CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

ESTABLISH ONGOING GOVERNANCE

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 v1.0
Prepared by:	PA Consulting Group	Document reference:	

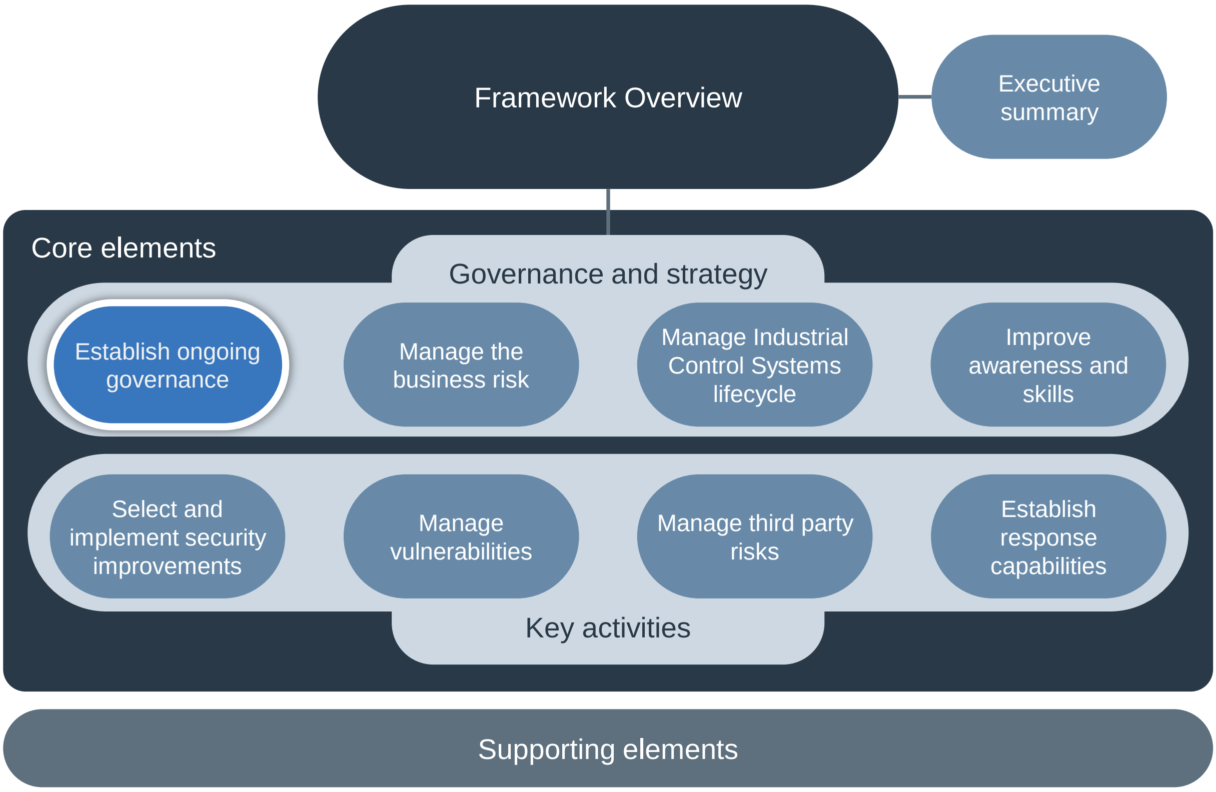
CONTENTS

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 Establish ongoing governance - summary

The objective of this guide is:

