CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

MANAGE THE BUSINESS RISK

A GOOD PRACTICE GUIDE

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 favouring by CPNI, CESG or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. The content of this document is based on information available as at the date of publication.

The case study although fictitious is based on the experiences of PA Consulting Group through their work with companies in ICS industries. Any similarities are strictly coincidental and are not based on any one specific company.

This is general guidance only and is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate specialist advice.

To the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers accept no responsibility for any errors or omissions contained within this document. In particular, to the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers shall not be liable for any loss or damage whatsoever, arising from any error or omission in this document, or from any person or organisation acting or refraining from acting upon or otherwise using the information contained in this document.

Copyright

Corporate Headquarters:

PA Consulting Group
123 Buckingham Palace Road
London SW1W 9SR
United Kingdom
Tel: +44 20 7730 9000
Fax: +44 20 7333 5050
www.paconsulting.com

Version no: Final v1.1

Prepared by: PA Consulting Group Document reference:

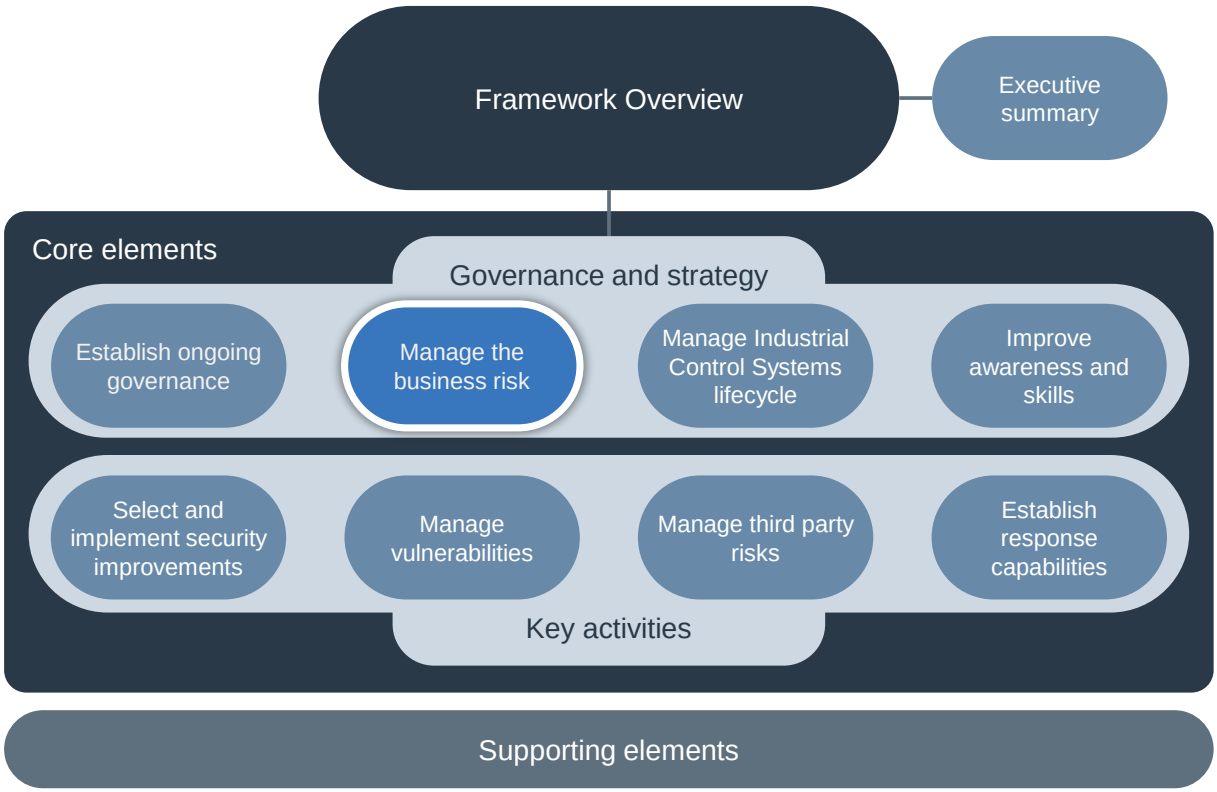
CONTENTS

1 INTRODUCTION

1.1 Framework context

The Security for Industrial Control Systems (SICS) Framework provides organisations with good practice guidance for securing Industrial Control Systems (ICS). This framework consists of a good practice guide Framework Overview, which describes eight core elements at a high level. This is supported by eight good practice guides, one for each core element and which provide more detailed guidance on implementation. Additional supporting elements of the framework provide guidance on specific topics. The framework, core elements and supporting elements are shown in Figure 1.

Figure 1 - Where this element fits in the SICS Framework



1.2 Manage the business risk - summary

The objective of this guide is:

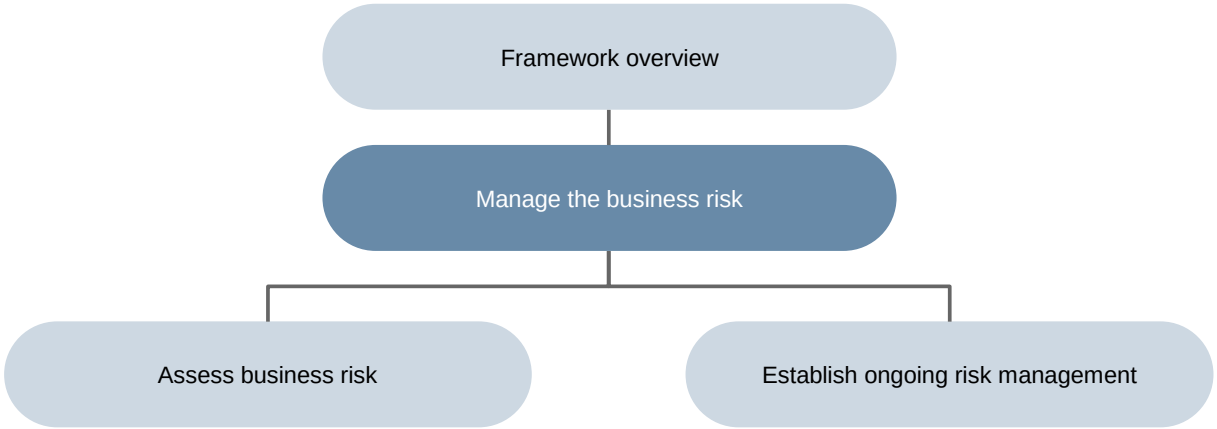
- To gain a thorough understanding of the risk that the organisation is facing in order to identify and drive the appropriate level of security protection required.

