Security in an engineering context

Hugh Boyes CEng FIET

Bodvoc Ltd

a change in thinking is required
security is not a feature, but a necessity

Our infrastructure is a target

BIM
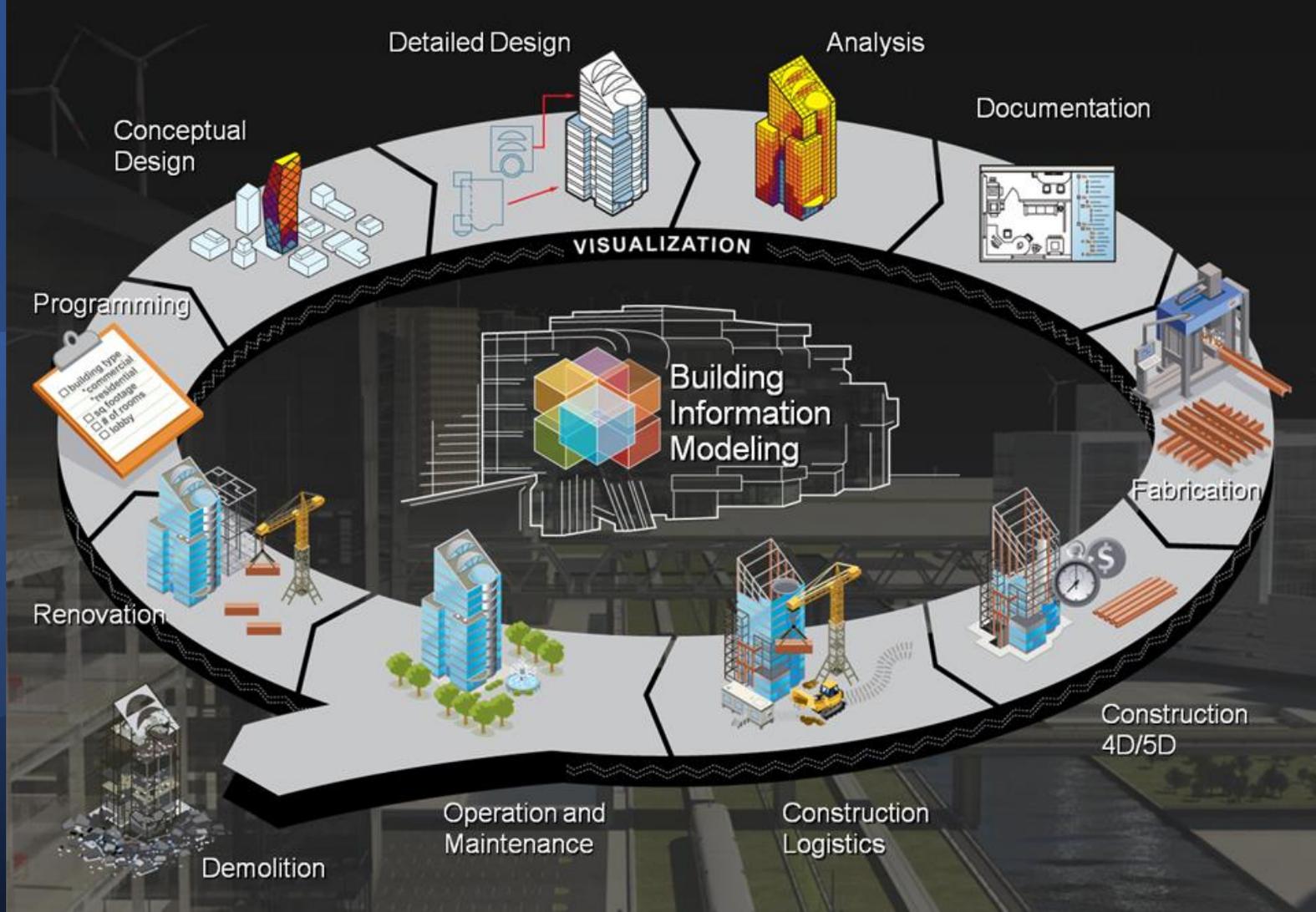
Sector-to-sector connections & dependence
