CPNI
Centre for the Protection of National Infrastructure

The Level 1 Operational Requirements Process

Security risk management and developing a strategic security plan

February 2016

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 use of this document and seek independent professional advice on your particular circumstances.

Scope

This guidance document has been written for the Critical National Infrastructure and other customers of CPNI who are exposed to national security threats. It sets out the Level 1 Operational Requirements (OR) process and expected outputs.

This document does not provide detailed advice on risk assessment methods. A number of sources of such advice are available, including ISO 31010 (Risk management – Risk assessment techniques) Annexes A and B.

What is an Operational Requirement?

A Level 1 OR assesses, evolves and justifies the actions to be taken and investments made to protect critical assets against security threats. It provides a structured process for: i) outlining and assessing security risks, ii) identifying risk mitigation options, iii) creating a high level statement of how the security needs of an organisation will be met, i.e. a strategic security plan (SSP), and iv) presenting a convincing business case for investing in this plan. It makes clear who owns the risks and identifies the stakeholders which should be involved in the development and delivery of the proposed plan.

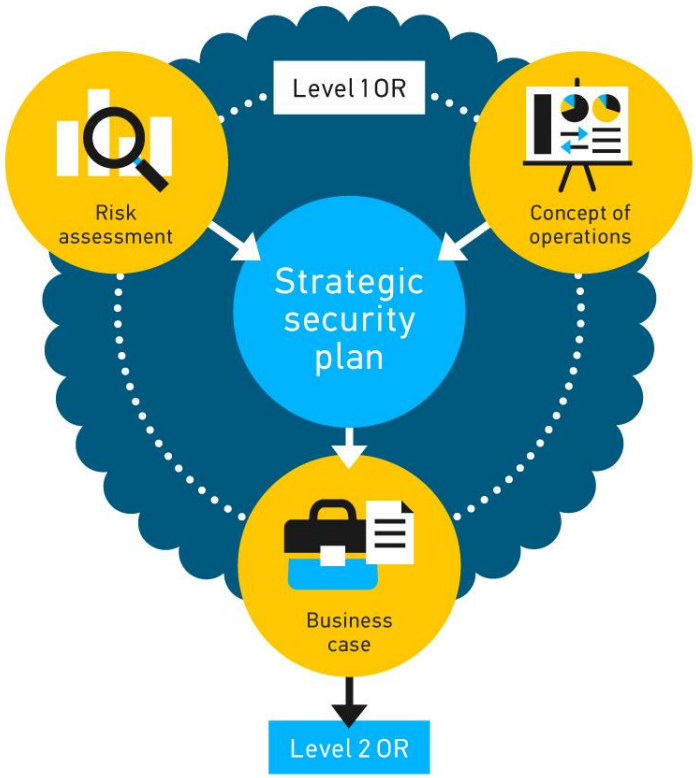

Figure 1: The components of the OR process.

A Level 2 OR is carried out based on the SSP and Level 1 OR outputs. It provides the detail required for individual security measures to be developed by project teams, and should be issued to those responsible for delivering these measures. It also provides the information necessary for the proposed solution to be costed or tendered.

Key points

- The OR process can be used by security managers and practitioners to assess, evolve and justify the actions to be taken and investments to be made to protect critical assets against security threats;
- It uses the risk assessment process as the basis for this;
- The completed document can be presented to senior decision makers and budget holders to gain support for investing in security measures;
- It will lead to smarter investment in security measures, ensuring organisations implement measures which are proportionate to the risks they face;
- The process should be reviewed regularly as the risks an organisation faces are likely to change over time;
- Security risk assessments conducted as part of the process should be formatted in a way which is compatible with the corporate risk assessment, for ease of integration with the overall business.

What is the Level 1 Operational Requirements process?

The Level 1 OR process is designed to counter cyber, personnel and physical security threats in an integrated manner. It operates in the context of stakeholder and regulatory requirements, the corporate risk register and an assessment of organisational readiness. The process is strategic in nature.

There are five main steps involved in the Level 1 OR process. These are summarised in Table 1.