This guide addresses the management of business risk arising from the cyber security threat to ICS using descriptive (qualitative) methods rather than measurable (quantitative) methods. It is intended to be used to support investment decisions relating to the security budget and provide up to date information to support the business risk management process.

A preliminary step to improving the security of ICS is to gain a thorough understanding of the business risk in the context of ICS security. Business risk is a function of threats, vulnerabilities and impacts. Only with a good knowledge of the business risk can an organisation make informed decisions on what the appropriate levels of security protection should be. This document provides details of two good practice principles as set out in Figure 2:

- **Assess business risk** – any security improvements should be based on the level of risk facing a particular system to ensure that an appropriate level of protection is provided. For example a low risk system is likely to require less protection than a high risk system. However these controls need to be correctly deployed in order to achieve the full security benefit. An understanding of the business risk is a key driver to where such protection measures are deployed.
- **Establish ongoing risk management** – managing the business risk arising from ICS is not a one off exercise – it is an ongoing process which is part of a wider risk management approach. Once the risk appetite of the organisation has been defined, a risk assessment has been carried out and the relevant security improvement measures have been implemented, it is important to maintain ongoing management of the business risk as threats change and more vulnerabilities are identified.

Figure 2 – Good practice principles to manage the business risk



2 ASSESS BUSINESS RISK

Organisations need to understand the ICS security risk that their businesses are facing in order to determine what an appropriate risk level (risk appetite) is. They can then establish what security improvements are required in order to reduce the level of risk exposure to align with the risk appetite.

There are many different methodologies (e.g. CESG: Risk management of cyber security in technology projects[1], ISO 31000[2] and NIST: 800-30 Guide for conducting risk assessments[3]) that can be used to assess risk. While each has their advantages, no one methodology is right for all situations therefore it is vital to choose one that is appropriate and can be used consistently throughout the business. The following sections outline an approach that can be used if existing business risk management processes are not in place or effective. Organisations should also consider adapting information management processes for the ICS environment.

The relevant good practice in the overarching document "Security for Industrial Control Systems – Framework Overview' is:

- Understand the systems
- Understand the threats
- Understand the impacts
- Understand the vulnerabilities.

2.1 Business risk assessment

There are many ways in which business risk can be defined. Risk assessment can also be a very subjective exercise if there is no structured way of estimating the risks. This is a particularly important consideration where the estimated risk is used to inform major investment decisions on security, or support risk assessments in other parts of the business, for example safety risk assessments. One useful definition is to express the risk as a function (F) of the likelihood of a risk occurring and the impact that would result if that risk were to occur.

Business risk = F (Likelihood, Impact)[4] (1)

[1] https://www.gov.uk/government/publications/risk-management-of-cyber-security-in-technology-projects/risk-management-of-cyber-security-in-technology-projects

[2] http://www.iso.org/iso/home/standards/iso31000.htm

[3] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[4] Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. AIChE - 2003.

The likelihood of a risk occurring can be expressed in terms of Threat, Target Attractiveness, and Vulnerability.

Likelihood = F (Threat, Attractiveness, Vulnerability) (2)

The 'Threat' characterises the intensity level of the threat applying to the organisation. It is defined as a combination of two components, the threat source – the agent with the capability to carry out the threat, and the threat event –the means by which the threat is delivered.

The 'Attractiveness' relates to how attractive a target might be to a potential attacker, this often relates to the motives of the attacker (e.g. criminal gain, terrorism) and may not apply to some risks. As 'Attractiveness' contributes to the likelihood of a risk occurring (i.e. a more attractive target is more likely to be attacked) for simplicity it can often be incorporated within the 'Threat'.

'Vulnerability' characterises the level of the weaknesses that the threat can exploit in order to create an impact on the assets. A low level vulnerability means no weaknesses or only those that require rather complex techniques to exploit them. A high vulnerability would correspond to attacks that could be mounted easily due to the lack of protection.

Combining (1) and (2) gives an expression for business risk in terms of threat, attractiveness, impacts and vulnerabilities.

Business risk = F (Threat, Attractiveness, Vulnerability, Impact) (3)

It should be noted that the presentation of these elements of business risk in (3) above does not represent a strict mathematical equation but rather an illustration of the relationship between the elements to support a computation of risk.

The following sections describe the elements required to understand the business risk.

2.2 Understand systems

In order to understand the ICS security risk facing a business, a thorough understanding of the systems that support that business is needed. The first step in this process is to agree the scope that this risk analysis will cover. The scope boundaries need to be clearly drawn and any systems that are identified as out of scope should have clear agreements about who owns them, how their risks will be handled and how appropriate assurance of the level of security protection for these systems should be sought.

2.2.1 Constructing an inventory

In many cases ICS may have been installed many years ago and detailed knowledge of their operation and configuration may not be readily available. In order to understand the business risk this information needs to be determined (where it is not immediately available) and collated into a full system inventory. Compiling such an exhaustive and detailed inventory might not be achievable in all circumstances. If it cannot be created at once, starting with a partial inventory (e.g. concentrating on critical systems first or at a higher level of granularity) is an option. It will then be possible to refine it further at a later stage as maturity progresses. Maintenance spares inventories often provide a good starting point for the construction of system inventories. These initial inventories can be improved by site inspections and dialogue with the maintainer.