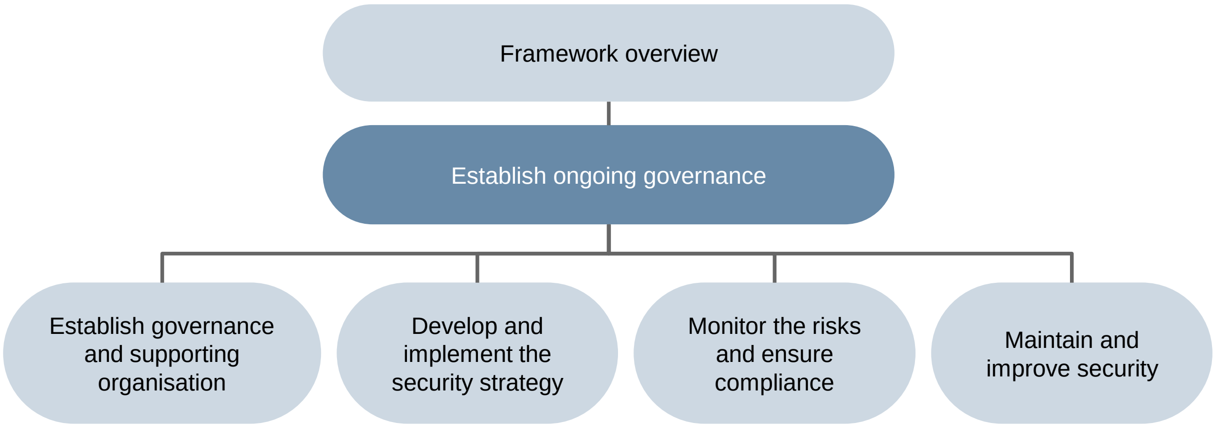
- To formally establish a governance framework to ensure that ICS security risks are managed consistently and appropriately on an ongoing basis.

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

Organisations need to ensure that the ongoing governance for managing their ICS security risks addresses these risks appropriately and that there is continuous review and improvement of security measures so they reflect any changes in the organisation and in its external environment.

Four principles of good practice should be followed to establish this ongoing governance. These are shown in Figure 2.

Figure 2 – Good practice principles to establish ongoing governance


Framework overview
Establish ongoing governance
Establish governance and supporting organisation
Develop and implement the security strategy
Monitor the risks and ensure compliance
Maintain and improve security

By following these principles, an organisation should be able to provide a strategy for ICS security; to monitor compliance; and manage the risks to ICS outlined in this guide.

2 ESTABLISH GOVERNANCE AND SUPPORTING ORGANISATION

A clearly defined governance process and supporting organisation with well-articulated roles and responsibilities are essential to ensuring that ICS security risk is effectively and comprehensively managed, and that defined intermediate and long term risk management objectives are shared.

Whilst it is impossible to define what a security organisation would look like in every context, a number of key principles can be established. For example, it is clear that a governance group is most effective if it has a blend of decision makers and technical experts from appropriate disciplines. This group should then fit into the organisation's existing governance and reporting structure and have the mandate to enable it to govern ICS security risk for the organisation at both strategic and operational levels. Alternatively, it may be possible for an organisation to use an existing governance group and to add ICS security risk to its agenda.

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

- Obtain senior management support for ICS security management
- Identify any impacts of legal and regulatory requirements on ICS security
- Define roles and responsibilities for all elements of ICS security throughout the organisation
- Appoint a single point of accountability for ICS 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 report into a single point.

2.1 Create the governance group

Regardless of the approach to governance, an organisation will need to ensure that the following functions are represented in the governance group:

- **Business** – provide a perspective of what the business needs, and who are likely to include one or more executives with sufficient influence over the board
- **ICS** – provide ICS capabilities and identification of critical assets and existing risk exposure
- **Security** – provide ICS and physical security expertise, experience and a perspective on integration
- **Engineering** – where engineering is a separate function to ICS, it may be necessary to ensure the group has access to guidance on practical operations and implementation
- **Enterprise IT** – ensure alignment when projects involve both Enterprise IT and ICS

- **Safety, Health & Environment** – provide key guidance to ensure alignment and compliance with safety, health and environmental requirements.

In addition, business / operational risk managers, business continuity and emergency planning, telecommunications and physical security functions may also need to be represented. Membership of the governance group can either be included in the core roles of an individual or if more suited to the business, the role may be independently represented.

2.2 Define roles and responsibilities

The precise way responsibilities are spread across the group will vary according to the organisation, and will take into account factors such as the industry, resources available, the chosen governance structure, and geography.