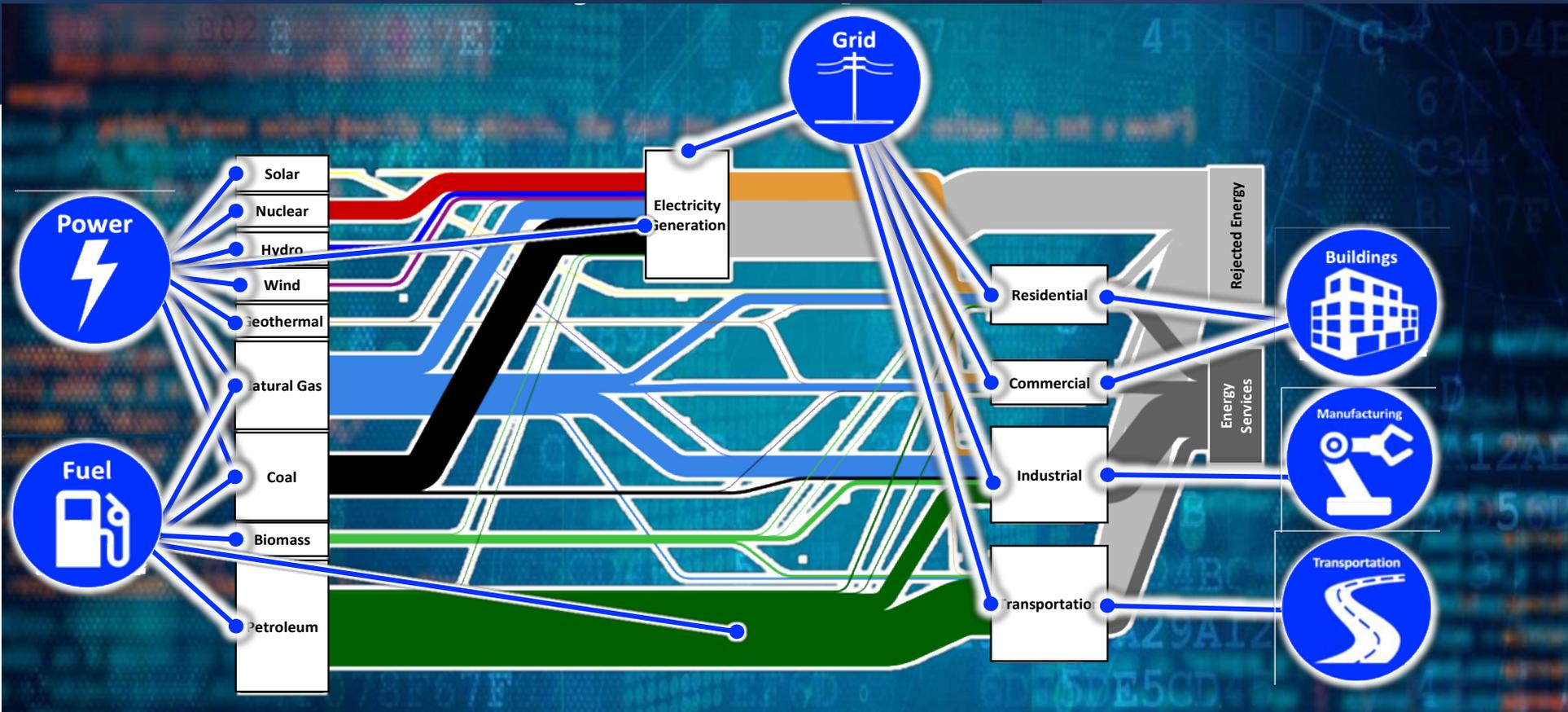
Digital planning of complex infrastructure
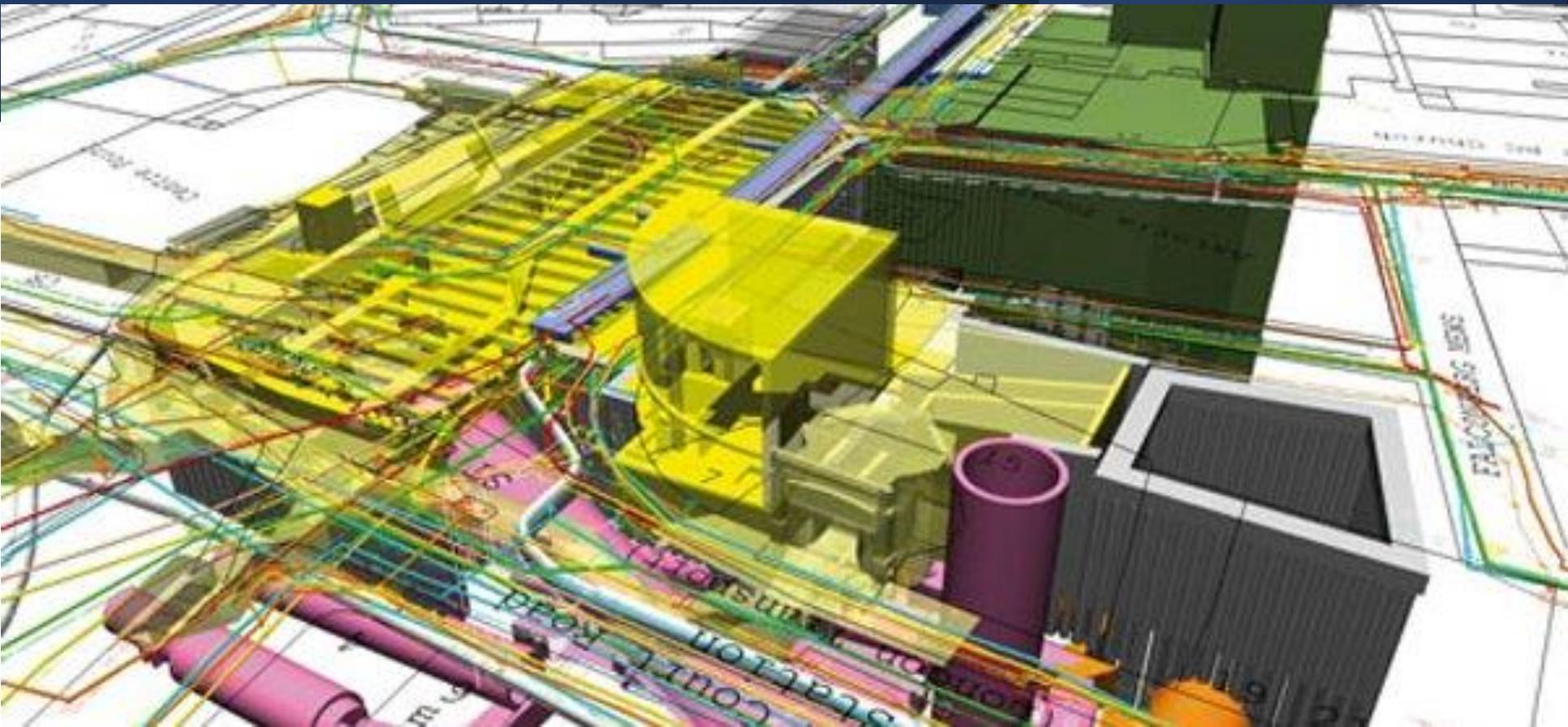
# Smart Cities and Digital Twins