There are a number of key elements that need to be considered when gathering a system inventory:

- What is the system (what is its scope, a single system or a system of systems)?
- What is its purpose (what does it do, how damaging would its loss or malfunction be to the business)?
- Who is the owner (operations, maintainer)?
- What is the supporting documentation (system and network diagrams)?
- What is the supporting technology (Windows, IP networks, PLC)?
- What are the current version and patch levels?

- What is its business and operational criticality (safety, environmental, reputational, and financial)?
- Who are the vendors (hardware, application software, third party software)?
- Who are the integrators, support organisations and other third parties?

These key elements can be further developed to include additional supporting information and detail as required, for example:

- How many locations, sites, systems and assets exist?
- What systems reside at the site?
- Is the site manned or unmanned?
- Where does the site and system fit in the overall 'value' or 'supply' chain?
- What contributions do the systems make to process or personnel safety?
- What are the operational business continuity objectives and the associated resilience requirements for the systems?
- Are there any Safety, Health and Environmental or other regulatory implications?
- Do the assets form part of the Critical National Infrastructure (CNI)? For further information on what might constitute the CNI please consult the CPNI website[5].
- Who is the single point of accountability (SPA) for each site, system and asset?
- Who are the key support organisations at the site (IT, ICS, off-site third party, on-site third party or in-house) and what is the support level?
- What are the site's critical system assets?
- What connections and data feeds are there to and from the control systems (include manual data feeds as well as electronic connections)?
- Are there any known issues with the systems?
- What projects are underway or scheduled?
- What are the dependencies relating to the site?
- Are there summary and detailed system and network diagrams?
- What are the hardware, software and their versions?
- Is all documentation secure and under a management of change procedure?

The answers to these questions enable the organisation to create an ICS inventory. The inventory is a fundamental building block for the ICS security framework and is the input to many other themes and sections. This inventory should be sufficiently detailed to provide the appropriate determination of risk. To ensure consistency of information and up to date data, this should be compiled in conjunction with other existing inventories in the organisation, for example as part of Enterprise Asset Management (EAM).

Inventories are notoriously difficult to generate and to keep up to date. An ideal situation might be to maintain a single inventory that can provide summary level of information as well as the detail. However, if this is being done for a large organisation then it may not be practical to construct a single detailed inventory. A hierarchical inventory might be more appropriate where a central high level inventory is maintained together with a link to local site inventories, which contain the detail.

It should be noted that these inventories, along with all ICS risk documentation, are potentially a source of sensitive information, which would be very useful for an attacker. Consequently material contained within inventories, such as risk and security assessments and mitigating controls, should be appropriately secured and subject to protective marking. Access to these inventories should be restricted to the minimum number of people who need access to this information.

[5] http://www.cpni.gov.uk/about/cni/

2.2.2 Dependencies

It is important to understand any dependencies between systems (both for systems in scope and out of scope). Some parts of an ICS might be dependent on the outputs of another system in the supply chain. For example an oil refinery might be dependent on a pipeline for its feedstock. Consequently, when determining the business risk for a refinery, the 'upstream' dependencies such as the supply pipeline should be adequately considered in the risk assessment. Similarly 'downstream' dependencies should also be considered. So a chemicals plant that uses a by-product of the refinery is a 'downstream' dependency and should also be subject to some level of scrutiny in the risk assessment. Where these dependencies involve third party infrastructure and assets it must be recognised that the degree to which the business may be able to mitigate any consequent risks could be quite limited.

2.3 Understand threats

ICS security threats are numerous, can originate from a variety of sources and can be comprised of many different types of event. It is important to address the common threats but consideration should also be given to the specific context applying to a company or a type of organisation. For example an oil company that is active in particularly sensitive regions of the world may have a different threat profile from a transport company operating solely in the UK.

The threat sources are often very different and have varied capabilities to deliver an attack. It is important to consider this in assessing the business risk as it influences the likelihood of an attack. Organisations need to ask what action the attacker could realistically undertake, how much time and money will they invest, will they use zero days or public exploits, how motivated are they, do they have opportunity? Threat sources that should be considered include (but should not be limited to):

- Hackers
- Internal attackers
- Criminals
- Illegal information brokers
- Disgruntled employees[6]
- Staff undertaking unauthorised actions (e.g. accessing the Internet)
- Corporate intelligence
- Contractors
- Foreign intelligence services
- Organised crime
- Terrorists
- Protesters and activists (e.g. environmental, political, animal rights).

The UK government provides more information on managing risk in the publication "Risk management of cyber security in technology projects".

Threat events that should be considered include (but should not be limited to):

- Introduction of malware (generic, targeted)
- Misuse of network connections
- Escalation of privileges
- Denial of service attack

[6] Employees include all those given legitimate access to an organisation's assets and/or premises, including staff, agency and contract staff. Such access may be exploited to gain access to assets not required as part of their legitimate business activities.

- Other targeted attacks exploiting vulnerabilities on the systems with the aim to affect availability, integrity or confidentiality.

These threat events are generic so it is often more useful to use particular scenarios to assess risk. However, it is important to ensure that these are broad enough to encompass all the specific threats and vulnerabilities an organisation may face.

Examples of consequences-based scenarios include, but are not limited to:

- Systemic loss of all machines based on a particular operating system (e.g. Windows, Unix, VMS etc.)
- Systemic loss of Ethernet/IP networking technologies
- Introduction of malware resulting in loss (or reduction) of functionality of ICS
- Misuse of network connections to cause loss of connectivity between the ICS and
  - Corporate networks
  - Other systems (e.g. supply chain, laboratory systems or other companies)
  - Remote field devices
- Unauthorised change of set-points or configuration by malicious or inadvertent internal or external actions
- Accidental change of system configuration by an authorised user
- Loss of integrity or availability of historical data
- Loss of confidentiality of process and related information.

