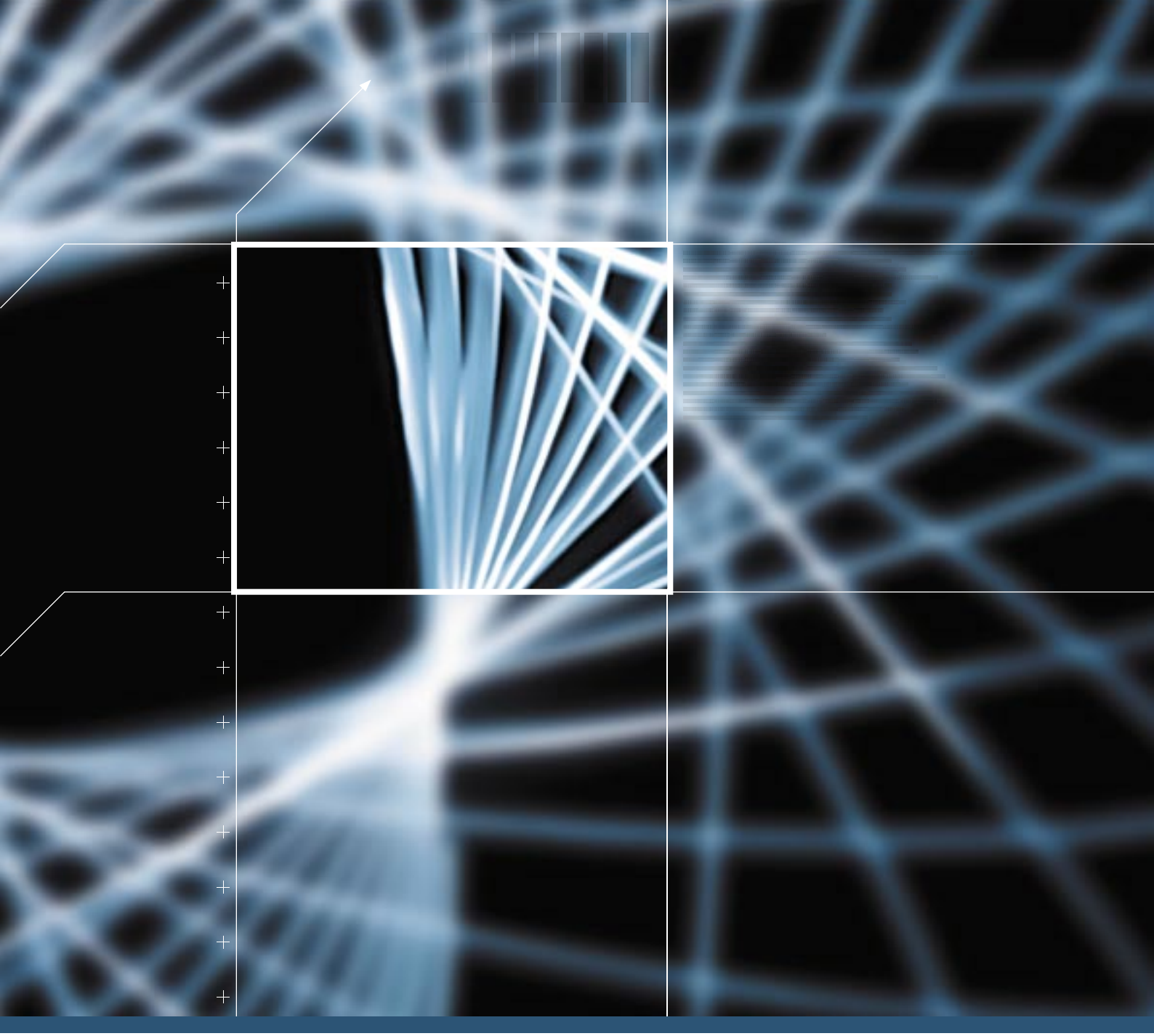

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 7. ESTABLISH ONGOING GOVERNANCE

CPNI
Centre for the Protection of National Infrastructure

This guide is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation's critical national infrastructure. The paper provides valuable advice on protecting these systems from electronic attack and has been produced by PA Consulting Group for CPNI.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Terminology

Throughout this framework the terms process control system and process control and SCADA system are used as generic terms to cover all industrial control, process control, distributed control system (DCS), supervisory control and data acquisition (SCADA), industrial automation and related safety systems.

1.2 Background

Process control and SCADA systems are making use of, and becoming progressively more reliant on standard IT technologies. These technologies, such as Microsoft Windows, TCP/IP, web browsers and increasingly, wireless technologies, are replacing conventional proprietary technologies and further enabling bespoke process control systems to be replaced with off the shelf software.

Although there are positive business benefits to be gained from this development, such a transformation brings with it two main concerns:

Firstly process control systems were traditionally only designed for the purpose of control and safety. Due to the need for connectivity for example for the extraction of raw plant information or for the ability to perform direct production downloads, the once isolated systems are being connected to larger open networks. This exposes them to threats that these systems where never expected to encounter such as worms[1], viruses and hackers. Security through obscurity is no longer a suitable kind of defence.

Secondly, commercial off the shelf software and general-purpose hardware is being used to replace proprietary process control systems. Many of the standard IT security protection measures normally used with these technologies have not been adopted into the process control environment. Consequently, there may be insufficient security measures available to protect control systems and keep the environment secure.

There are potentially serious consequences should these vulnerabilities be exploited. The impacts of an electronic attack on process control systems can include, for example: denial of service, unauthorised control of the process, loss of integrity, loss of confidentiality, loss of reputation and health, safety and environmental impacts.

1.3 Process control security framework

Although process control systems are now frequently based on standard IT technologies, their operational environments differ significantly from the corporate IT environment. There are a great number of lessons that can be learned from the experiences gained by the IT security experts and after tailoring some standard security tools and techniques can be used to protect process control systems. Other standard security measures may be completely inappropriate or not available for use in a control environment.

[1] The Wikipedia reference for a worm – A computer worm is a self replicating computer program. It uses a network to send copies of itself to other systems and it may do so without user intervention. Unlike a virus, it does not attach itself to an existing program. Worms always harms the network (if only consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

This process control security framework is based on industry good practice from the fields of process control and IT security. It focuses on seven key themes to address the increased use of standard IT technologies in the process control and SCADA environment. The framework is intended to be a point of reference for an organisation to begin to develop and tailor process control security that is appropriate to its needs. The seven elements of the framework are shown below in Figure 1.

