Physical Security Lifecycle

Understand

Understand the people, information and assets you need to protect, their value to your organisation, health and safety needs, and the business impact of loss or harm to inform your security requirements.

You should understand how your facility will be used, who will use it and what will be stored there. Identify any classified information or assets stored in there. You also need to consider any other legislative requirements.

When co-locating, work in partnership with the other organisations to build this understanding

Assess

Assess the risks to your people, information and assets to enable you to identify security measures to reduce those risks to an acceptable level.

You need to identify the security threats and vulnerabilities relevant to your people, information and assets. Analysing your existing security measures and the likelihood and impact of each risk will let you evaluate where further action is required.

Consider the combined security risk of all co-locating organisations.

Design

Design fit-for-purpose security measures that are proportionate to the risks identified and in line with your organisation's risk appetite.

Make sure you consider third party suppliers and the role they play. Factor security requirements into your business continuity / disaster recovery requirements.

Consider legislative and policy requirements or guidance (e.g. health & safety, Government Property Group, zone requirements).

Accept security approach/plan
The responsible executive (normally the CSO) accepts that the proposed security design is fit for purpose.

Implement

Implement the agreed security measures including policies, processes, procedures and technical security controls.

Provide security awareness training for all staff and contractors.

Validate

Certification
Confirmation that the agreed security controls have been correctly implemented.

Validate that the risk mitigations and security controls identified in your design have been correctly implemented and are fit-for-purpose.

For security zones this requires a formal accreditation process (and in some cases certification).

Accreditation
The agency head, or their delegate, gives approval to operate and accepts any residual risks. SCIFs must also be accredited by the GCSB.

Go Live

Operate & Maintain

Staying secure requires ongoing activity to keep up to date with evolving security threats and vulnerabilities and to keep your security controls up to date and remain fit for purpose.

Take steps to ensure ongoing security awareness with staff and contractors.

Respond
Identify and respond to security incidents or breaches. See "Incident Management" Infographic.

Review

Undertake regular reviews to ensure your security measures remain fit-for-purpose. Identify changes in your use of facilities, your organisation or the threat environment. Use this information to inform improvements.

Retire

When a building or facility is no longer needed make sure you consider the security implications of any information, assets or chattels during decommissioning.

Specific items may need to be destroyed, redeployed or disposed of in a secure way.