the security risks
  - the tolerated security risks and
  - the mechanisms for reviewing and updating the security strategy

- The security strategy should
  - take into consideration the relevant legislative requirements and standards
  - be approved by the top management of the organization(s)
  - be under restricted access regarding any part that identifies sensitive information
    - a strict need-to-know basis

Metropolia

Section 6: Developing a security strategy

- Assessing security risks
  - potential threats
  - potential vulnerabilities
  - the nature of the harm which can be caused, and
  - the likelihood that a vulnerability will be exploited
- Developing security risk mitigation measures
  - identify and record possible mitigation measures for each risk
    - mitigation measures can utilize information management controls (listed in appendix)
  - mitigation measures should be evaluated and selected for adoption
    - the cost of implementing the mitigation measure
    - the risk reduction achieved
    - the predicted cost impact
    - impacts on the asset of the mitigation measure
      - usability, efficiency and appearance
    - the potential for the measure to create further vulnerabilities, and
    - the potential business benefits of the measure

Metropolia

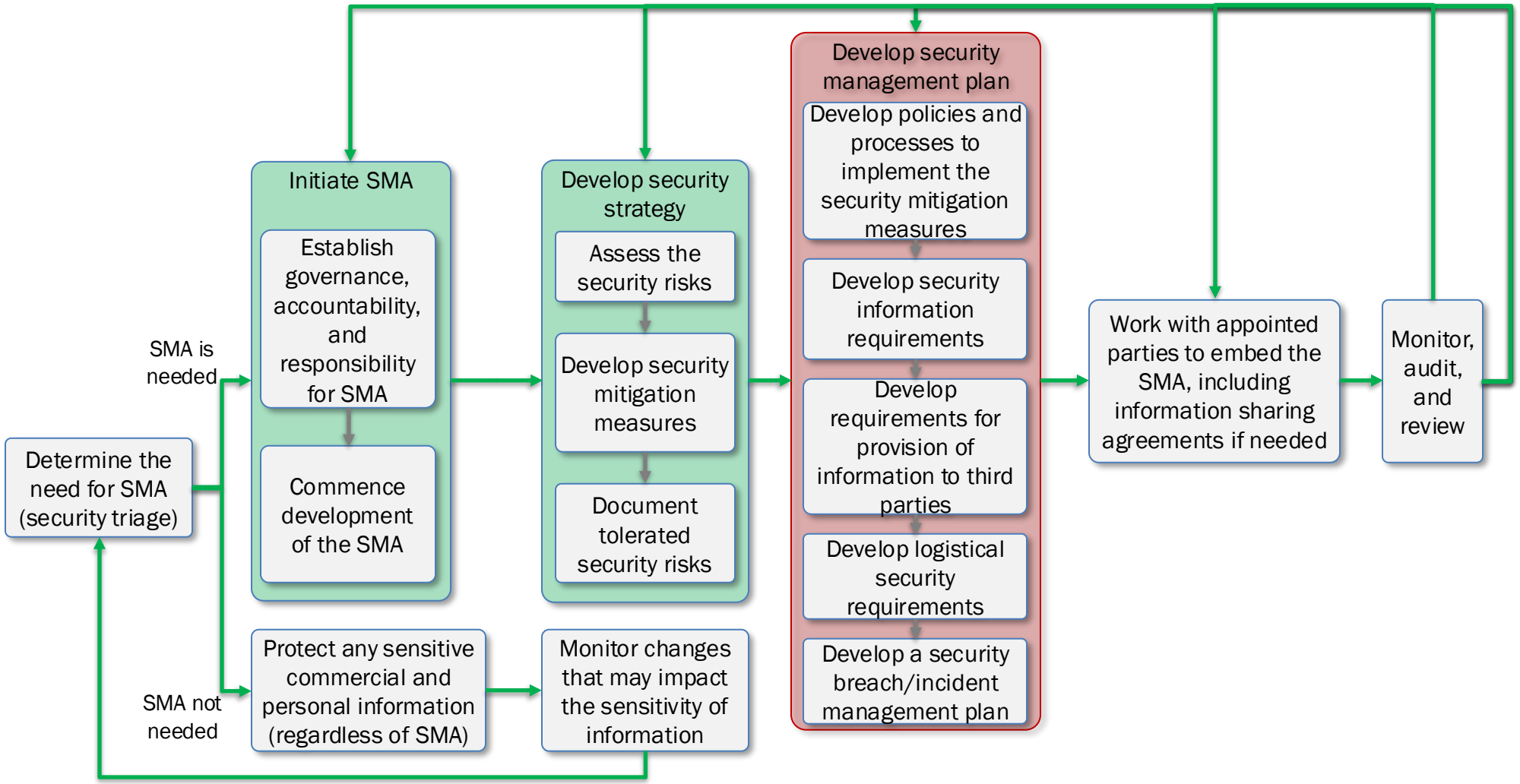
Section 6: Developing a security strategy