2.4 Understand impacts

Once threats have been converted into risk scenarios then it is much easier to consider the impact that these might cause. That means assessing each scenario for each site, system or sub system and what the real life impacts might be, not only on that system, but also for any system that is dependent upon it. For example if an organisation is assessing an ICS controlling a power station for a chemicals plant, it needs to consider what impact the loss of that system would have on the operation of the chemicals plant, including the effects on safety. When determining these impacts, there is a need to refer back to the inventory and the dependencies already identified.

Classification of impact: in risk assessment, one way of quantifying possible impacts or consequences of a threat is in terms of monetary value. This is particularly the case when considering financial processes. However when considering ICS security risks it can be difficult to determine accurate financial impacts for security incidents. Quantifying the financial consequences is a specialist field and might not be needed to assess ICS security risk and the resulting appropriate security measures.

An alternative is to outline impacts in terms of the specific effect on the business rather than through a monetary figure. For instance, it could be shown that the impact of a malware infection on an ICS might be a decision to shut down the plant operations, and framing it in this way could be easier to understand than a complex calculation of the financial impact.

Examples of possible impact descriptions are:

Safety, Health and Environmental event or damage to plant: an event that results in either harm to individuals or the environment or damage to the plant.

Non-compliance with regulatory requirements or minor Safety, Health and Environmental event: an event that results in the site being non-compliant with regulatory requirements. For example, a consistent breach (e.g. excessive flaring in a chemicals plant or refinery) or loss of regulatory historical data.

Forced controlled shutdown of operations: an event that results in the emergency shutdown system being automatically invoked with no human intervention. For example, when sensor data is lost for all or some of the production processes.

Product corruption: where a manufactured product is produced out of specification because of loss of system integrity, for example spoilt food production.

Elected controlled shutdown of operations: an event that results in the site electing to shutdown its operations. For example, when view is lost of all or some of the production processes.

Reduction in operating efficiency: an event that results in the plant continuing its operations in a less efficient or profitable manner or result in reduced production. For example, the raw material mix is changed resulting in the product being produced in a less efficient manner.

No Impact: no impact on operations.

Other impacts that should be considered are:

- loss of confidential information
- damage to Critical National Infrastructure
- loss of continuity of operations
- damage to reputation
- the effect on value or supply chain.

A way of understanding vulnerabilities in these areas is to do a gap analysis against the ICS security controls developed in SICS Framework element 'Select and implement security controls'.

Time variance of impact: when assessing the impact of a particular event, it is important to consider how it might vary with time. Incidents may initially have a minor impact that increases in severity if allowed to continue over a long period of time. An example of this is the loss of environmental monitoring information which may not be serious in the short term but is likely to be much more critical in the long term owing to legal and regulatory requirements around the availability and integrity of this information.

Successive impacts: the effect of coincident or successive impacts should be considered, this is especially important where a common cause failure could be responsible.

2.5 Understand vulnerabilities

Understanding what vulnerabilities exist requires a detailed review of all the system elements, (e.g. servers, workstations, network infrastructure etc.). Examples of common vulnerabilities include, but are not limited to:

- Uncontrolled connections to other systems
- Unsecured remote access
- Lack of physical security protection
- No anti-malware solution or out of date signatures
- Lack of access control
- Weak passwords or poor account management
- Lack of security patching
- Lack of system monitoring
- Single points of failure affecting system resilience and continuity
- Use of software which is insecure by design (has not followed a secure design process)
- Critical data can be modified to produce unintended function (data integrity)
- Digital footprint i.e. the amount of open source information available on the business, its operations, systems and software that can be used for reconnaissance purposes.

When considering the security of the overall system it is important to remember that it is only protected as well as its weakest link. For example, there is little benefit from having a well-managed, tightly configured firewall if there is a poorly protected modem connection to the outside world or an unsecured wireless network bypassing the firewall.

A pragmatic approach to vulnerability assessment is to assess the system(s) against a set of controls, see the SCIS framework element ‘Select and implement security controls’, for further details.