Step	Objective	Key Questions
1	Identify all assets to be protected, highlighting those that are critical	Which stakeholders should be involved in the Level 1 OR process? Which assets are most critical to your organisation and why?
2	Identify threats and vulnerabilities	Who may be trying to harm your organisation? What is their intent, capability and culture? How vulnerable is your organisation and its critical assets to these threats?
3	Assess the risks	What risks does your organisation face? Which risks should your organisation focus on?
4	Identify risk mitigation options and develop an SSP	What options are available for mitigating the risks? What will the residual risks be post implementation? What will the security plan cover and how will the individual elements be integrated?
5	Review organisational readiness to deliver the SSP	How capable and ready is your organisation to implement the proposed security plan?

Table 1: The five step Level 1 OR process.

Step 1: Identify critical assets to be protected

In each organisation some assets will be more critical than others. Your organisation should list the assets it has. These may be tangible (e.g., people, equipment and information) or intangible (e.g., processes, service provision and reputation). You should prioritise the importance of these by looking at the impact that damage to or loss of an asset could have. This prioritisation process is important as it will help your organisation focus where to invest money and resources. Stakeholders play a key role in defining the assets and identifying why they are critical to an organisation. Therefore the first step is to identify and engage with the stakeholders, prioritise their interests, and identify plans for resolving conflicting priorities. A strategy for engaging with stakeholders should be established and communicated to all.

Step 2: Identify threats and vulnerabilities

The Level 1 OR process relies on an understanding of the threats posed to your organisation and how vulnerable your organisation is to these threats. Your organisation should identify the potential threat actors, whether external or internal to your organisation or both. Examples include terrorists, hostile foreign intelligence services, criminals, commercial competitors, disgruntled staff and protestors. Threat actors may be identified by your organisation itself, by the law enforcement agencies and security and intelligence agencies or by other stakeholders. You should seek to answer the following questions with respect to the threat actors identified, in order to ascertain their capability and intent:

- Why might they be trying to target your organisation?
- Which assets might be the targets of their actions?
- How might they try to target your organisation?

When assessing the threat(s) it is important to consider: i) the national threat level; ii) the historical context of similar threats; iii) the emergence of new threats, iv) internal records of previous incidents; v) whether the threat is external or internal, witting or unwitting; and vi) future threats during the life of the asset. The threat assessment should be reviewed regularly.

Example threats:

- An explosive attack by an extremist attempting to cause fatalities and casualties in order to strike fear and gain maximum publicity for their cause.
- A cyber - attack by an organised crime group interested in stealing and changing customer records, by fooling employees into revealing customer details, or by mounting technical attacks on the services offered online to customers.
- A disgruntled employee who deliberately leaks privileged information from their employer to the media and onto the internet, i.e. an insider threat
- An attack by a hostile group seeking to compromise, or disrupt the operation of, a built asset

The next step is for your organisation to determine how vulnerable its assets are to the threat(s) identified, by recording:

- which assets are the targets of the threat(s) and where they are;

- how threat actors might exploit particular vulnerabilities to commit an attack[1];
- what the main shortfalls in current security arrangements are.

Example vulnerabilities related to the explosive threat:

- The building is not physically robust enough to resist the defined threat. There is also a lack of governance, policy and procedures in how the organisation would manage and recover from such an incident.

Example vulnerabilities related to the cyber threat include:

- The organisation does not ensure that its software and systems are adequately patched across the enterprise. This could allow a threat actor to use un-patched vulnerabilities to compromise the systems.

Example vulnerabilities related to the insider threat include:

- The organisation does not ensure that IT access permissions held by staff who have left the organisation have been disabled. This could allow the threat actor the opportunity to access sensitive/protected material.

Example vulnerabilities related to the hostile group threat

- The organisation does not protect information related to the location, properties and operation of sensitive assets and systems, or which could impact on the safety and security of personnel and other users of the built asset.

Step 3: Assess the risks

Combining the perceived likelihood of an attack (determined from threat and vulnerability assessments) with the impact on an organisation's assets, if targeted and attacked successfully, forms the basis of a risk assessment.

