CPNI
Centre for the Protection
of National Infrastructure

# INTRODUCTION TO BS EN ISO 19650-5:2020

## SECURITY-MINDED APPROACH TO INFORMATION MANAGEMENT

# INTRODUCTION

BS EN ISO 19650-5:2020 is a specification for security-minded information management. It details and specifies the principles and requirements for security-minded management of sensitive information that is obtained, created, processed and stored as part of, or in relation to, an initiative, project, asset, product or service.

The increasing use of digital technologies, including Building Information Modelling (BIM), in the design, construction, manufacture, operation and management of assets or products, as well as the provision of services, within the built environment, is already having a transformative effect on the parties involved, a trend which is likely to continue, and leading to:

- increased levels of collaboration, within and across sectors;
- more transparent, open ways of working;
- capture of real-time information about asset use and condition; and
- sharing and use of digital data and information.

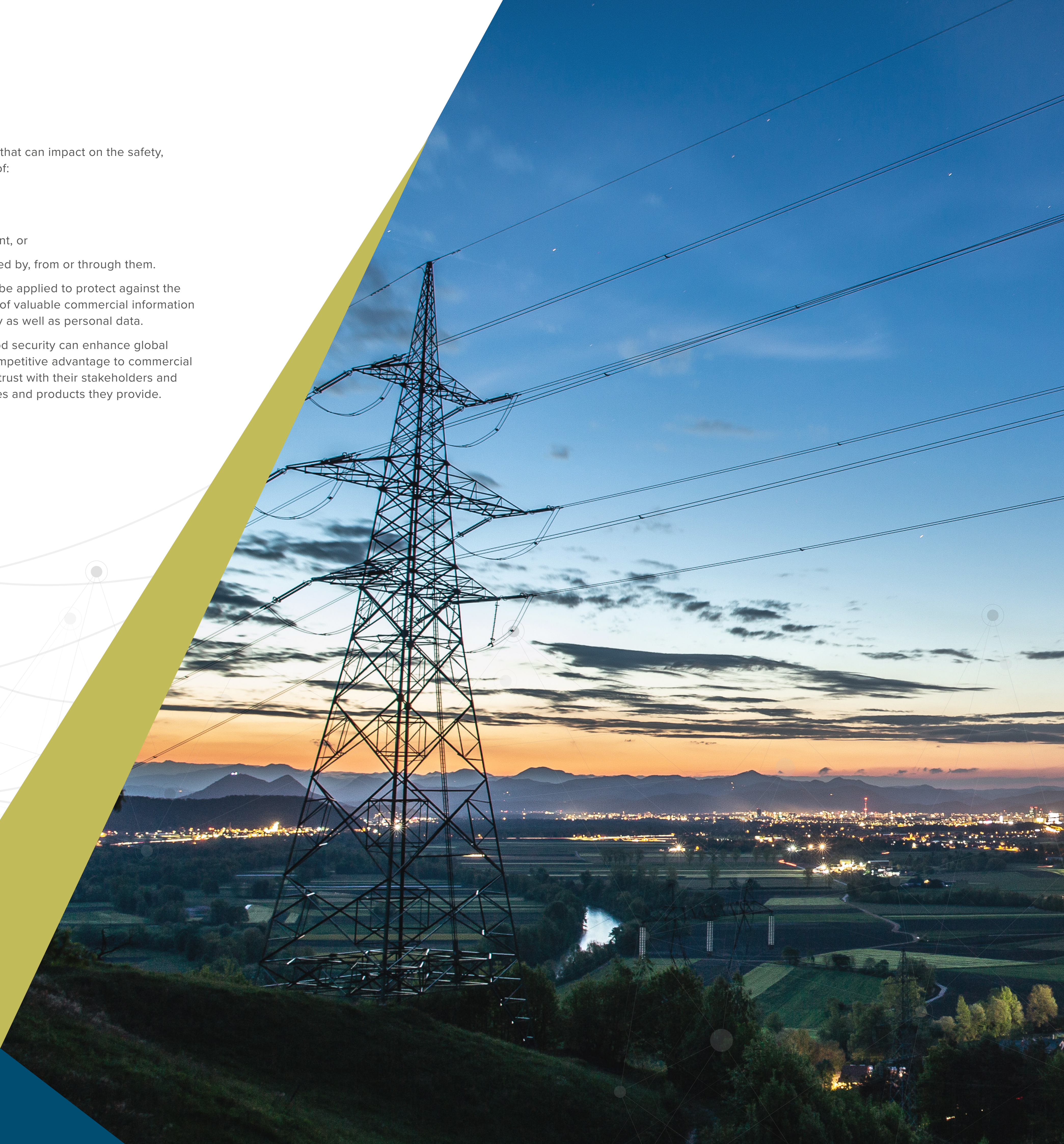
BS EN ISO 19650-5 provides a framework to assist organisations in understanding the key vulnerability issues and the nature of the controls required to manage the resultant security risks to a level that is tolerable to the relevant parties. Its use should not in any way undermine collaboration or the benefits that BIM, other collaborative work methods, and digital technologies can generate.