Generic asset lifecycle

Conception → Pre-implementation → Implementation → Operation → Disposal
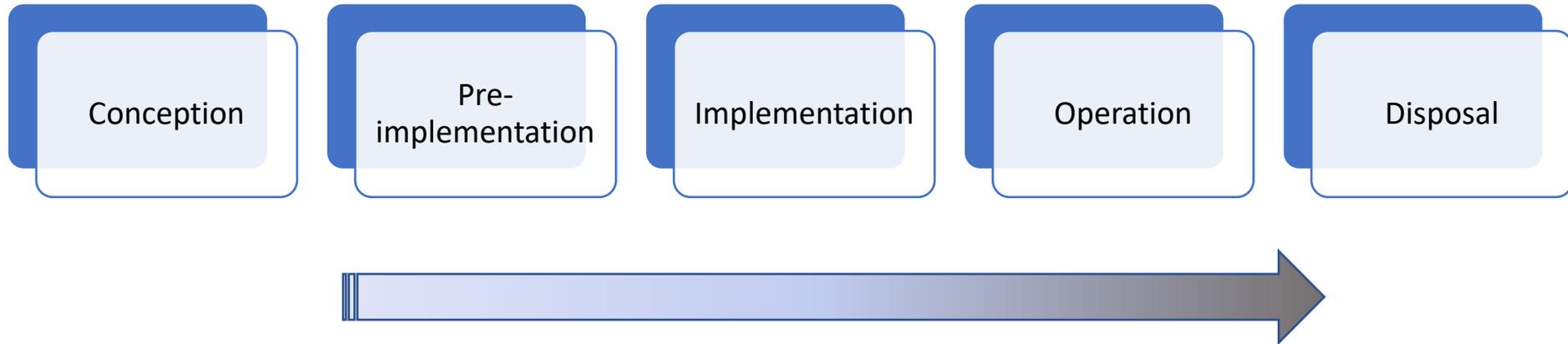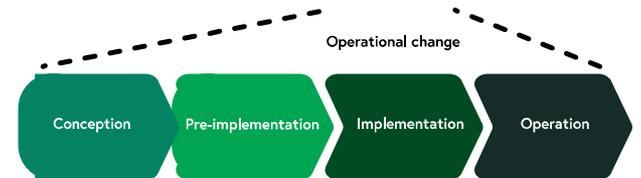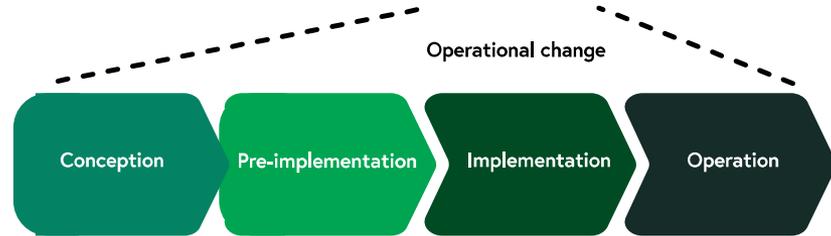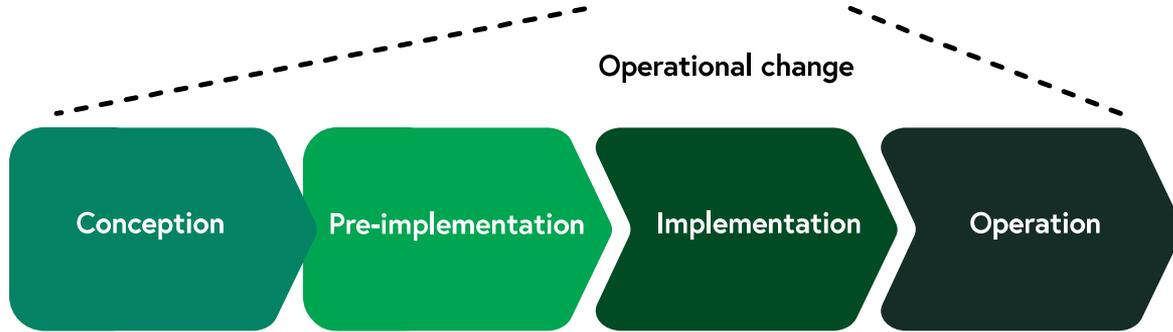
Managing security over the asset(s) lifecycle

THREAT AGENTS

Legend: Primary group for threat: ✔ (red) Secondary group for threat: ✔ (green)	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Insider threat	✔ (red)		✔ (green)	✔ (red)		✔ (green)	
Physical manipulation / damage / theft / loss	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (green)	✔ (green)	✔ (green)
Exploit kits	✔ (red)		✔ (red)	✔ (red)			
Data breaches	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (green)
Identity theft	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (red)	✔ (green)	✔ (green)
Information leakage	✔ (red)	✔ (green)	✔ (red)	✔ (red)	✔ (green)	✔ (green)	✔ (green)
Cyber espionage		✔ (green)	✔ (green)	✔ (green)			