- Documenting residual and tolerated security risks
  - record and document
  - continue assessment

- Review of the security strategy
  - mechanism for periodic and event-driven reviews
    - with significant changes in the surroundings
    - when new vulnerabilities are revealed
  - consider potential impact in ongoing appointments
    - especially scope changes
  - following a review
    - update the security strategy
    - document the review as part of the strategy
  - maintain the access on a strict need-to-know basis

Metropolia

Section 7: Developing a security management plan



Metropolia

Section 7: Developing a security management plan

- The security management plan should contain
  - the policies derived from the agreed mitigation measures
  - the processes derived from the security policies
  - the security information requirements defining sensitive information
  - the requirements to share information with others
  - where applicable, logistical security requirements
  - a security breach / incident management plan
  - details of accountability and responsibility for the security management plan
  - monitoring and auditing requirements
  - the mechanisms for reviewing and updating the security management plan

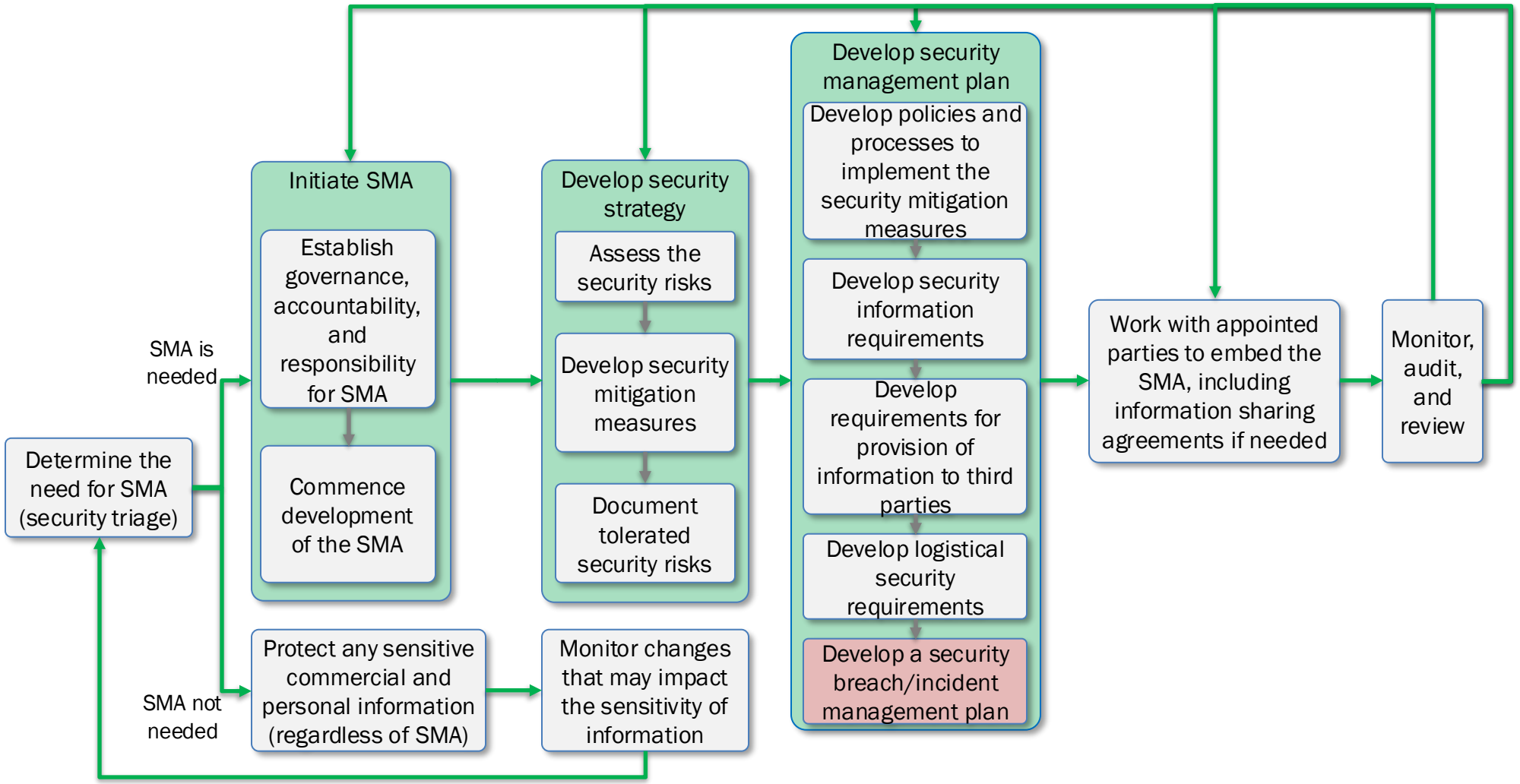
Metropolia

Section 7: Developing a security management plan

- Sharing information with third parties
  - required assessment before sharing
    - the need to comply with regulatory and statutory process
    - needs from public access or transparency legislation
    - needs of marketing, technical, academic, etc. publications
  - assessment should consider whether the information
    - contains sensitive information
    - allows sensitive information to be deduced;
    - helps to determine the pattern-of-use of an asset or the pattern-of-life of individuals or groups not otherwise publicly available
- Logistical security of sensitive security-related assets
  - timing of the installation to limit access to them
  - security measures around assets installed early
  - limit physical hostile reconnaissance
- Monitoring and auditing
- Review of the security management plan

Metropolia

Section 8: Security breach/incident management plan



Metropolia

Section 8: Security breach/incident management plan

- The security breach/incident management plan should include:
  - an assessment of what security breaches/incidents can occur, with their
    - risks and
    - impacts on the organization
  - the process to be followed on a security breach/incident, including
    - business continuity measures
    - recovery actions
    - collection of evidence
  - the review process after a security breach or incident; and
  - the mechanisms for reviewing and updating the security breach/incident management plan

- Access on a strict need-to-know basis
  - especially the parts of the plan that record the risks to the organizations