Implementation of the measures outlined in the ISO will assist in reducing the risk of the loss, misuse or modification of sensitive information that can impact on the safety, security and resilience of:

- assets;
- products;
- the built environment, or
- the services provided by, from or through them.

The measures can also be applied to protect against the loss, theft or disclosure of valuable commercial information and intellectual property as well as personal data.

Further, embedding good security can enhance global positioning and give competitive advantage to commercial enterprises by building trust with their stakeholders and customers in the services and products they provide.

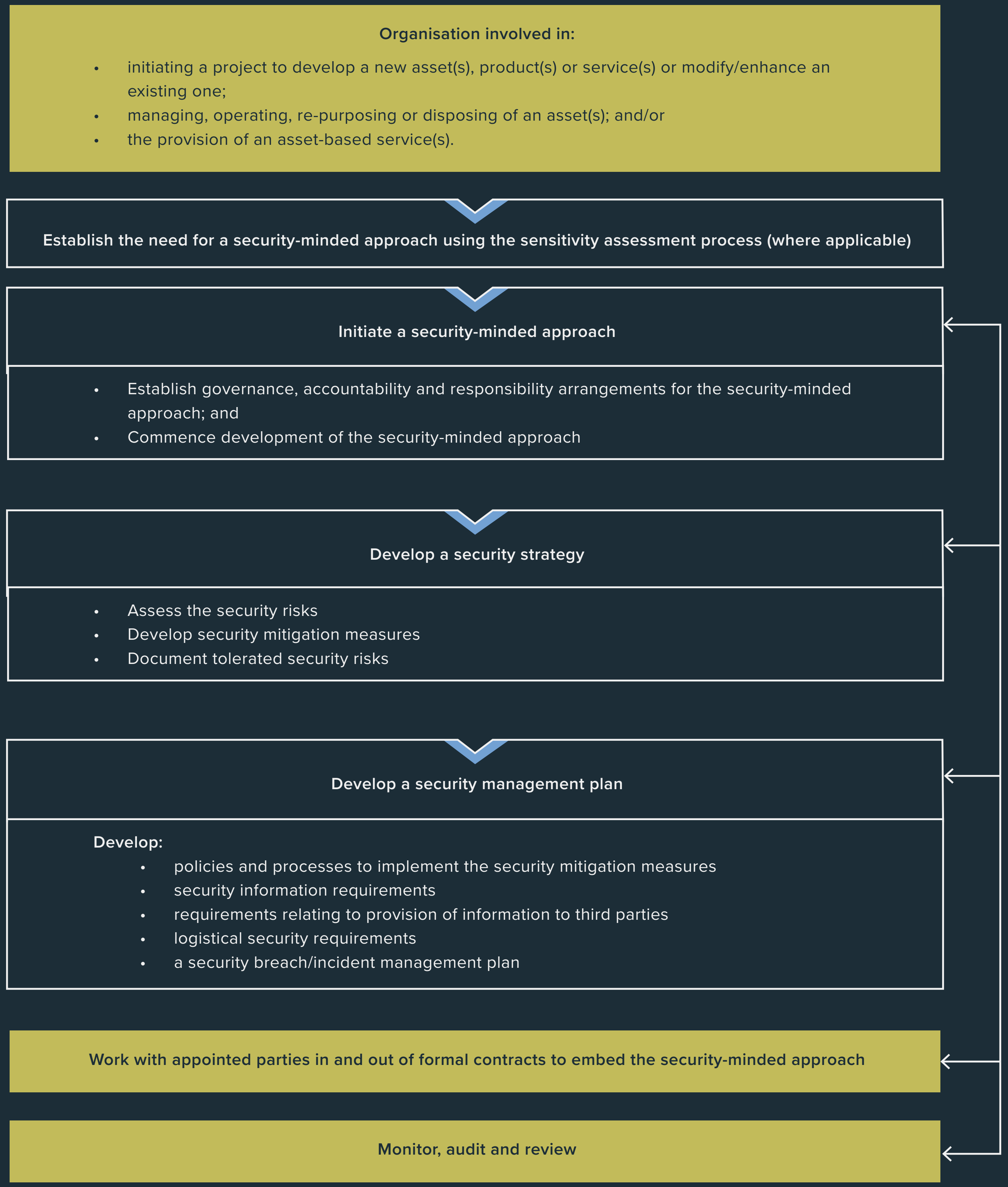


## WHO IS IT FOR?

BS EN ISO 19650-5 should be applied by any organisation involved in the use of information management and technologies in the creation, design, construction, manufacture, operation, management, modification, improvement, demolition and/or recycling of assets or products, as well as the provision of services, within the built environment.

It will also be of interest and relevance to other organisations wishing to protect their commercial information, personal information and intellectual property.

## SUMMARY OF THE PROCESS SET OUT IN **BS EN ISO 19650-5**



**Organisation involved in:**

- initiating a project to develop a new asset(s), product(s) or service(s) or modify/enhance an existing one;
- managing, operating, re-purposing or disposing of an asset(s); and/or
- the provision of an asset-based service(s).

**Establish the need for a security-minded approach using the sensitivity assessment process (where applicable)**

**Initiate a security-minded approach**

- Establish governance, accountability and responsibility arrangements for the security-minded approach; and