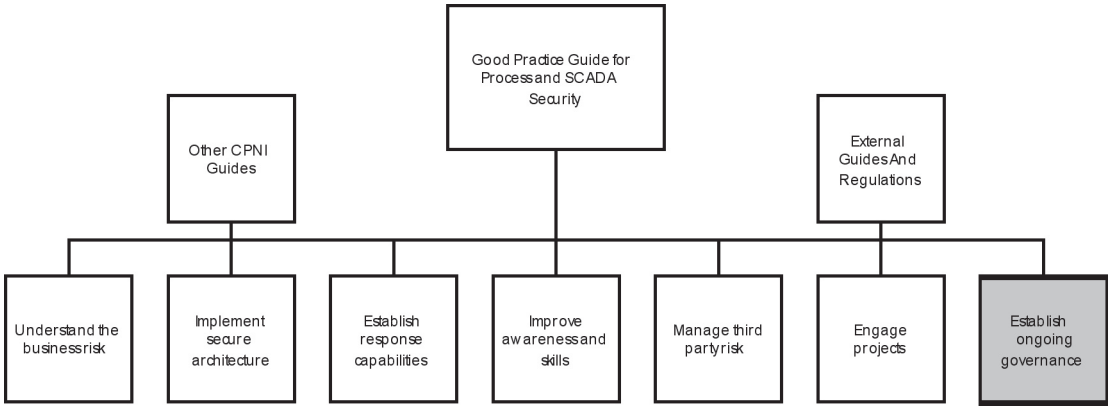

Figure 1 – Where this guide fits in the Good Practice Guide framework

Each of these elements is described in more detail in their separate documents, this document provides good practice guidance on understanding the business risk. All the documents in the framework can be found at the following link http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx .

1.4 Purpose of this guide

The **'Good Practice Guide - Process Control and SCADA Security'**, proposes a framework consisting of seven elements for addressing process control security. This **'Establish Ongoing Governance'** guide builds on the foundation provided in the top-level document by providing good practice guidance for defining and implementing appropriate governance frameworks for process control systems security.

This guide will not provide detailed policies and standards or procedures.

1.4.1 Target audience

Anyone involved in establishing process control security governance or standards:

- Process control and automation, SCADA and telemetry engineers
- Information security specialists
- Physical security specialists
- Business leaders
- Risk managers
- Health and safety officers
- Operations engineers.

2. ESTABLISH ONGOING GOVERNANCE SUMMARY

Formal governance for the management of process control systems security will ensure that a consistent and appropriate approach is followed throughout the organisation. Without such governance the protection of process control systems can be ad-hoc or insufficient, and expose the organisation to additional risk. An effective governance framework provides clear roles and responsibilities, an up-to-date policy and standards for managing process control security risk, and assurance that this policy and standards are being followed.

Governance: The system by which organisations are directed and controlled.

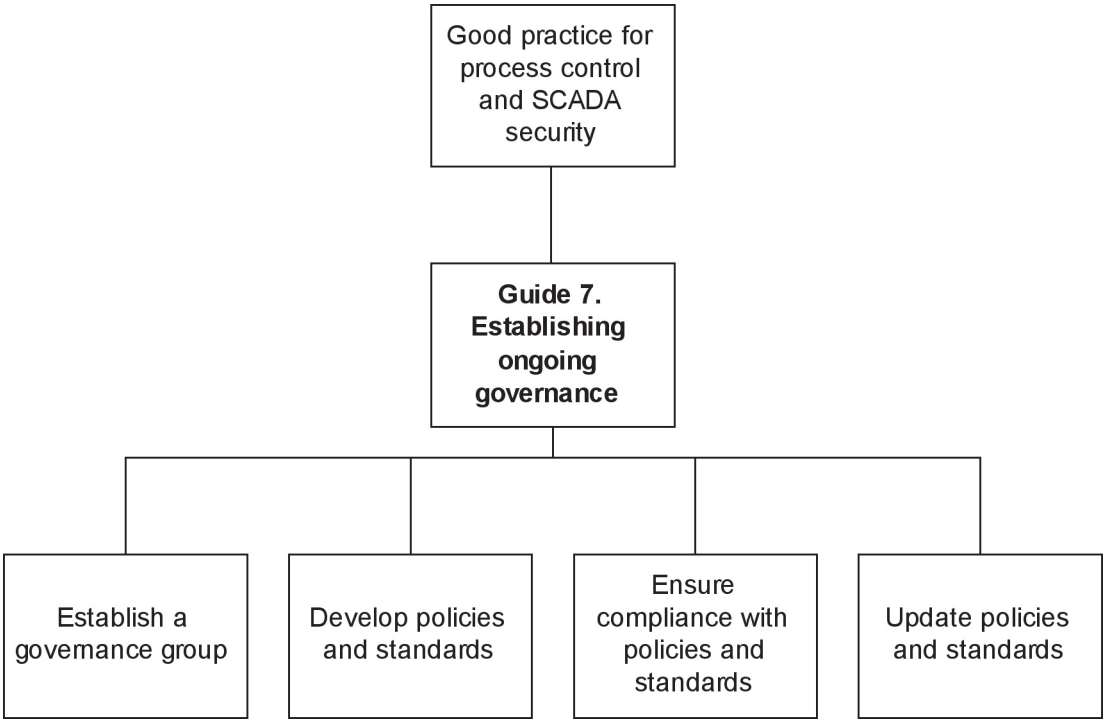

Figure 2 – Establish Ongoing Governance Document Structure

3. ESTABLISH A GOVERNANCE GROUP

3.1 Context of this section within the overall framework

The governance group (sometimes referred to as a committee or council) provides a pivotal role by governing each of the seven elements of the framework. The governance group will have responsibility for process control security risk and impacts; therefore it will be involved in all of the themes of the process control security framework. Individuals in the business will have accountability for process control security. The diagram indicates a simple flow of information that helps when deciding the most appropriate members to serve in the governance group and the key considerations when selecting members.