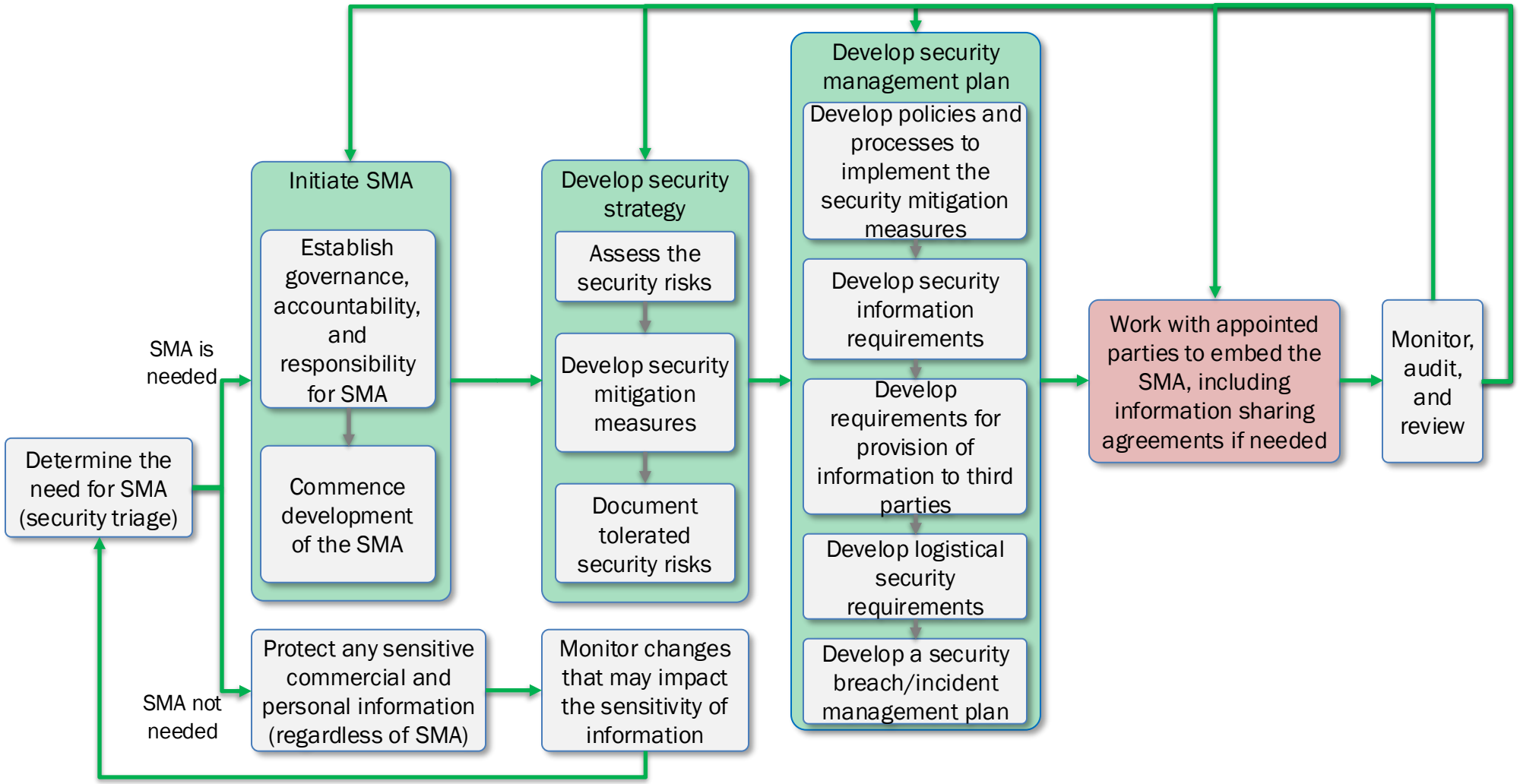
Metropolia

Section 8: Security breach/incident management plan

- Specify what to do on discovery of a security breach or incident
  - the persons to be contacted immediately
  - the processes used to identify the concerned parties
  - the mechanisms to notify concerned parties and information to be provided; and
  - handling any third party in the event of a security breach or incident
    - regulator, media or public interest
- How to contain and recover
  - measures to reduce further damage