- Commence development of the security-minded approach

**Develop a security strategy**

- Assess the security risks
- Develop security mitigation measures
- Document tolerated security risks

**Develop a security management plan**

**Develop:**

- policies and processes to implement the security mitigation measures
- security information requirements
- requirements relating to provision of information to third parties
- logistical security requirements
- a security breach/incident management plan

**Work with appointed parties in and out of formal contracts to embed the security-minded approach**

**Monitor, audit and review**

# WHAT IS A SENSITIVE ASSET, PRODUCT OR SERVICE?

## Built assets

A built asset, in whole or in part, is sensitive if it:

a) forms part of the critical national infrastructure;

b) fulfils a defence, law enforcement or national security or diplomatic function;

c) is a commercial site involving the creation, trading or storage of significant volumes of valuable materials, currency, pharmaceuticals, chemicals, petrochemicals, or gases;

d) constitutes a landmark, nationally significant site or crowded place; and/or

e) is used or is planned to be used to host events of security significance.

## Assets, products and services

**An asset, product or service is sensitive if:**

- there is sufficient risk that it can be used to significantly compromise the integrity, safety, security and/or resilience of an asset, product or service, or its ability to function;
- the risk to the safety, security and/or privacy of individuals or communities or their personal information exceeds the risk appetite of the organisation.

If an asset, product or service does not fall into one or more of the categories described, there may be business benefits from applying a security-minded approach across its lifecycle.