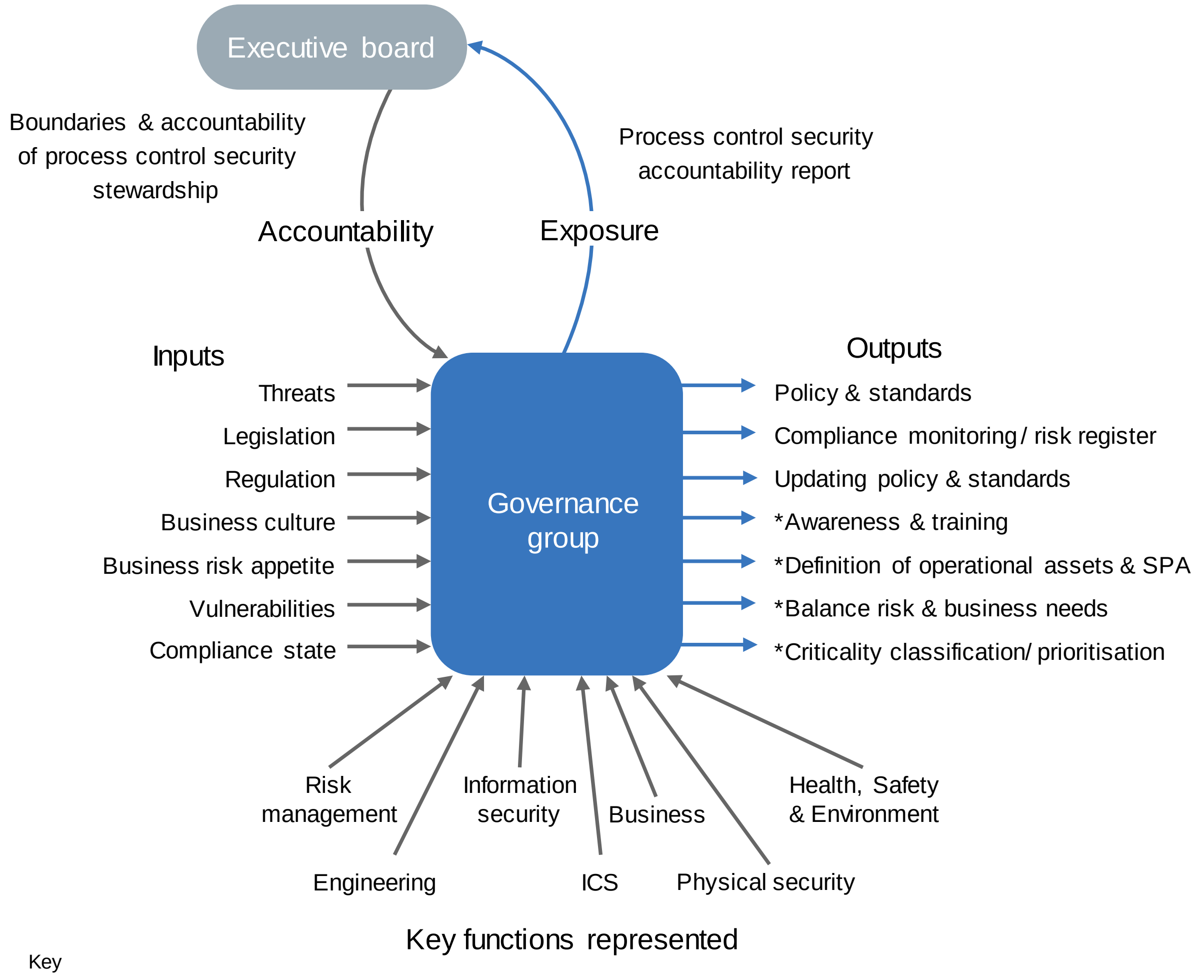
However, there are some responsibilities that generally should be part of the governance of ICS security. These are to:

- Balance business needs with the costs of mitigation measures or determine the processes and limits by which this is done
- Build safety, health and environmental requirements into ICS security
- Consider legal requirements (e.g. Data Protection Act, sector specific or national regulations)
- Consider HR implications of ICS security
- Manage the ICS awareness and communication plan
- Monitor and report ICS security status to the board
- Define appropriate reporting and escalation channels for all issues of security and link to incident response process
- Engage design authorities
- Set operational scope and boundaries
- Define roles, responsibilities and accountabilities for ICS security across the organisation
- Maintain a register of ICS projects (ensuring appropriate security to prevent unauthorised access to project information)
- Maintain ownership of the corporate risk register related to ICS security risk register
- Own and maintain the ICS security strategy
- Obtain funding for any centralised activities
- Own any centralised ICS security programme and monitor decentralised activities
- Create and maintain an inventory (including version and patch details) of the ICS for a site / location, with identified system owners.