  - assessment of what has happened
    - what has been lost, compromised, damaged or corrupted
  - specify circumstances when collection of evidence for law enforcement purposes is needed
    - when forensic readiness measures are needed
- Review following a security breach or incident
  - assessment of the ongoing risk
  - update policies and processes to prevent reoccurrence
  - if needed, require collaboration from delivery teams

Metropolia

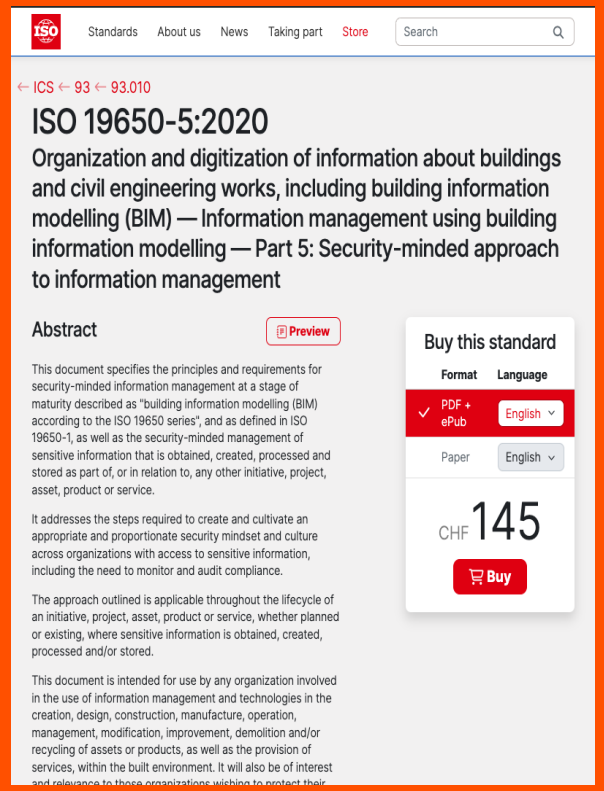
Section 9: Embed the SMA to appointments' work