2.6 Outputs of assessing the business risk

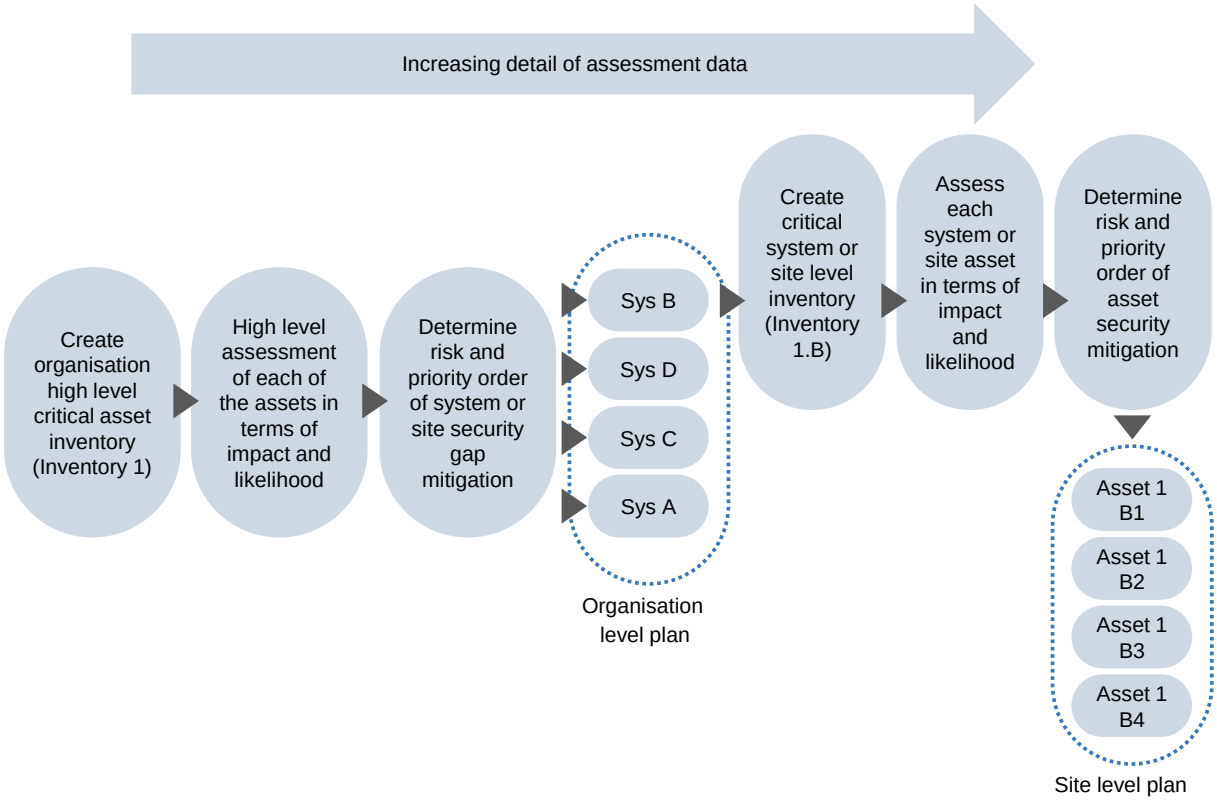
The key outputs from the risk assessment process are:

- a risk register and summary of business risk
- an inventory of ICS
- prioritised sites and systems
- a list of key threats based on impact assessment
- prioritised vulnerabilities.

2.7 Applying this risk assessment approach

Most of this guidance is directed at the site or system level. In a large organisation with many sites and geographies to consider it may not be practical to work at this level. Consequently it may be necessary to break the problem down into more manageable tasks. This can be done by performing a high level, lightweight risk assessment across the whole organisation or enterprise and then performing a more detailed assessment for each of the systems or sites, as shown in Figure 3.

Figure 3 - High level enterprise ICS security risk assessment



2.7.1 Step 1 - defining the risk assessment approach and supporting scales

In order to avoid any distortion linked to the implementation of multiple risk assessments in the same organisation and to reduce the subjective influence of the assessor, a consistent approach for assessing risks should be agreed. This approach should define:

- the methodology for assessing business risks
- the scales that are used to measure the risks and their constituents (threat, attractiveness, vulnerability, impact)
- any supporting tools used to perform the assessment and to report the results.

In order to represent the risks accurately, the scales for assessing threat, attractiveness, vulnerability and impact should be defined to reflect the context of the organisation and be used consistently. For organisations using an Enterprise Risk Management framework, the scales used to evaluate those risks can be transposed to the ICS security risk assessment.

Where safety and environmental impacts are considered as part of the risk assessment, these aspects can be used to inform the current safety justifications for existing ICS. This approach can be extended to support the safety justifications for ICS in development.

When assessing impacts, the different levels of impact should be defined against the range of relevant different business objectives. For example, a typical impact assessment scale could have the following dimensions:

Table 1 - Impact assessment scale

	Low Impact	Medium Impact	High Impact
Financial losses			
Operational efficiency			
Loss of confidential information			
Reputational damage			
Safety and environmental implications			

2.7.2 Step 2 - High level prioritisation of the enterprise

The first iteration of the risk assessment should provide a high level enterprise view of the prioritised ICS security risk. The critical ICS which form the candidates for this assessment are usually well known to the operations and maintenance staff so an initial inventory of candidate systems and sites for assessment can be easily compiled. The high level risk assessment will provide an indication of the security gaps with the greatest impact to the enterprise by considering the ‘value chain’, interdependencies and impacts that have enterprise level significance. The analysis will provide the enterprise with both the priority security issues and confirm the systems or sites that should be addressed first.

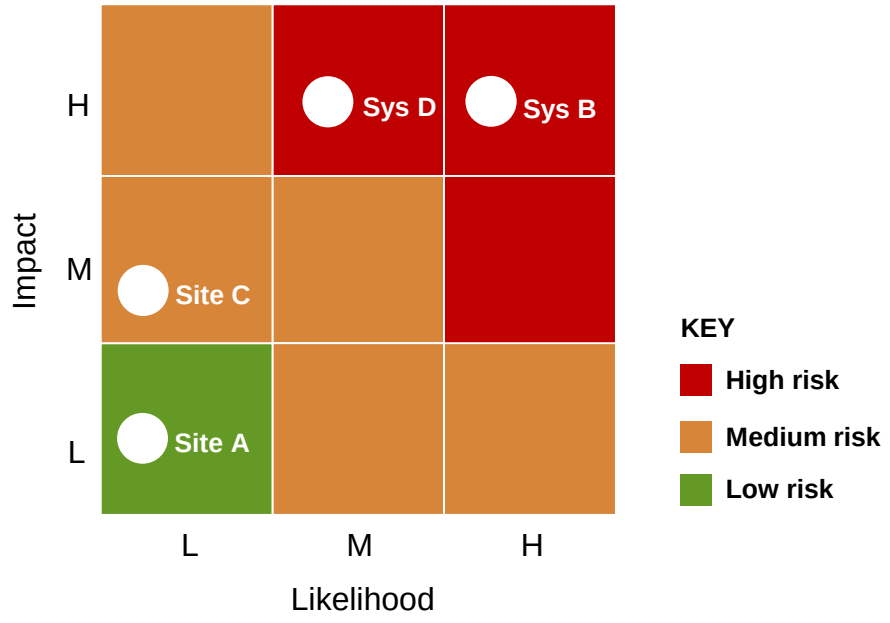
An easy way of determining the priority order is to plot the asset scores on a risk matrix. The risk parameters highlighted above can be plotted in a Risk Table (Table 2). In some cases each of the factors (Threat, Attractiveness and Vulnerability) will be given an equal weighting, at other times they may be weighted to reflect the particular situation. Care should be taken when aggregating different systems and sites to ensure that they are using the same risk assessment methodology, otherwise the risk profile may become distorted.