Holistic Approach to Security

© 2019, Bodvoc Ltd
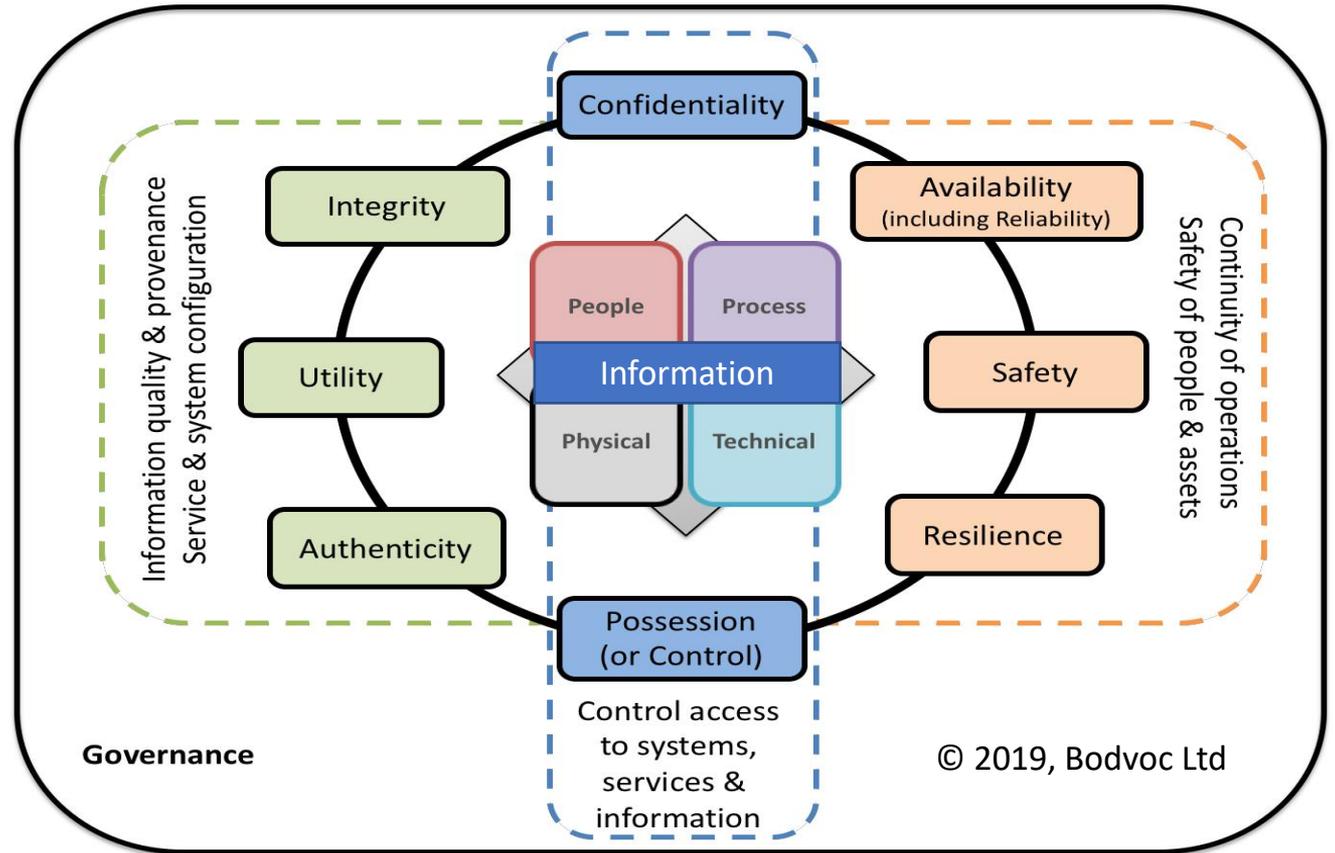
Asset-based risk management approach
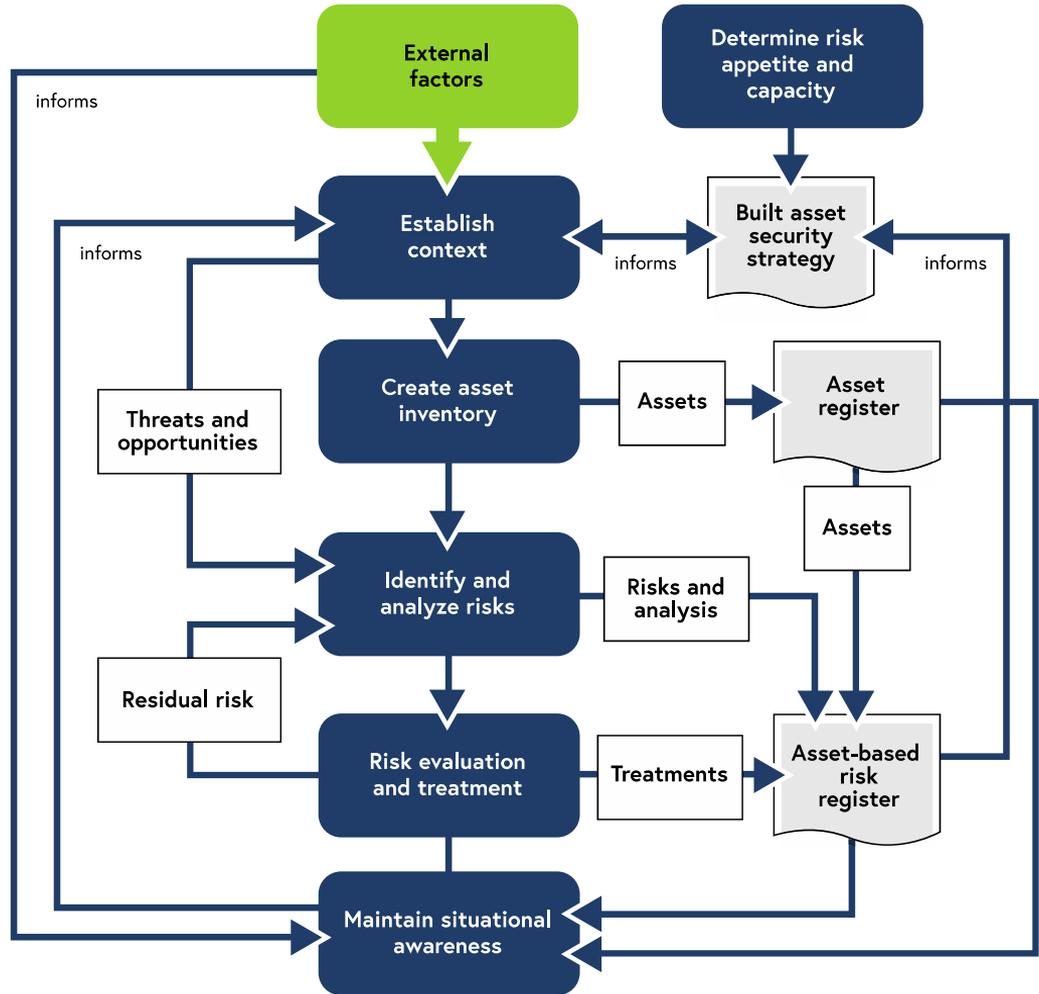
Information management vs Cyber security

- Covers the information lifecycle.
- Involves people and processes
- Lifecycle should be supported by appropriate measures to assure and maintain the quality of the organization's data and information.

- Covers the system lifecycle.
- Often focussed on technology and physical access
- System should maintain data and information integrity, i.e., prevent unauthorized changes, it does not assure the quality of the data and information.

Both require governance, strategic management and clear policies

Engineering Council Guidance on Security

Key Principles

1. **Adopt a security-minded approach to your professional and personal life**

2. **Apply responsible judgement and take a leadership role**

3. **Comply with legislation and codes, understand their intent and be prepared to seek further improvements**

4. **Ensure good security-minded communications**

5. **Understand, comply with and seek to improve lasting systems for security governance**

6. **Contribute to public and professional awareness of security**

Holistic security thinking to protect the digital and physical built environments

Hugh Boyes CEng FIET

Bodvoc Ltd