The accountability for ICS security may be delegated by the governance group either directly to another group or by creating a number of reporting levels. The approach will depend on the organisation, its size, culture, existing reporting structure, etc. Organisations that rely very heavily on ICS or that would suffer significant business impact if ICS were lost are more likely to require a governance group that is very closely associated with the executive board.

A governance group with specific delegated accountability will need to provide a clear indication of the organisation’s 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 an ICS incident is clearly communicated. This ensures that any significant impact on the business is understood and discussed at the appropriate level and action can be taken. It is also very important that the governance group clearly understands the boundaries of their accountability. Figure 3 provides an overview of the governance group accountabilities and activities.

Figure 3 – Governance group considerations


Executive board
Boundaries & accountability of process control security stewardship
Process control security accountability report
Accountability
Exposure
Inputs
Threats
Legislation
Regulation
Business culture
Business risk appetite
Vulnerabilities
Compliance state
Governance group
Outputs
Policy & standards
Compliance monitoring/ risk register
Updating policy & standards
*Awareness & training
*Definition of operational assets & SPA
*Balance risk & business needs
*Criticality classification/ prioritisation
Risk management
Information security
Business
Health, Safety & Environment
Engineering
ICS
Physical security
Key functions represented

Key
*Indicates the topic is covered in more detail in other framework themes
SPA: Single Point of Accountability

The amount of time spent on governance group duties depends on the magnitude of the risk and what existing governance structures are already in place. So in some cases being part of the ICS governance group may be a part-time role.

When allocating security responsibilities across the organisation, the following areas should be addressed:

- **Strategic** – setting the ICS security strategy, initiating the ICS security programme and monitoring the ICS security risks and the effectiveness of the strategy
- **Tactical** – implementing the ICS security programme, developing the supporting policies and standards, providing ICS security awareness and training advice, monitoring risk and compliance, and setting and approving budgets
- **Operational** – operating and following the policies and standards, having a specialised ICS Security Response Team which monitors, analyses and responds to alerts, events and incidents, and to risk exposure.

3 DEVELOP AND IMPLEMENT THE SECURITY STRATEGY

In ICS environments governance structures are unlikely to be put in place until it is recognised that there is a risk to be addressed. So the process needs to start by establishing what risks exists followed by establishing the necessary governance structures. This should be followed by a risk assessment and a definition of the risk appetite which then should inform the strategy.

The ICS security strategy should define the objectives and these should then be supported by policies and standards. The policies set out the areas where actions should take place and standards provide a consistent organisational interpretation of how to achieve the desired goals of the defined policy. They also provide a set of repeatable building blocks that define the creation, operation, maintenance and removal of ICS components.

These mechanisms allow an organisation to communicate the desired level of ICS security protection and how this should be achieved.

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

- Define a strategy that aligns with the business and operational needs and that sets the objectives for ICS Security and the actions to reach those
- Build the business case to support the ICS security programme
- Define, document, disseminate and manage under change control, formal policy and standards for ICS security
- Ensure that the policy and standards accurately reflect the organisational requirements and support business requirements
- Ensure policy and standards are agreed by all relevant parties.

3.1 Establish the strategy

Using the diagnosis of the situation gained through the assessment of the business risks, the governance group is then responsible for setting the guiding policy for ICS security. This guiding policy reflects the risk appetite of the organisation, and the objectives of the security programme, these are usually designed to prevent risks that could affect the organisation's strategic objectives. The security programme constitutes the action plan or roadmap to achieve those objectives.

Once the strategy has been established, a security programme should be developed to support implementation. When defining the security programme, the following key elements may be included:

Business case

It may be necessary to construct a business case in order to secure funding for ICS security improvements. This business case should clearly articulate the current risks and the need for security improvements. The output from SICS Framework element "Manage the business risk" may be useful in constructing this business case. The case should also clearly show how the proposed investments would change the business risk profile for the ICS and should clearly articulate the residual risk. The key parts of the business case are the:

- Overview of the business risk appetite and profile (including the potential threats, impacts and vulnerabilities)
- Benefits of improving ICS security including the improved risk profile after improvements (i.e. the business benefit)
- Requirements for a security programme, key activities, resources and costs.

It may be necessary to develop a business case at different levels within an organisation or construct a local business case for improvements to a specific site or ICS. In a large organisation, there may need to be an overarching business case for the entire organisation. A key advantage of doing this is that work carried out centrally will also support individual site teams in their activities and reduce the total effort an organisation will need to mobilise the security improvement programme.