# INITIATING A SECURITY-MINDED APPROACH

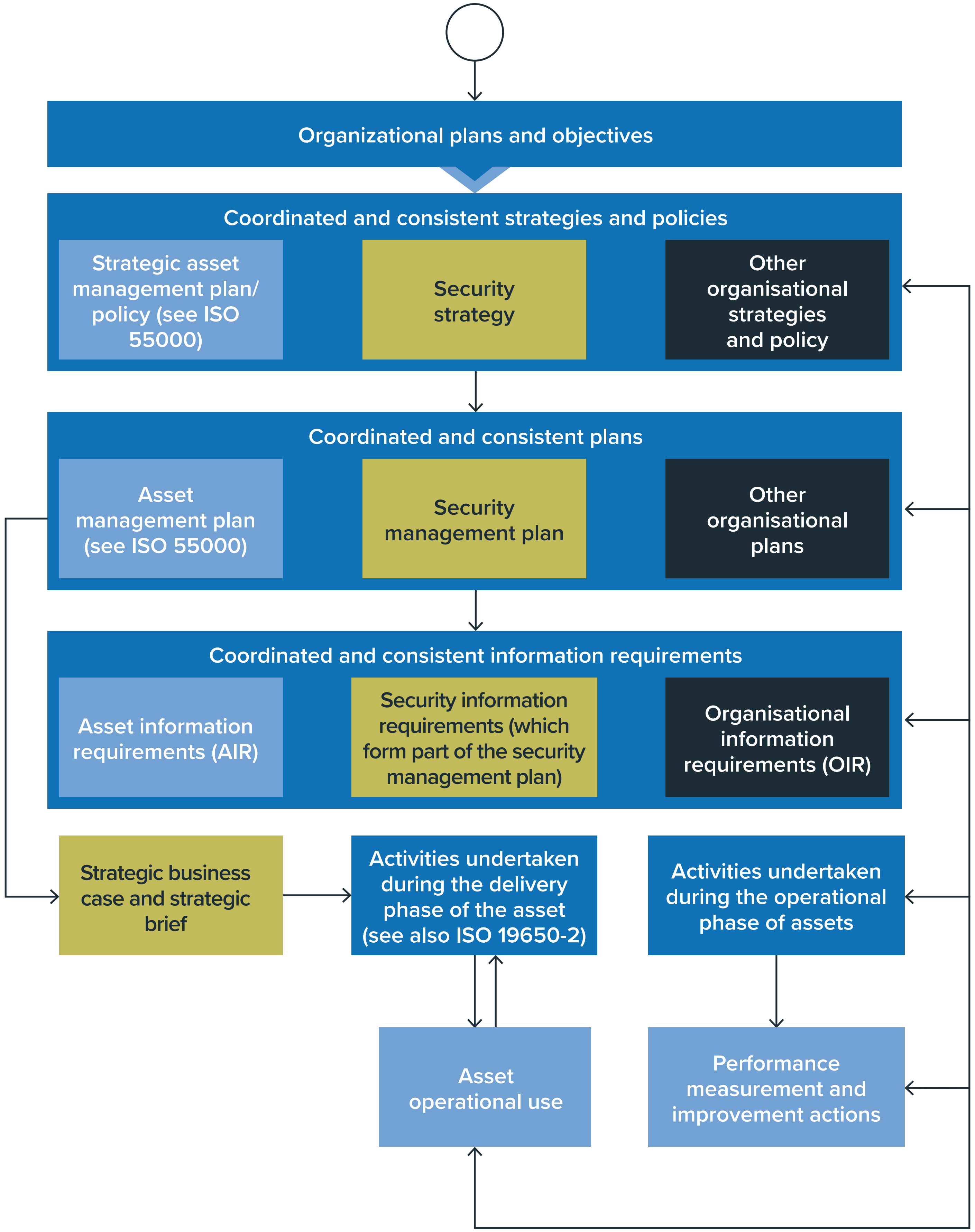
The initiation, development and implementation of a security-minded approach requires:

- creating a robust governance structure;
- appointing the individual(s) who will be accountable for the approach to be adopted; and
- defining the individual(s) responsible for implementing the different aspects of the approach.

# EMBEDDING SECURITY

If it is to be successful, the security-minded approach should be applied throughout the lifecycle of an initiative, project, asset, product or service, whether planned or existing, where sensitive information is obtained, created, processed and/or stored.

It should also be integrated with other organisational strategies, policies, plans.



Organizational plans and objectives

Coordinated and consistent strategies and policies

Strategic asset management plan/ policy (see ISO 55000)

Security strategy

Other organisational strategies and policy

Coordinated and consistent plans

Asset management plan (see ISO 55000)

Security management plan

Other organisational plans

Coordinated and consistent information requirements

Asset information requirements (AIR)

Security information requirements (which form part of the security management plan)

Organisational information requirements (OIR)

Strategic business case and strategic brief

Activities undertaken during the delivery phase of the asset (see also ISO 19650-2)

Activities undertaken during the operational phase of assets

Asset operational use

Performance measurement and improvement actions

**Disclaimer:**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards to the use of this document and seek independent professional advice on your particular circumstances.

**CPNI**

Centre for the Protection
of National Infrastructure

> INTRODUCTION TO BS EN ISO 19650-5:2020
SECURITY-MINDED APPROACH TO
INFORMATION MANAGEMENT