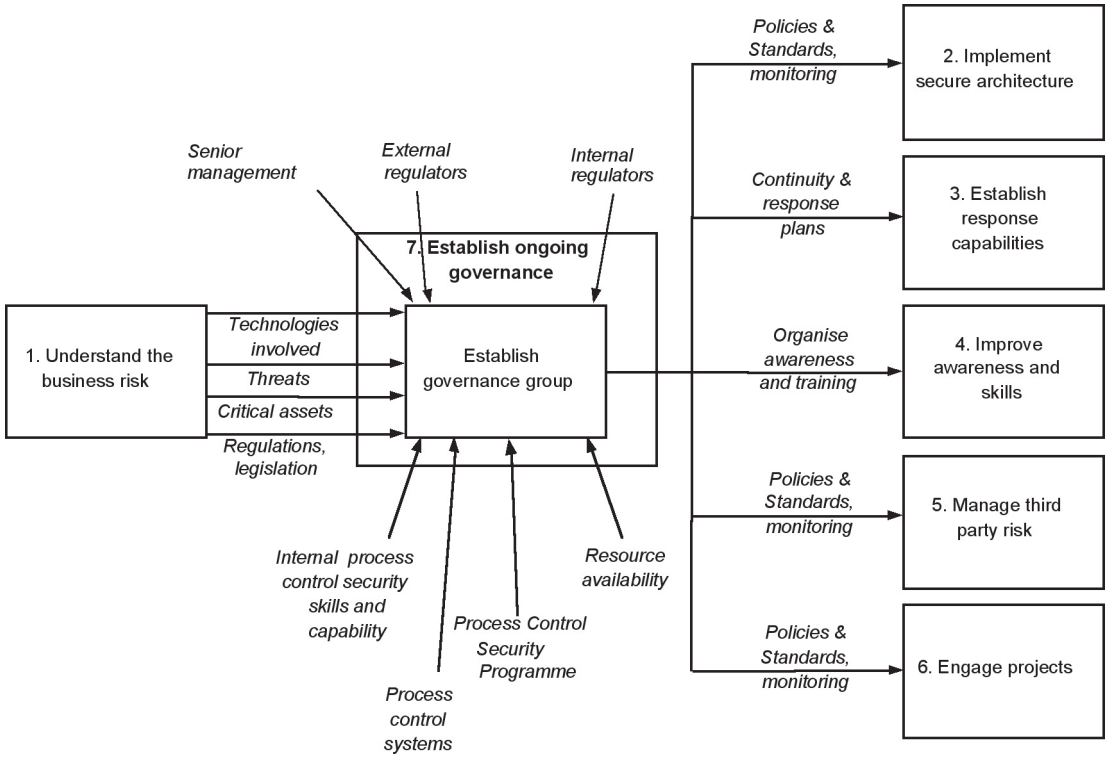

Figure 3 – Where 'Establish a governance group' fits in the framework

3.2 Rationale

A clearly defined governance group with well articulated roles and responsibilities is essential to ensure that process control security risk is effectively and comprehensively managed. Whilst it would be impossible to define how this governance group would fit into every organisation, the members should be a blend of decision makers and technical experts from appropriate disciplines. This group needs to fit into the organisation existing governance and reporting structure and have the mandate to enable it to govern process control for the organisation at a both strategic and operational level.

3.3 Good practice principles

The relevant good practice principles in the overarching document Good Practice Guide Process Control and SCADA Security are:

- Obtain senior management support for process control system security.
- Identify impacts of legal and regulatory requirements on process control security.
- Ensure process control system security practices align with the business and operational needs.
- Define roles and responsibilities for all elements of process control security.
- Appoint a single point of accountability for process control security risk. Depending on the size of the organisation this may be one person or it could be a number of regional points of accountability reporting into a single point.

3.4 Good practice guidance

Regardless of the approach to governance that an organisation favours it will need to ensure that the following functions are represented as a minimum:

- Business – provides a perspective of what the business needs, likely to be one or more senior managers.
- Process control – provides process control representation and capabilities, identification of critical assets and existing exposure.
- Security – provides information and physical security expertise, experience and integration perspective.
- Engineering – where engineering is a separate function to process control, input may be required to ensure practical operations/ implementation guidance.
- Safety, health & environmental – key guidance to ensure alignment and compliance with safety, health & environmental issues.

It is essential to have each of the functions on the process control security governance group as they represent the key perspectives that will ensure a balanced approach to meeting business's process control security needs. Other functions that should be considered for representation are business/operational risk managers, business continuity and emergency planning, IT infrastructure, telecoms and physical security. They can either be included in the core roles or if more suited to your business, the role can be independently represented.

How responsibilities are spread across these roles will be specific to the culture of your organisation, the resources you have available, and the chosen governance structure, geographic reach, etc. Typical responsibilities that would be part of the governance of process control security are:

- Balance business needs with costs of mitigation measures
- Build safety, health and environmental requirements into process control security
- Consider legal requirements
- Consider HR implications of process control security
- Manage the process control awareness and communication plan
- Monitor and report process control security status to the board
- Engage design authorities

- Set operational scope and boundaries
- Define accountabilities
- Maintain a register of process control projects (ensuring appropriate security to prevent unauthorised access to project information)
- Maintain ownership of the corporate risk register related to process control security related risk register
- Own and maintain the process control security strategy (short term and long term plans)
- Own the process control security programme.

The accountability for process control security may be delegated by governance group either directly or via a number of reporting levels depending on the organisation, it's size, culture, existing reporting structure, etc. Organisations that rely very heavily on process control or that would suffer significant impact if process control systems were lost are more likely to have a governance group that is more closely associated with the executive board. In return for specific delegated accountability the governance group will be tasked with providing a clear indication of the organisations level of exposure and how they plan to address it. A strong reporting channel is essential to ensure that the scale of any potential impact from a process control incident is clearly communicated so that any significant impact on the business is understood and discussed at the appropriate level. It is also very important that the governance group clearly understands the boundaries of the accountability that has been delegated to them. The diagram below provides an overview of the governance group considerations.