There are many valid ways of conducting security risk assessments. The choice depends on the intended purpose and use of the risk assessment, and the complexity of the threats and/or vulnerabilities. Advice on risk assessment methods can be obtained from a number of sources including CPNI's guidance on Personnel Security Risk Assessment[2] and CESG's guidance on Managing

[1] It is important to consider how the threat actor might gather the information needed (hostile reconnaissance) to allow the threat to be realised. For example online information about your organisation held by both you and third parties, detailed and accurate digital information about your building and its operation held by both you and your supply chain, physical locations where hostile reconnaissance could be carried out (outside your boundaries) and the actions of your employees in and around the workplace. Where possible ensure that these vulnerabilities are addressed as part of the mitigations.

[2] CPNI (2013) Guidance – Personnel Security Risk Assessment. www.cpni.gov.uk/advice/Personnel-security1/risk-assessment/

Information Risk[3]. The results of a risk assessment should be presented in a way which is appropriate to your organisation and, importantly, in line with the corporate risk assessment where possible.

Example impacts related to the explosive threat include:

- Loss of life and injury
- Damage to the building and disruption to business operations
- Reputational damage

Example impacts related to the cyber and insider threat include:

- Compromise of confidentiality of customer data
- Financial penalties imposed by the Information Commissioner's Office (ICO)
- Reputational damage and loss of business

Example impacts related to the hostile group threat

- Compromise of built asset information and data
- Compromise of the built asset itself and disruption to its operation
- Reputational damage and financial costs associated with recovery

Risk assessments are best undertaken with involvement from key stakeholders to help build a shared understanding of the issues, their relative importance and how to manage them. In the case of terrorism and state sponsored espionage, your organisation may need to take advice from a CPNI adviser, Counter Terrorism Security Adviser (CTSA), or a member of the relevant Computer Emergency Response Team (CERT) on the likelihood of an attack occurring, and work with them to assess the consequences.

Step 4: Identify risk mitigation options and develop a strategic security plan

When your organisation has reached a point where it understands the risks it faces the next step is to use the results to ascertain and analyse the options available. Initially the risks should be prioritised and a risk treatment approach specified, i.e. will your organisation avoid, accept, transfer or mitigate the risks. Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits expected. The owner(s) of the risk(s) should also be identified.

Risk mitigation involves deciding what options should be considered to reduce the likelihood or consequences to an acceptable level. It is a composite of many interwoven and layered elements, all of which contribute to protecting the assets and assist in identifying where to prioritise efforts. It involves deterring, detecting, delaying or responding to threat actor(s) during attack planning or execution. There are three ways of doing this, which can be used in combination if desired:

- Remove the threat(s) – this is the most desirable outcome but is often not possible and depends greatly on the source and nature of the threat(s) and the resources available to the organisation;

[3] CESG (2015) Guidance – Managing Information Risk. www.gov.uk/managing-information-risk#choose-the-right-risk-assessment-method

- Reduce the vulnerabilities – this may be achieved through the use of operational/procedural measures, physical/technical measures, or a combination of both;
- Reduce the impact – the outcome is likely to include a response and recovery plan and/or an increase in the redundancy in your organisation or asset. Organisations should seek to increase resilience to an attack and implement a response plan and business continuity strategy. This will assist them in managing an incident both during an attack and in the recovery phase afterwards.

Example approaches to reducing vulnerabilities to the explosive threat include:

- Deterring adversaries from entering the site and/or building
- Detecting adversaries entering the site and/or the building
- Delaying adversaries from reaching the critical assets
- 'Hardening' the assets such that the impact of an attack is less severe

Example approaches to reducing vulnerabilities to the cyber threat include:

- Deterring adversaries from gaining access to the corporate IT system
- Detecting adversaries gaining access to the corporate IT system
- Delaying adversaries from gaining access to the corporate IT system

Example approaches to reducing vulnerabilities to the insider threat include:

- Deterring adversaries from gaining access to working for the organisation
- Detecting disgruntled employees working for the organisation

Example approaches to reducing vulnerabilities to the hostile group threat include:

- Protect information about the properties and, where not generally directly visible directly or through other sources, the location of sensitive assets and systems
- Address where the aggregation or association of data could compromise the security or operation of a built asset

Physical, personnel and cyber security measures should be considered in a holistic approach when identifying risk mitigation options. Once the risk mitigation strategies have been identified their suitability should be assessed. This can be done by using scenario analysis to explore the feasibility, impact on identified security risks and operations, and business impact. A rough cost-benefit analysis of the options can then be produced, and an SSP and an operating concept developed and signed off.