Metropolia

Section 9: Embed the SMA to appointments' work

- Before formal appointment
  - information sharing agreements, if needed
  - protect sensitive information in tendering
  - evaluate tenders from information security perspective
    - evaluate the security training and support requirements of parties
- Measures contained in appointment documentation
  - manage the security risks of a delivery team
    - the appointment documentation details the security plans, policies and processes
    - detailed allocation of information security function in the delivery team is agreed
  - requirement to pass the security requirements to sub-appointments
  - clear indication of security compliance needs in the appointment documentation
    - requirement to assist in any security breach/incident investigation and follow-up
  - appointment should allow adjustment in case of changes in the surroundings
  - requirement for sufficient decommissioning and demobilization processes
    - requirement for disposal of shared information
- Post appointment award
  - monitor and enforce security-related provisions
- End of appointment
  - check the compliance of a delivery team
    - the delivery, storage, disposal and destruction of sensitive information



ISO19650-5 Appendix: Security controls

Metropolia

ISO 19650-5 Information security controls

Personnel aspects

a) identification of high-risk functions – related to security strategy, sensitive assets, ...
b) security screening and vetting of individuals in contact of sensitive assets
c) security competence requirements
d) induction of all new personnel and contracted organizations to their requirements and security-minded culture
e) general security training and awareness
f) role-based security training
g) ongoing security training requirements
h) access and permission requirements to information
i) demobilization of organizations and personnel

ISO 19650-5 Appendix B

Metropolia

ISO 19650-5 Information security controls

Physical aspects

a) physical security measures at sensitive locations
b) where applicable, physical security measures at built assets
c) where applicable, protection of neighboring built assets not otherwise generally visible and/or accessible; and
d) protective measures required for computing, electronic devices and equipment

Metropolia

ISO 19650-5 Information security controls

Technological aspects

a) the cyber security of systems capturing, processing and storing sensitive information;
b) the security of interconnections and interactions between such systems;
c) the security around systems controlling physical assets;
d) the permissible interoperability of systems and resilience of each system to failure;
e) configuration management and change control processes and procedures for systems;
f) the secure disposal of information and access held by organizations no longer worked with
g) secure disposal of legal/regulatory information after the period of retainment is over.

The systems used for capturing, processing and/or storing sensitive information

- should be secure by default or
- the system settings configured to maximize protection of that information.

Metropolia

ISO 19650-5 Information security controls

Software selection – sensitive systems: evaluation criteria

a) confidentiality;
b) availability (including reliability);
c) safety;
d) resilience;
e) possession;
f) authenticity;
g) utility
h) integrity (completeness, accuracy, consistency, coherence and configuration)

IoT systems

- understand the security architecture
- determine how it meets the security requirements
- assess security risks
- put in place security risk mitigation measures

Metropolia

ISO 19650-5 Information security controls

Information security

a) requirements for inspections facing sensitive information;
b) secure storage, access, and disposal of information
c) limits to the maximum amount of sensitive information to store or exchange;
d) embedding the requirements of external sensitive information;
e) protection against loss, disclosure, corruption, or loss of access or unauthorized changes to information
f) monitoring and recording changes to processes and technologies

Policies should be applicable across the generic information lifecycle

a) capture
b) acquisition
c) maintenance
d) synthesis
e) usage
f) archival
g) publication
h) purging

Metropolia

Assessments when providing information to third parties

a) Who will have access to the information?
b) Should other parties and stakeholders be consulted before sharing?
c) What is the justification for sharing? In particular:
    1) the objective;
    2) the potential benefits;
    3) the risks if not shared;
    4) sharing is proportionate to the objective and benefits; and
    5) whether the objective and benefits can be achieved without sharing;
d) What is the authority to share the information? In particular:
    1) Does the organization have the right, legal authority and power to do so?
    2) Are there any legal obligations to share?
    3) Was provided in confidence?
e) Any other information protection issues;
f) What are the security risks with sharing? Do they exceed the risk appetite of the organization(s)?
g) What are appropriate and proportionate security risk mitigation measures?
h) What is the willingness and capability of the party receiving to manage the information appropriately?
i) Are there any residual security risks and remaining information protection issues?

If intolerable risks or vulnerabilities are identified, sharing should be prohibited until appropriate mitigation measures are implemented.

Metropolia

Thank you!

Metropolia