Further guidance on developing a detailed business case for security can be found in the NIST 'Guide to Industrial Control Systems (ICS) Security[1].

Phased approach

A programme has an increased chance of success if it adopts a phased approach rather than addressing all the subjects at once because it gives:

- Better control over a more focused set of activities
- Measurable intermediate milestones to validate that objectives are being achieved
- The opportunity to use pilots and prototypes to test the validity of new solutions before rolling them out extensively.

Management of organisational change

The implementation of a new security programme constitutes a significant change that spans the organisation. To maximise the chance of its success, the following issues should be addressed:

- The need for communication with the different stakeholders about the reasons for change and the benefits of the programme
- The need for training, resourcing and development of the necessary supporting skills
- Benefits management to ensure the expected outcomes are realised and measured.

[1] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3.2 Develop supporting policies and standards

The creation of ICS security policy and standards can be handled either as an entirely unique entity or combined with existing IT security or engineering standards. Both approaches can work equally well, as long as they are able to accurately represent the quality and detail required to protect ICS to the stated business requirements.

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

- ICS is business critical or has an impact on safety
- There are available resources with strong ICS skills in the organisation
- The current security policy and standards are not adequate to cover the ICS
- There are other cultural or historical reasons to support this approach.

Alternatively, it may be appropriate to combine ICS security policies and standards with existing security policies and standards, or add an ICS security section to the standards documents if:

- ICS is business critical and closely integrated into key business processes
- There is good engagement between security, ICS and IT support
- There is good alignment with enterprise security controls and the controls required to secure ICS
- There are limited ICS resources and capabilities and so these issues would otherwise not be addressed.

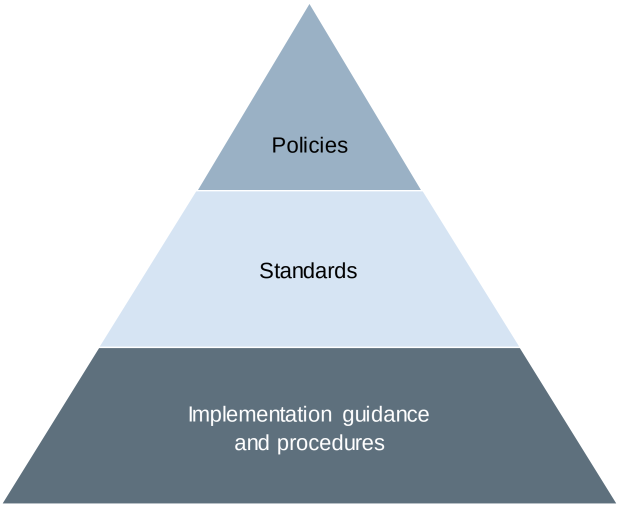
Care must be taken if combining the policies and standards as ownership, agreed quality and security principles need to be clearly defined to ensure both IT and ICS security goals are met in an effective way. This is seldom a simple process as the operational requirements of IT security and ICS security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

To deal with these complexities, a dedicated architecture and standards working group could be formed to report into the governance board, ensuring that both IT and ICS groups are involved in defining policy, standards and implementation guidance.

Where ICS standards already exist they will require regular reviews to ensure they remain consistent with industry standards and reflect changes to the risk appetite of an organisation. Most organisations have a procedure for updating internal standards and it is recommended that ICS standards are included in this process.

Figure 4 shows how the detail and number of documents varies between policy, standard and guidance. The higher up the triangle less detail, fewer documents and less frequent changes are needed. The opposite applies lower down the triangle with implementation guidance documents being the most detailed and most likely to need updating regularly.

Figure 4 – Relationship of policy, standards and guidance documents



3.2.1 Write a policy

ICS 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 its own without associated standards would be too high level to communicate what needs to be done. It is the standards (and related implementation guidance) that provide the information needed to implement the policy goals to the required level of consistency.

Policy should provide specific statements of principles or guiding actions that demonstrate a clear commitment by the organisation; statement of values or intent that provides a basis for consistent decision-making and resource allocation; and definite methods 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
- Set out statements of what and / or why instead of how
- Address strategic and major operational issues.