Table 2 – Risk Table

Site	Threat (T)	Attractiveness (A)	Vulnerability (V)	Likelihood (T x A x V)	Impact (I)
Site A	M	L	L	**L**	**L**
Sys B	H	H	H	**H**	**H**
Site C	L	L	L	**L**	**M**
Sys D	M	M	L	**M**	**H**

In this example the risk table of systems and sites are then plotted on a risk matrix (Figure 4) using the likelihood and impact values.

Figure 4 – High level enterprise risk matrix



2.7.3 Step 3 - Individual systems/site risk assessment

The system/site risk assessment is based on the high level enterprise risk assessment and builds on the key risk areas identified and analyses them at the next level of detail.

After selecting the initial system or site priority for the organisation, a similar process can be used at a site level to help each one determine their priorities. Each site creates a more detailed inventory and then assesses the individual assets in terms of threats, vulnerabilities and impacts. In this way a site can prioritise which assets or services should be tackled first.

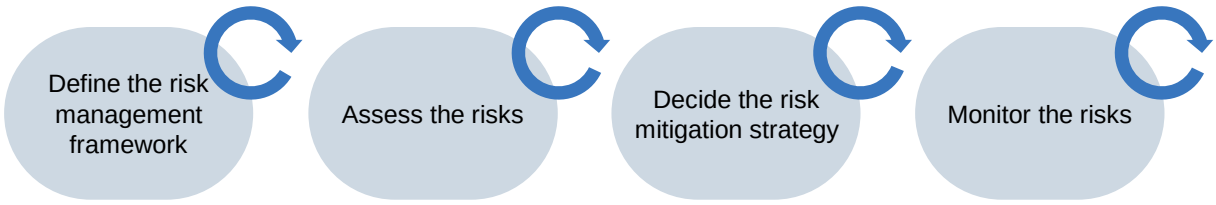
Once an enterprise risk assessment has been carried out a similar process of understanding the systems, threats, vulnerabilities and impacts should be followed at a site, system and asset level to understand their particular business risks.

3 ESTABLISH ONGOING RISK MANAGEMENT

This section sets out how to build an ongoing ICS security risk management approach that is integrated into the organisation's enterprise risk management framework. The process should be linked to governance to ensure that risk ownership is defined, risk processes followed and that systems are conforming with current standards, including ensuring that unauthorised systems changes have not been introduced. This ongoing risk management should then be applied to all other themes in the framework and should be aligned with the agreed business risk appetite.

Assessing the risks associated with the security of ICS is part of a wider risk management set of disciplines and ICS security risks are only one type of risk that an organisation has to manage.

Figure 5 - Risk management lifecycle



The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- Business risk is a function of threats, vulnerabilities and impacts. Any changes to parameters (e.g. installing a new system) could change the business risk. Consequently, an ongoing risk management process is required to identify any of these changes, re- evaluate the business risk and initiate appropriate security improvements.

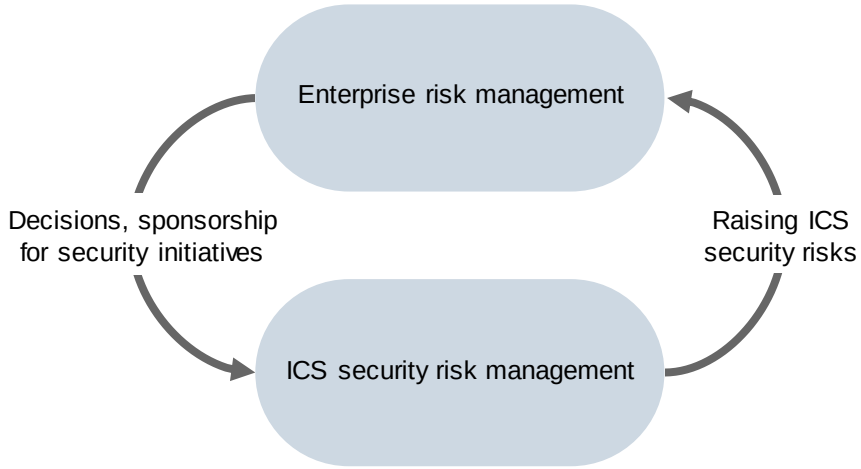
3.1 Defining the framework for risk management

Before initiating risk management activities, an organisation should define the corresponding governing framework. This framework should reflect the organisation's strategy and governance, and describe:

- the importance and objectives of risk management
- the overall process for risk management
- the approach to risk assessment
- the organisation for risk management (e.g. risk ownership, risk management decision making)
- the positioning of ICS security risk management within the wider enterprise risk management (ERM) framework.

In integrating with an ERM framework, the organisation should ensure that relevant ICS security risks are visible to senior management and can be reported on the company risk register. This requires ICS security risks to be aggregated at the organisation level. This is key to ensuring that the organisation risk register is accurate but also to ensuring that senior management can see those risks and support the implementation of the relevant security measures. This relationship between ICS security risk management and enterprise risk management is illustrated in Figure 6 ISO 31000 - Risk management[7] provides more information about ERM.

Figure 6 – ICS security Management and enterprise risk management



Other governance aspects related to ICS risk management are described in SICS Framework element 'Establish ongoing governance'.