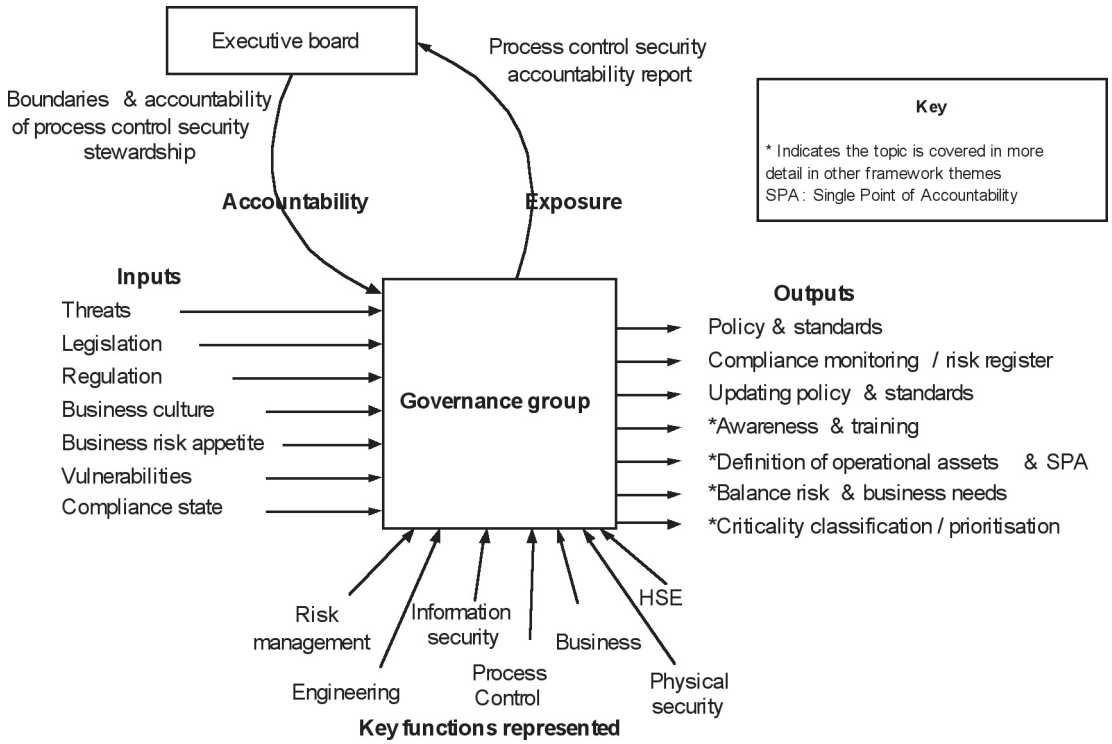

Figure 4 – Governance group function

Serving on the process control governance group is usually a part-time role; how much time is spent on governance group duties is down to the magnitude of the risk and what existing structures are already in place. The duties of the governance group include:

Strategic: setting the process control security policy and initiating the process control security programme.

Tactical: implement the process control security programme, provide process control security awareness and training advice, and policy and standards compliance monitoring. Setting and approving budgets.

Operational: forming and liaising with the Process Control Security Response Team which monitors, analyses and responds to alerts and incidents. Monitoring risk exposure.

4. DEVELOP POLICY AND STANDARDS

4.1 Context of this section within the overall framework

Developing process control security policies and standards is closely connected to the framework theme 'Understand the business risk'. Much of the output from understanding business risk will feed directly into setting appropriate policies for process control security within an organisation. The process for determining policies needs to be driven by business risk, and will usually happen at a senior management level. After consideration of the business risk and organisation's risk appetite, the senior management will seek input from control teams, IT security, safety, health and environmental and the business to determine what is an effective policy. It is also important to consider what external regulations and legislation needs to be considered, and what mitigation measures or technology is currently available.

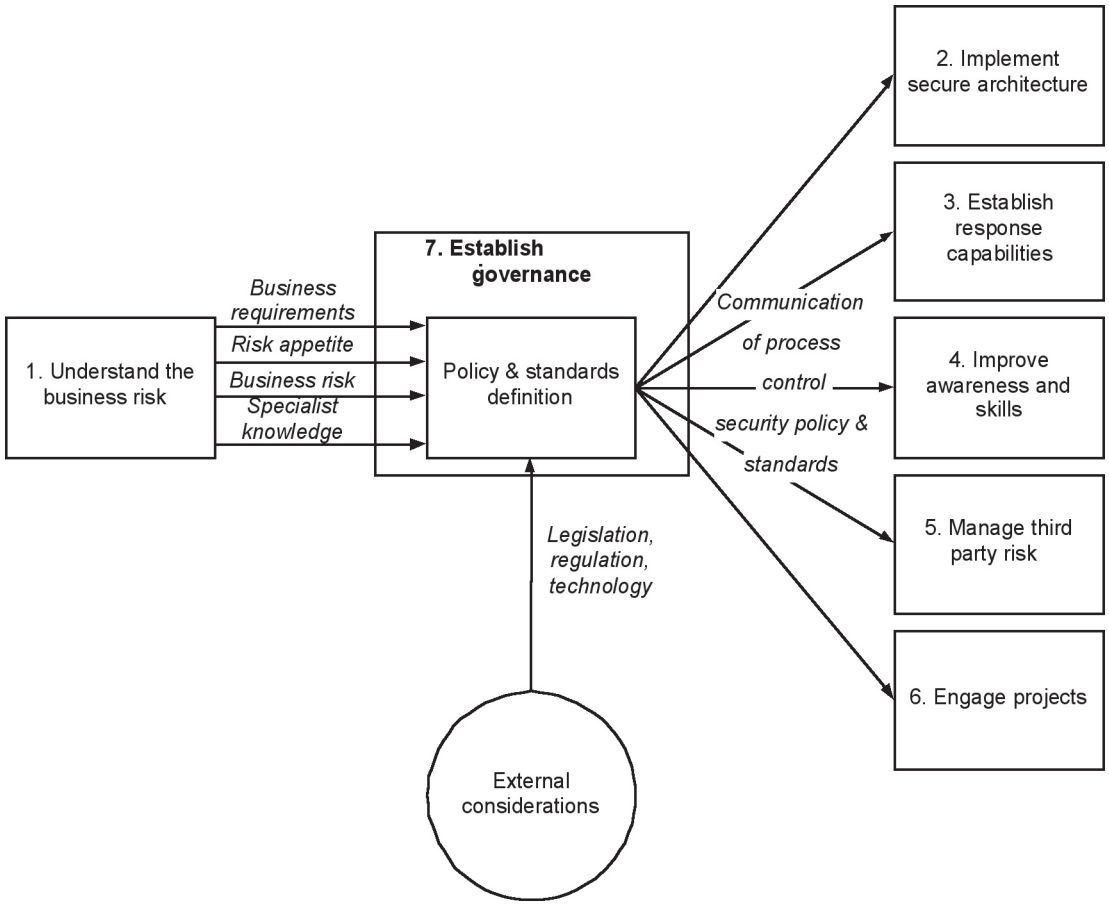

Figure 5 – Where 'Develop policy & standards' fits into the framework

Each of the remaining five process control security framework themes will refer to, and make use of the organisations process control security policies and standards and a high level overview is provided below.

4.2 Rationale

Process control security policies are the translation of an organisations risk appetite into the boundaries within which actions can take place, and standards are a set of repeatable building blocks that define the creation, maintenance and removal of process control system components. A policy will define the organisation's boundaries, and standards provide a consistent organisational interpretation to achieve the desired quality of the defined policy.