The SSP should include information on:

- the components involved (including protective security measures, response planning, personnel procedures and training, and information security measures) and how they will be integrated together to ensure a cohesive plan;
- how they will deliver the improvements needed;
- the criteria which will be used to monitor and evaluate its success.

The SSP should ensure that a scalable defence-in-depth/layered approach to security is adopted. It should identify the timescales associated with the introduction of the plan, any critical interdependencies and areas where integration is necessary. Your organisation should identify the procurement approach it is going to adopt at the outset. Consideration needs to be given to whether the development and implementation of the SSP will be outsourced or undertaken in-house. This information is essential for informing key decisions your organisation needs to make in order to effectively implement the plan.

Example strategic security plan components related to the explosive threat include:

- Protective security measures: a deterrent communications strategy, layered physical security measures, personnel security screening, visitor screening, manned-guarding
- Response planning: briefings with staff and emergency services, action plan for the event of an attack (e.g. site lock-down, interdiction), evacuation/containment strategies, business continuity strategy
- Personnel procedures and training: staff training and awareness , maintaining an appropriate security culture

Example strategic security plan components related to the cyber threat include:

- Protective security measures: a suite of management, technical and operational controls[4,5], clearly defined and communicated information security policies
- Response planning: exercising, briefings with staff, action plan for the event of an attack (e.g. review firewall and monitoring systems), incident management strategy
- Personnel procedures and training: information security staff training and awareness, maintaining an appropriate security culture, role-based access control

Example strategic security plan components related to the insider threat include:

- Protective security measures: a suite of human resources processes and procedures clearly defined, owned and communicated personnel security policies
- Response planning: action plan for investigation of insider acts, briefings with staff, incident management and business continuity
- Personnel procedures and training: monitoring, staff training and awareness

Example strategic security plan components related to the hostile group threat include:

- Protective security measures: a suite of policies, processes and procedures covering the people, physical and technological aspects of the built asset, asset information and building-related systems
- Response planning: implementation of arrangements for, and overseeing of, capture, handling, dissemination, storage, access and use of sensitive information and data
- Personnel procedures and training: staff training and awareness, identification of high-risk positions, screening and vetting requirements, role-based access control

[4] CPNI (2015) Guidance – Critical Security Controls. www.cpni.gov.uk/advice/cyber/Critical-controls/
[5] CESG/CPNI/BIS/Cabinet Office (2015) Guidance – 10 Steps to Cyber Security. www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary#steps-to-cyber-security-at-a-glance

Organisational opportunities and constraints

Implementation of the strategic security plan might be constrained and determined by the:

- business needs;
- resources available to implement and maintain the plan;
- procedures currently in place which the plan must conform to;
- organisational structure, roles and responsibilities which support implementation of the plan;
- national and international standards which the plan must comply with;
- management systems which the plan must align with, e.g. health & safety, environmental;
- statutory, regulatory, contractual and supply chain collaboration requirements;
- availability of suitable expertise and trusted partners for implementing the plan;
- operating environment, local communities and stakeholders.

Concept of operations

CPNI recommends that a concept of operations (ConOps) be developed to support the SSP. The ConOps describes at a high level how your organisation will deliver the SSP. In relation to the construction of new built asset or the management of those already existing, where asset information and data is held electronically, it should be cross-referenced to the Built Asset Security Management Plan required by PAS 1192-5:2015[6]. The ConOps should include:

- an overview of the SSP;
- the environment within which the SSP will be implemented;
- the delivery concept associated with the SSP;
- command, communication and co-ordinating concepts.

[6] BSI (2016) Standard - PAS 1192-5:2015 Specification for security-minded building information modelling, digital built environments and smart asset management. http://shop.bsigroup.com/forms/PASs/PAS-1192-5/

Step 5: Review organisational readiness

An organisational readiness review should be carried out on the SSP that has been developed. It determines the preparedness of your organisation for change and serves two important purposes in the Level 1 OR process, namely:

- to reality-check at a high level the feasibility of the chosen risk mitigation option;
- to check that the operational capabilities are in place to ensure the plan can be implemented and remains effective over time.

Both of these save time and money and safeguard against failure of the SSP. Table 2 provides a checklist that can be used for this purpose, and can be tailored to your organisation's requirements.