3.2 Assessing the risks

Assessment of the risk which is detailed in section 2 is integral to managing the risk, and more specifically to implementing and communicating the results of the risk assessment to the wider business.

3.3 Deciding the risk mitigation strategy

Based on the assessment of the risks, the organisation should identify, prioritise and decide how they want to deal with them. This involves understanding the organisation's risk appetite which will reflect its own strategic objectives and external influences such as the legal and regulatory environment. The objective is then to drive the risks towards this level of acceptable risk through the implementation of

[7] http://www.iso.org/iso/home/standards/iso31000.htm

security controls. More information on defining the risk appetite can be found in the HM Treasury Orange Book on Management of risks – Principles and concepts[8].

Note: some organisations choose to use impact or criticality assessments rather than risk assessments when deciding which adverse events to respond to. This may be because they consider that there is too much uncertainty in the evaluation of likelihood or that some impacts are considered so intolerable that they have to be addressed whatever their likelihood of occurrence.

Decisions about the risk treatment options, priorities and the expected level of residual risk should be taken in accordance with the organisation's defined risk management framework and governance (e.g. SPA, Security Governance Group).

More details on risk treatment implementation is provided in the SICS Framework element 'Establish ongoing governance'.

3.4 Monitoring the risks

Undertaking an assessment of the business risk can be a long process and requires input from a number of stakeholders and resources. By defining triggers that initiate the assessment process it ensures that the process is only run when needed. Such triggers are likely to vary from one organisation to another depending on the type of process, current level of security, current architecture, resources, etc. Examples of typical triggers are:

- Changes to:
  - Risk appetite
  - Threat level
- Criticality and risk of system
- Compliance assurances required
- New projects
- System changes
- Mergers and acquisitions
- Political circumstances
- Elapsed time since last assessment
- Incidents (internal and external).

Following a re-assessment of business risk it is essential that a number of corresponding items are also re-assessed to ensure that they are still in line with the overall business risk. They include:

- ICS security programme – to ensure the overall direction is still aligned with the business risk
- Governance – to ensure that the structure and composition suits the business risk needs
- Inventory – any changes to the inventory need to go through a formal change request and change control, and is communicated to appropriate stakeholders
- Response plans – these need to accurately reflect the current systems and processes

The process of re-assessment is likely to be resource intensive and should be proportional to the risk to critical systems. There is often a natural tendency to establish a standard routine of security assessment such as an annual review for each site, system and asset. However, this may not be the most efficient use of resources as some sites may be reviewed too frequently and others not frequently enough. The frequency of re-assessment should be matched to the criticality of the systems such as their impact on the enterprise and/or supply chain. One of the key outputs from each assessment of the business risk should be an indication of how frequently reassessments of the risk should take place.

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

4 CASE STUDY: LECTRIC DISTRIBUTION

4.1 Lectric Distribution on the start of a security journey

Lectric Distribution, is a Power Distribution Network Operator (DNO) with several regional distribution networks that has become aware of the increased threats facing their infrastructure. They historically procured their control systems without including any security considerations in their supply chain because those systems were operated on what they considered was a secure isolated environment. However, recently, they detected a malware infection on their control network through a workstation anti-malware tool on the corporate network which detected the infection when removable media originating from the field was attached to it.

Fortunately, the payload of the malware did not cause any real impact on the infrastructure but this happened at a time when reports on Stuxnet and other attacks were still fresh in people's mind, this first cyber incident on the control network therefore acted as a wakeup call.

The Plant Manager decided to take charge of this problem, and used the SICS Framework element 'Manage business risk' as a reference to guide her actions and assessing the business risks looked like a good place to start. She requested the help of the Enterprise Risk department and of Corporate IT to carry out this security risk assessment as those departments had the risk and the security expertise.

4.2 Lectric Distribution risk assessment approach

They came up with the following approach:

- **Scope**: They decided to carry out the assessment on a selection of their facilities that were representative of the entire estate
- **Team**: Each assessment was carried out with a team led by a member of the Enterprise Risk department and supported by a security specialist from the IT department and a control engineer with knowledge of operational technology and ICS. For one of the assessments, they decided to use a team of external consultants with experience in ICS security
- **Approach**: All teams followed the same approach broadly based on the SICS Framework element and used:
  - A list of ***threats*** coming from a risk assessment
  - The CPNI GPG on "Select and Implement ICS security controls" as a list of good practices against which to identify ***vulnerabilities*** their ICS environment
  - They opted for an ***evaluation of the risk*** based on Impact, Vulnerability (i.e. level of complexity to implement an attack exploiting this vulnerability), and level of Threat. They did not include the attractiveness factor as they did not think they could evaluate it accurately enough

– The following ***scales for impact*** came directly from their own Enterprise Risk Management framework.

Table 3 - Case Study: Lectric Distribution impact criticality scales

1: Low Impact	2: Medium Impact	3: Significant Impact	4:Critical Impact	5: Most severe impact
Impact on Health Safety and Environment				
slips and trips	minor injuries	major injury	incapacitating injury	death
Impact on electricity supply per percentage of nominal output				
<5%	> 5 % < 25%	> 25% < 50%	> 50% < 75%	> 75%
Impact on electricity supply: duration of incident				
<2 Hours	>2 hours <4 hours	>4 hours <12 hours	> 12Hours < 48 Hours	>48 Hours
Loss of confidential information				
Loss of information that was not meant to be in the public domain but that has no particular impact	Loss of information that could lead to adverse press coverage and minor embarrassment	Loss of information that could lead to adverse press coverage and major embarrassment	Loss of information that would constitute a breach under the data protection act or Payment Card Industry standard	Loss of information compromising the ability of the organisation to execute the strategy
Financial loss (loss of revenue, cost of repairs, customer compensation, penalties from regulator) per percentage of annual turnover				
x%	xx%	xxx%	xxxx%	xxxxx%

4.3 Lectric Distribution risk assessment results

They described each risk instance using the SICS Framework, an example of identified risks is shown in Table 4.