Example: A policy might describe what traffic is allowed, albeit at high level, for example 'no traffic originating in the office systems may pass into the process control system'.

Policies and standards are the mechanism by which an organisation can communicate the desired level of process control security protection and how this should be achieved.

4.3 Good practice principles

The relevant good practice principles in the overarching document Good Practice Guide Process Control and SCADA Security are:

- Define, document, disseminate and manage under change control, formal policy and standards for process control system security
- Ensure that the policy and standards accurately reflect the organisational requirements, support business requirements
- Ensure policy and standards are agreed to by all relevant parties.

4.4 Good practice guidance

The creation of process control security policy and standards could be either handled as an entirely unique entity or combined with existing IT security standards or engineering standards. There are a number of reasons for both approaches and either work equally well as long as they are able to accurately represent the quality and detail required to protect process control systems to the stated business requirements.

An organisation may choose to create a separate set of policies and standards if:

- Process control systems are business critical or have an impact on safety
- There is a strong process control resource capability
- The current security policy and standards are not adequate to cover the process control systems
- Other cultural or historical reasons.

Similarly it may be appropriate to combine process control security policies and standards with existing security policies and standards, or add a process control security section to these standards documents if:

- Process control systems are business critical and closely integrated into key business processes
- There is good engagement between security, process control and IT support

- There is good alignment with corporate security controls and the controls required to secure process control systems
- There are limited process control resources and capabilities.

Care must be taken if combining the policies and standards as clear ownership, agreed quality, security principles and many other aspects need to be unambiguously defined to ensure both IT and process control security goals are met in an effective way. This is seldom a simple process as the operational requirements of IT security and process control security can differ in a number of fundamental areas such as version updates.

A dedicated architecture and standards working group could be formed to report into the governance board ensuring that both IT and process control groups are involved together in defining policy, standards and implementation guidance.

Figure 6 shows how the detail and number of documents varies between policy, standard and guidance. The higher up the triangle there is less detail, fewer documents and fewer changes and the converse applies as you go down the triangle with implementation guidance documents being the most detailed and most likely to need updating regularly.

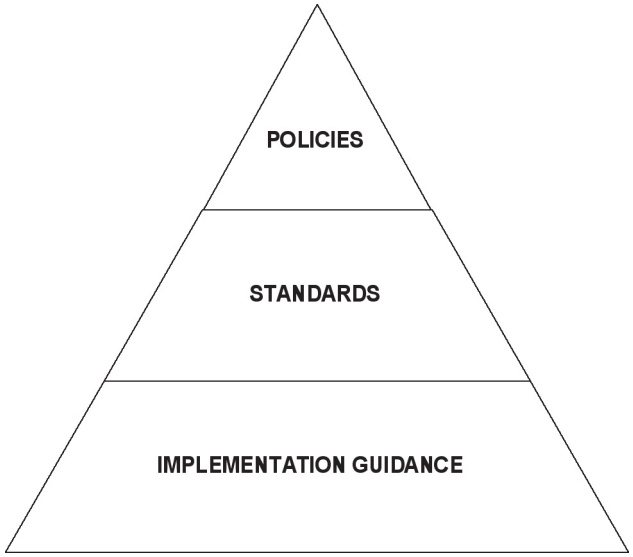

Figure 6 – Relationship of policy, standards and guidance documents

4.4.1 Policy

The policy will need to provide specific statements of principals or guiding actions that imply clear commitment by the organisation; statement of values or intent that provides a basis for consistent decision-making and resource allocation; and definite method or courses of action to guide and determine present and future decisions. Typical characteristics of policies are that they:

- have widespread application
- change infrequently
- are usually expressed in broad terms

- are not technical documents
- are statements of 'what' and/or 'why'
- address major operational issues.

Process control security policies are usually high level documents that give the basic 'framework' with respect to a business or technical need. In most cases a policy on it's own without associated standards would be too high level to communicate what needs to be done. It is the standards (and implementation guidance) that provide the information needed to implement the policy goals to the required quality level.

The minimum detail that should be included in a policy document is:

- the policy statement of intent – 'the controls that need to be in place, to this quality'
- to what, or whom the policy applies to – 'the scope or boundaries of the policy'
- who owns the policy – 'who will publish and update it'
- what triggers the update of the policy – 'when should the policy be reviewed'
- the exception criteria and process – 'when is the policy not applicable'.

When writing a policy it is important to recognise that there are a number of factors including existing business policies and standards that may influence the process control security policy. It is all too easy to write a process control security policy in isolation without considering the business, operational, or financial impact of the statements that are being made. Documents that are written in this way are very unlikely to be endorsed and accepted by the business and will result in a waste of valuable effort.

When writing a process control security policy it is important to continually check that it meets with the following criteria:

- alignment with business strategy
- alignment with IT strategy and policies
- alignment with safety, health and environmental policy
- alignment with physical security policies of the organisation
- consistent use of existing/ established terminology
- consistency with the level and audience of other policies.

The Governance Group is accountable for setting process control security policy and ensuring it is signed-off at whatever level the organisation requires.

4.4.2 Standards

The characteristics of standards with respect to policies are that they:

- are narrow in application
- are prone to change
- are often stated in detail
- may include some technical detail
- include statements of 'how,' 'when' and sometimes 'who'
- describe related processes.

Process control security standards documents provide a common approach to be followed throughout the organisation. They enable quicker delivery, at a known quality that generally reduces the complexity of the task. Standards provide a consistent repeatable approach that reduces duplication by sharing specialist knowledge that has been adapted for a specific organisation. The development of good quality standards will break down tasks into manageable chunks and will provide a better understanding of the task and the risks that are being mitigated.

Standards are likely to be drafted with the help of specialist internal development groups or with the aid of third parties. Standards define the boundary lines required to meet the quality and capability described in the policy document. Standards are strongly influenced by relevant legislation and regulation (Health and Safety, DTI, environmental), existing industry standards, the technology available and future business or industry requirements.

When considering what to include in a standard the minimum detail that would be expected in a standards document is:

- The policy statement to which the standard applies – 'which policy or policies'
- The intended audience or readership – 'the level of detail'
- The definition and application of the standard – 'what is it, how is it applied in term of people, processes and technology'
- To what or whom the standard applies – 'the scope or boundaries of the standards'
- Who owns the standard – 'who will publish and update it'
- Update of the standard – 'when should the standard be reviewed'
- The exception criteria – 'when is the standard not applicable'.

Due to the detail involved in standards and the frequency of the changes, it is common for them to need sign-off only at the governance group level. This does not mean that the process is any less stringent, but it does reflect that the detail will only be understood by a limited group of reviewers.