People – there are sufficient competent and motivated personnel to implement the security plan
All key stakeholders understand their roles and responsibilities
The proposed plan is consistent with stakeholder expectations
Key operational/technical/risk assumptions have been validated with stakeholders
Process – the procedures and processes in your organisation are fit for purpose
The implementation can be completed within the agreed budget
All external dependencies are known and can be coordinated
The SSP can deliver what was promised in the business case
Delivery and implementation risks are understood and mitigation responses in place
Timescales are consistent with stakeholder expectation
Infrastructure – the necessary equipment, machinery, hardware and systems are in place
The necessary equipment, hardware and supporting infrastructure have been identified/inspected
Trusted suppliers are in place with suitable knowledge, resources and delivery capabilities[7]
Sufficient contractual measures are in place to ensure security requirements are met by the whole supply chain

Table 2: Organisational readiness review checklist.

[7] CPNI (2015) Guidance – Security in the Supply Chain. www.cpni.gov.uk/advice/Personnel-security1/Security-in-the-Supply-Chain/

Level 1 Operational Requirements document

The Level 1 OR document brings together the outputs of the process outlined, and provides a structured means for your organisation to record its findings. It is recognised that your organisation may need to adapt the process to suit individual circumstances. The list below provides an outline of the components that should be included in the OR document:

- Executive overview;
- Site or building to be protected;
- Stakeholders;
- Critical asset(s);
- Threat(s) and vulnerabilities;
- Impact;
- Proposed strategic security plan;
- Organisational constraints;
- ConOps;
- Implementation and integration;
- Critical dependencies;
- Costs and benefits;
- Organisational readiness.

N.B. The completed OR document is likely to be security-sensitive and should be safeguarded accordingly.

The Level 1 OR should form the basis of the business case for investing in a SSP. It should be presented to senior decisions makers and budget holders to gain support for investing in security measures. The investment will be dependent on the level of risk appetite the senior decision makers have. Once the investment has been agreed the plan should be used to inform the requirements for the security measures, through the Level 2 OR process.

Glossary of terms

Asset information	Data or information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organisation. It can include design information and models, documents, images, software, spatial information and task or activity-related information.
Built asset	Building, multiple buildings (e.g. a site or campus) or built infrastructure (e.g. roads, railways, pipelines, dams, docks etc.) that is the subject of a construction project or where asset information is held in a digital format.
Concept of Operations	Describes at a high level how an organisation will deliver the strategic security plan and how security operations will be conducted.
Critical asset	Something of value to an organisation, requiring protection. Assets are varied and include people, property, buildings, information, processes and reputation.
Impact	The consequences of a risk being realised.
Likelihood	The chance of something happening, as a function of threat and vulnerability.
Operational Requirement	Level 1: A structured process for outlining and assessing security risks, identifying risk treatment options, and presenting a convincing business case for investing in a strategic security plan. Level 2: Provides the detail required for individual security measures to be developed by project teams.
Organisational readiness	The preparedness of an organisation for change.
Residual risk	The risk which remains after risk mitigation has taken place.
Risk	The anticipated impact to a defined set of assets, resulting from a defined set of threats and vulnerabilities.
Risk assessment	Assessing the risks to an organisation and its assets in terms of the likelihood of a threat event taking place, and the impact that such an event might have.
Risk management	The decisions an organisation makes and the actions it takes in response to risks that have been identified.
Risk mitigation	Measures taken to reduce a risk.
Risk register	A management tool that enables an organisation to understand its overall risk profile. A risk register is a dynamic document that is populated by the organisation's risk assessment processes, enables risk to be quantified and ranked, and enables decisions on how to manage risks.
Risk treatment	Avoidance, acceptance, transfer or mitigation of the risk.
Sensitive information	Information, the loss, misuse or modification of which, or unauthorised access to, could: adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organisation; cause commercial or economic harm to an organisation or country; and/or

	jeopardise the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information.
Stakeholder	A person or group that has an interest in the project.
Strategic security plan	A high level statement of how the security needs of an organisation will be met.
Threat actor	Individuals, groups or states which pose a (national security) threat.
Threat assessment	An assessment of the threat based on the intent and capability of a threat actor.
Vulnerability	A weakness which can be exploited by a threat to create an impact.