Table 4 – Case Study: extract from Lectric Distribution risk register

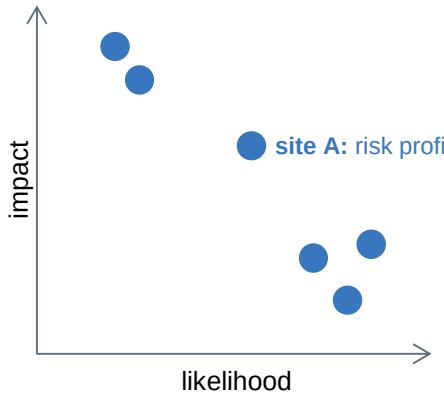
Risk instance	Risk level	Vulnerability	Threat source	Threat event	Vulnerability level	Threat Intensity	Impact	Comments
Unexpected consequences of service providers when connecting remotely to the control environment without prior authorisation	9	Uncontrolled remote connections in control environment	Service provider (SP)	Mistake	High	Low	3	There is no history of careless behaviour with suppliers as there is a strict organisational procedure before carrying out any maintenance work. However, the potential impact of mistakes could be critical on the supply.
Introduction of malware by maintenance personnel through use of removable media	24	No removable media control	Maintenance personnel (Privileged users)	Malware	Medium	High	4	Those events have the capability to propagate widely in the network as there is no effective protection. Major disruption of supply.
Destruction of equipment	3	Weak physical security	Physical Intruder	Vandalism	Low	Low	3	Disruption of supply limited as hardware infrastructure standardised and spare readily available

The risk level is derived from a risk matrix, an example of which is shown in Figure 4, the impact is derived from impact criticality scales as shown in Table 3, and the likelihood is derived from a risk table, an example of which is shown in

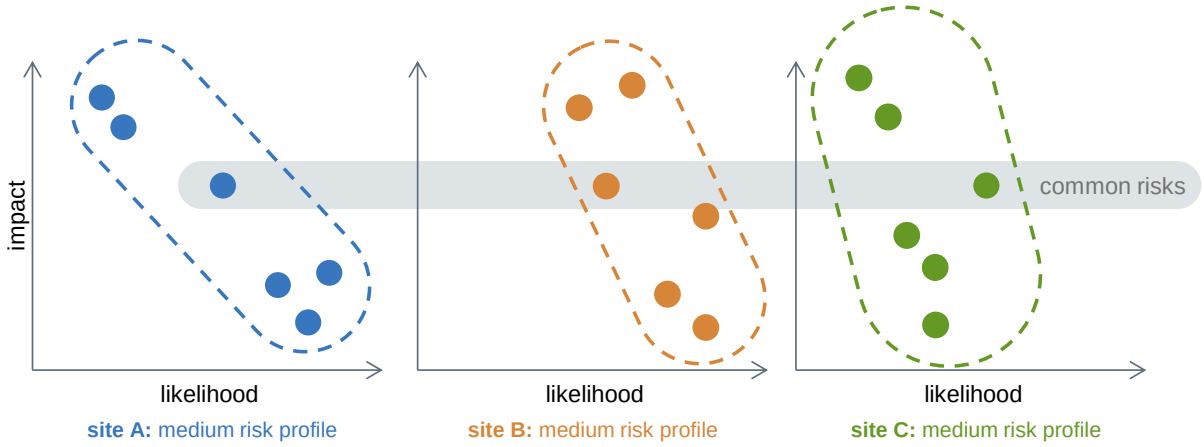
Table 2.

Having performed several risk assessments using the same approach and the same scales for evaluating the risks, Lectric Distribution now had valuable information on:

- The risk profile for each site



- Comparable data on risks between sites drawn from the multiple risk assessments, allowing them to identify:
  - The sites which require immediate attention
  - Common risks that can be managed together to benefit several sites, for example a common mitigation can be rolled out across the sites, with potential economies of scale, and standardisation of the solution.



The Plant Manager now had an evaluation of the risks that allowed her to identify some first priority actions. She also identified that many of the actions, short or long term, were beyond her scope of responsibilities and required wider company participation and sponsorship.

The Director of Enterprise Risk received the results of the ICS security risk assessments and he reported the aggregated results in the Lectric Distribution enterprise risk register. He decided to add this to the agenda of the next Board of directors meeting and invited the Head of Telemetry to present the results.

He decided that a strategy should be established to assess those business risks and he wanted this to be managed according to clear governance rules.

A TERMINOLOGY RELEVANT TO THIS GUIDE

Risk[9]	A measure of the extent to which an entity is threatened by a potential circumstance or event.
Risk appetite	The level of risk that is considered to be acceptable by the leadership of the entity taking into account the balance of risk with corresponding costs or loss of opportunity.
Threat	Any circumstance or event with the potential to harm an ICS through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorised disclosure of information, unauthorised modification of information, unauthorised destruction of information, or loss of information or information system availability.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source

[9] Taken from NIST SP 800-30 definitions

ACKNOWLEDGEMENTS

PA are grateful for the support and input from CPNI, CESG, the ICS community and those involved with CNI protection during the development of this good practice guidance framework. Contributions have been gratefully received and are too numerous to mention individually here.

About the authors

PA Consulting Group
123 Buckingham Palace Road
London
SW1W 9SR

Tel: +44 20 7730 9000
Fax: +44 20 7333 5050

Email: info@paconsulting.com
Web: www.paconsulting.com

For further information from PA Consulting Group on Industrial Control Systems security:

Email: IndustrialCyberSecurity@paconsulting.com

Web: http://www.paconsulting.com/industries/energy/energy-and-water-cyber-security/