4.4.3 Implementation guidance

There is a third group of documents that are often used to support standards, usually known as 'implementation guidance' documents. Where a standard has a number of possible applications, these guides provide the additional detail to ensure the appropriate translation of the standard into practical solutions for specific environments without the problem of overcomplicating the standard itself. They are generally the most detailed of all the documents and only focus on a specific application of the standard, such as how to configure a specific firewall to the 'standard' required.

4.4.4 Reference standards and guidance

There are a number of sources of guidance with respect to developing process control security standards from vendors, government institutions and industry regulators. Most of the guidance will help define the required quality expectations. Some of the main sources of standards and guidance are listed below:

- CPNI – Centre for the Protection of National Infrastructure, (www.cpni.gov.uk)
- CPNI Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
- CPNI Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
- CPNI Good Practice Guide Patch Management
- CPNI Best Practice Guide Commercially Available Penetration Testing
- CPNI guide on Personnel Security Measures
- ISO 17799 – International Code of practice for information security management
- ISO 27001 (formerly BS 7799-2) – International Specification for Information Security Management
- PCSRF – Process Control Security Requirements Forum
- IEEE – Institution of Electrical and Electronics Engineers
- IEC – International Electrotechnical Commission
- Industry – specific guidance from organisations such as API, NERC, AGA, OLF, CIGRE
- Vendor specific guidance.
- Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
- Securing WLANs using 802,11i
- Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
- Cyber Security Procurement Language for Control Systems
- NERC Critical Infrastructure Protection (CIP)
- DHS Catalog of Control System Security Requirements
- NIST Guide to Industrial Control (ICS) Systems
- ISA SP99, Manufacturing and Control Systems Security

When writing policies, standards and guidance the above reference points can be taken as a starting point from which to adapt an organisational specific set of documents based on the business requirements, characteristics and culture.

The primary objective is to capture the important requirements. Avoid falling into the trap of writing a wish list based on a specific supplier or piece of hardware/ software.

Simply copying industry best practice across your organisation without tailoring it may not improve your process control security, and may even hinder your operations and waste valuable time and resources. However, the application of good practice principles to an identified threat in your organisation will help mitigate the problem according to an organisations level of risk appetite.

Quality documents written to address specific risk appetite and threats will be easier to implement, monitor, update and comply with and will be vastly superior to copying generic best practice.

5. ENSURE COMPLIANCE WITH POLICY AND STANDARDS AND REPORTING TO EXTERNAL REGULATORS

5.1 Context of this section within the overall framework

Effective governance requires not only the existence of adequate policies and standards, but also monitoring of compliance.

The compliance process provides a very important feedback loop to highlight any difficulties with the policy and standards, and can be a trigger to update or amend where the existing guidance does not achieve the desired goals.

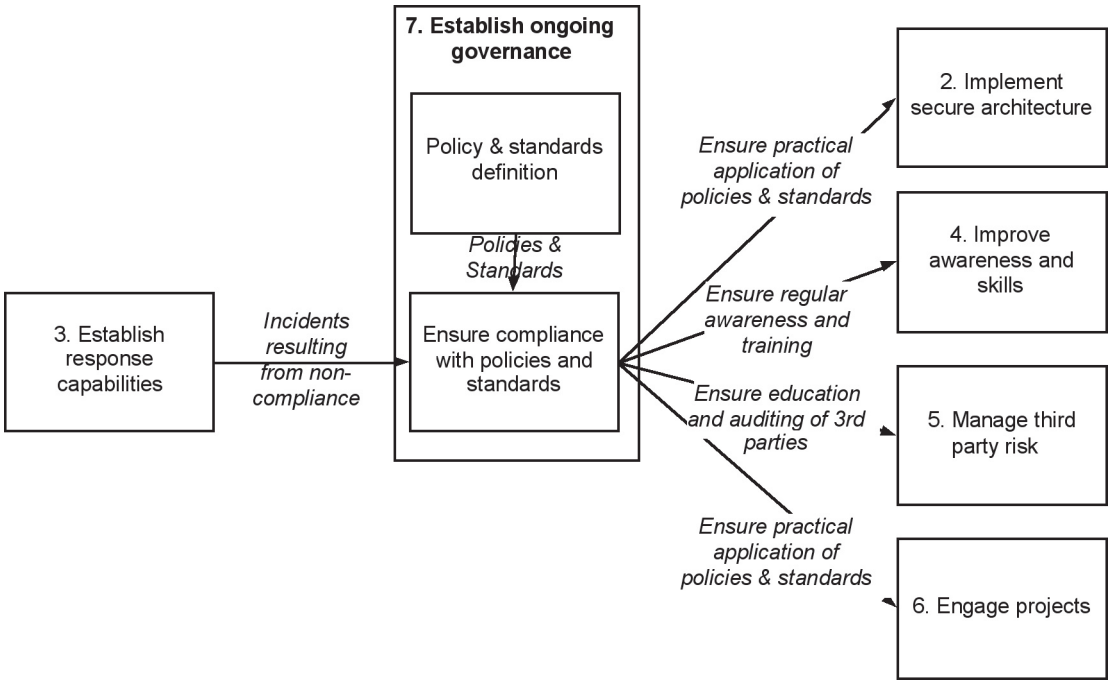

Figure 7 – Where 'Ensure compliance with policies and standards' fits into the framework

5.2 Rationale

The activity of ensuring compliance with policy and standards is vital to assure the appropriate actions are being taken to the right quality requirements and is a key function of the establishing governance theme. Compliance with policy and standards will:

- Assure that process control systems are protected to the agreed level of business risk
- Ensure that wasteful duplication of effort is being avoided and that consistent solutions are being deployed across the organisation.

5.3 Good practice principles

The relevant good practice principle in the overarching document 'Good Practice Guide Process Control and SCADA Security' is:

- Implement an assurance programme to ensure that the process control system policy and standards are complied with on a continuous basis.

5.4 Good practice guidance

There are a number of approaches to ensuring compliance with policy and standards and again these approaches should be tailored to match the organisation's culture, capabilities, and existing initiatives. Some organisations feel happier with detailed information on which areas are compliant and which are not. Others prefer to receive exception reports only indicating where non-compliance has been recorded. The task of compliance can be broken down into three key decisions:

- What information is required, in what detail and when?
- How will the information be collected and by whom i.e. what compliance process will be used?
- What impact does non-compliance have on the business?

5.4.1 What information is required, what detail and when?

The question that needs to be asked for the first decision is 'What level of information is manageable whilst still providing enough detail to be of value in decision making?'

This will vary between organisations but it is worth remembering that too much information can be as bad as not enough. If people feel that the information they are submitting is not being read then the quality will soon decline, if someone is trying to flag a problem with a policy or standard but doesn't have the scope to do so, then there is the possibility that they may write their own informal guides and just pay lip-service to the company documents.

Key information that should be sought for compliance reporting:

- Management to identify person responsible for implementing report outcomes
- Single point of accountability for compliance
- Relevant deviation from policy or standards
- Business impact implications
- Date of planned resolution
- Relevant circumstances context (e.g. reasons for non compliance).

5.4.2 How will the information be collected and by whom?

This issue is one of the capability and resources available to ensure compliance and can be approached in a number of ways. Depending on the quantity, quality and frequency of compliance checking an organisation can opt to resource the activity in-house through self-assessment, peer review or an internal audit department. This approach has many benefits including a greater sense of ownership of any issues or excellence, but it can occupy valuable

time of specialist internal resources. Another approach is to outsource the task to a third party specialising in process control security. This option provides more objective results and there is less chance of problems being hidden but it is likely to cost more. There is also the issue of security information being passed to a third party presenting a possible vulnerability, so external resourcing should be considered carefully. If there are external bodies involved no-compliance may have a regulatory impact and needs to be identified.

External compliance monitoring doesn't have to be a formal audit and could involve a more informal iterative approach.

Option summary:

- Self-assessment – an assessment that is conducted by the department accountable
- Peer review – an internal review by an associated department which is not accountable
- Internal audit – an audit conducted by the organisations internal audit function
- External audit – an audit conducted by an external organisation
- Assisted self-assessment – an assessment that is conducted by the department, assisted by a process control security specialist
- External health check – a review of key industry specific vulnerabilities conducted by an external organisation.

Further guidance on auditing can be found in the NIST 'Guide to Industrial Control Systems (ICS) Security' (see appendix A).

5.4.3 What impact does non-compliance have on the business?

The final key decision is what, if any, additional business risk is posed, if a significant deviation from your organisations policy or standards has been reported. It is important to capture sufficient information about non-compliance to make an informed decision about the potential threat to feed into the 'understand the business risk' component of this framework.

- What is the likelihood of the risk materialising?
- How quickly will it impact the business?
- What mitigation is in place or is planned?

The minimum process control security compliance monitoring advised: there are many areas that can be assessed with respect to compliance but as with most things a balance needs to be struck between the hard facts and the context of the situation. Three areas that should always be carefully monitored are segregation, systems monitoring & detection and patching. To most organisations these areas present the largest threat to the business. Therefore there should be policies and standards in place and special attention should be given to monitoring compliance in the organisation, such as:

- **Segregation** – are process control networks appropriately segregated from office networks and the outside world by an appropriate means?
- **Monitoring & detection** – is the process control firewall log baselined and reviewed; is user/ system activity monitored; are anti-virus logs monitored, etc.
- **Patching** – how quickly are patches applied, where are they received from, are all machines patched, etc.

- **AV protection** – how quickly are updates made, what is the scanning method or frequency
- **Response plans** – are plans reviewed and updated regularly (e.g. annually)
- **Backups** – backup and restore procedures.

Typical compliance monitoring activities include:

- Using automated tools or checklists based on the applicable (technical) standards.
- Interviewing systems owners, users, managers e.g. to assess awareness
- Examining documentation as evidence of process being carried out (e.g. change control, exception processes)
- Using penetration testing or vulnerability scanning (with caution).

Determining how often compliance checks should be carried out will vary between organisations. It is not uncommon to run the checks daily if automated systems allow it; for checks such as access privilege it is more likely to be monthly or quarterly depending on staff turnover, use of contractors, etc. Full system reviews are likely to be conducted annually or less frequently if the systems are low risk. The key point is to match the frequency of monitoring to the volatility and perceived risk of the system.

6. UPDATE POLICY AND STANDARDS

6.1 Context of this section within the overall framework

Updates to policies or standards can be triggered from any other theme of the process control security framework. The business may decide it wants to change from its current stance on risk, security advancements in architecture may prompt an update, or the decision to outsource the provision of a firewall may trigger a policy or standard change to accommodate the change in risk. A common source of change is that the practical application of a standard proves over-burdensome so the standard is relaxed or otherwise modified to make compliance easier. There are also a number of external factors that may cause components within the framework to cycle through security processes that eventually result in an update to a policy or standard. Irrespective of the source of the trigger it is essential that the organisation has an effective process to respond to the request for change and take the appropriate action.

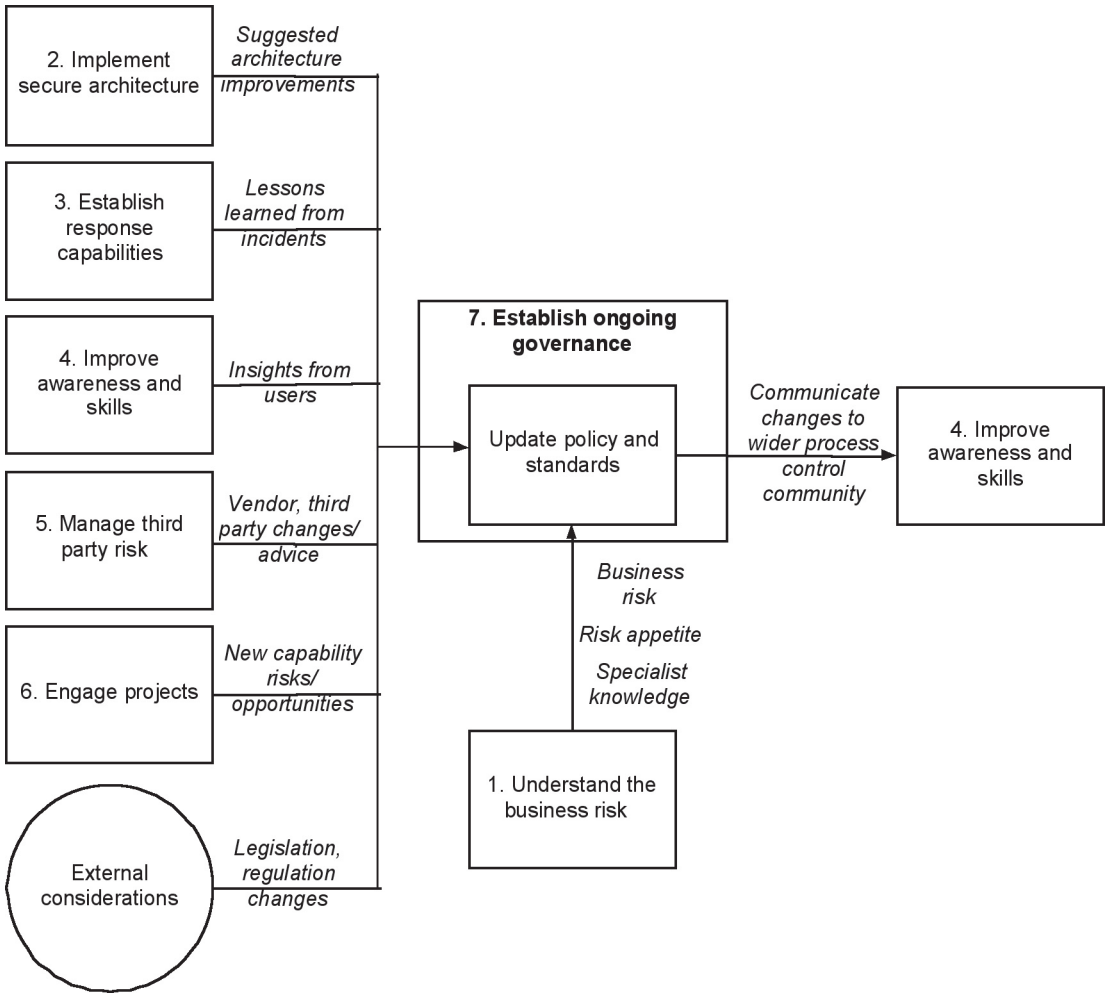

Figure 8 – Where 'Update of policy and standards' fits into the framework

Following the update of policy and standards it is also very important to communicate the changes to raise awareness or develop new skill capabilities in the wider process control environment.

6.2 Rationale

Process control technology, legislation, regulation and threats are continually progressing and evolving. Therefore it is essential that policy and standards are updated regularly to accurately respond to these changes.

6.3 Good practice principles

The relevant good practice principle in the overarching document Good Practice Guide Process Control and SCADA Security, is:

Establish an ongoing programme to ensure that the process control security policy and standards are regularly reviewed and updated. This could take the form of annual reviews or a review prompted by changes:

- to current threats
- in legal and regulatory requirements
- in the business requirements
- in operational requirements
- to operational equipment
- to the strategy or long term plan.

6.4 Good practice guidance

There needs to be a balance between constantly updating documents and ensuring that the documents are relevant; this is why the structure and detail covered in policies and standards need to be carefully written. By investing time in constructing good quality, flexible, but unambiguous policies and standards your organisation should be able to amend only specific sections, rather than having to conduct a complete re-write.

A key principle when writing policy and standards is to consider what the expected lifespan will be before it will need to be updated; this approach cannot accommodate unexpected changes but it should be able to factor in technology developments.

As with the initial creation of a policy or standard, updating can be a time-consuming process. Amendments are likely to need a number of stakeholders to review and comment and the impacts on process control systems and the wider business need to be carefully considered. Some changes can be more straightforward than others and it is good practice to categorise the change so that only the stakeholders that need to be involved are asked to review the updates. The categories that an organisation chooses need to consider the organisational structure and change control/ review process, but a number of organisations use the following categories:

- local update
- country update
- regional update
- enterprise-wide update.

It should be noted that the governance group should provide continuity to ensure that relevant information is made available and is disseminated appropriately even if the policy or standards updates have a limited stakeholder sign-off.

The optimum position within an organisation would be if updating policy and standards are built into ‘business as usual’ procedures such as Safety, Health and Environmental audits so that they became a part of existing everyday activities.

Where it is not possible to comply with a policy and standard then an exception policy should exist to ensure that this non-compliance is authorised, a risk assessment has been carried out and the residual risk is understood.

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 4.4.4

Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision, www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Process Control Security Requirements Forum
www.isd.mel.nist.gov/projects/processcontrol/

Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

International Electrotechnical Commission (IEC)
www.iec.ch

Norwegian Oil Industry Association (OLF)
www.olf.no/english

American Petroleum Institute (API)
www.api.org

North American Electric Reliability Corporation (NERC)
www.nerc.com

American Gas Association (AGA)
www.aga.org

International Council on Large Electric Systems (CIGRE)
www.cigre.org

National Institute of Standards and Technology (NIST)
www.nist.gov

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf.

Securing WLANs using 802,11i –
http://csrp.inl.gov/

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

DHS Catalog of Control System Security Requirements
www.dhs.gov

DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

ISA SP99, Manufacturing and Control Systems Security
www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

Section 5.4.2

NIST Guide to Industrial Control Systems (ICS) Security
http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

GENERAL SCADA REFERENCES

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/BS-78582006/

BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

CPNI SCADA Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

DHS Control Systems Security Program
http://csrp.inl.gov/

DHS Control Systems Security Program Recommended Practice
http://csrp.inl.gov/Recommended_Practices.html

Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdfISA SP99 –

DHS Catalog of Control System Security Requirements
www.dhs.gov

Manufacturing and Control Systems Security
www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.html

Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf.

Achilles Certification Program
www.wurldtech.com/index.php

American Gas Association (AGA)
www.aga.org

American Petroleum Institute (API)
www.api.org

Certified Information Systems Auditor (CISA)
www.isaca.org/

Certified Information Systems Security Professional (CISSP)
www.isc2.org/

Global Information Assurance Certification (GIAC)
www.giac.org/

International Council on Large Electric Systems (CIGRE)
www.cigre.org

International Electrotechnical Commission (IEC)
www.iec.ch

Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

National Institute of Standards and Technology (NIST)
www.nist.gov

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

Norwegian Oil Industry Association (OLF)
www.olf.no/english

Process Control Security Requirements Forum www.isd.mel.nist.gov/projects/processcontrol/
US Cert
www.us-cert.gov/control_systems/

WARPS
www.warp.gov.uk

ACKNOWLEDGEMENTS

PA and CPNI are grateful for the comments and suggestions received from the SCADA and Control Systems Information Exchange and from other parties involved with CNI protection around the globe 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

This document was produced jointly by PA Consulting Group and CPNI.

Centre for the Protection of National Infrastructure
Central Support
PO Box 60628
London
SW1P 9HA
Fax: 0207 233 8182
Email: enquiries@cpni.gov.uk
Web: www.cpni.gov.uk

For further information from CPNI on process control and SCADA security:
Internet: www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

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 process control and SCADA security:
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security