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

- **Policy statement of intent** – the controls that need to be in place, to this level of security
- **Who and what the policy applies** – the scope or boundaries of the policy
- **Who owns the policy** – who will publish and update it
- **Policy update triggers** – when should the policy be reviewed
- **Exception criteria and process** – when is the policy not applicable, and by what processes can exceptions be granted.

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 ICS security policy. It would be a mistake to write an ICS security policy in isolation without considering the business, operational, or financial impact of the statements. Such documents are very unlikely to be endorsed and accepted by the business and will result in loss of credibility and a waste of effort.

As well as being aware of genuine operational requirements, when writing an ICS security policy it is important to check that they align with:

- Business strategy
- IT strategy and policies
- Safety, health and environmental policy
- Security policies of the organisation
- Use of existing / established terminology
- The level and audience of other policies.

The governance group is accountable for setting ICS security policy and ensuring it is signed-off at whatever level the organisation requires.

3.2.2 Create standards

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

- Are narrow in application
- Are prone to change
- Are often detailed
- May include some technical detail
- Include statements of 'how,' 'when' and sometimes 'who'
- Describe related processes.

ICS security standards documents provide a common approach to be followed throughout the organisation. They enable quicker delivery, at a known consistency that generally reduces the complexity of the task. Standards provide a codified repeatable approach that reduces re-work 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. It is important that standards are concise in order to ensure that those reading them have a common interpretation.

Standards are likely to be drafted with the help of specialist internal standards 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. They are strongly influenced by relevant legislation and regulation (Health and Safety, Data Protection, environmental), existing industry standards, the technology available and future business or industry requirements.

When considering what to include in a standard, the following would be expected as a minimum:

- **A policy statement to which the standard applies**
- **Description of the intended audience or readership** – the relevant roles and hence the level of detail
- **Definition and application of the standard** – what is it, how is it applied in terms of people, processes and technology
- **Outline of who and what the standard applies to** – the scope or boundaries of the standards
- **Outline of who owns the standard** – who will publish and update it
- **Arrangements for updating of the standard** – when the standard should be reviewed
- **Mandatory requirements** – what must staff work to
- **Exception criteria** – when the standard is not adhered to.

Due to the detail involved in standards and the frequency of the changes, it is common for them to be signed off only at the governance group level, or even a designated technical sub-committee. This does not mean that the process is any less stringent than policy definition, but it does reflect that the detail will only be understood by a limited group of reviewers.

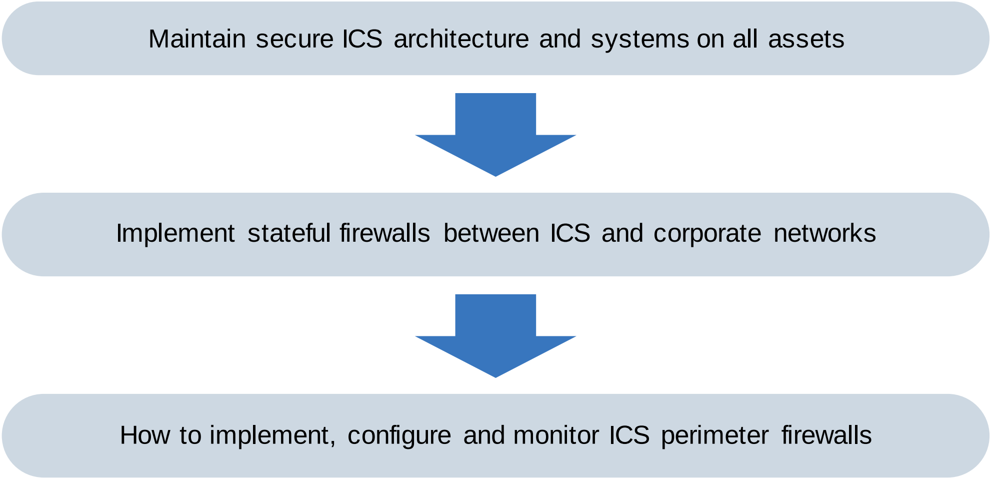
3.2.3 Implementation guidance and procedures

There is a third group of documents that are often used to support standards, usually referred to as ‘implementation guidance and procedures’ 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. This avoids creating 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.

As part of the guidance and procedures, there should be a template security management plan which is based on the ICS security framework (policy, standards and guidance). When populated it provides a plan for the implementation, operation and improvement of ICS security for a specific system, site or asset based on the risk assessment for which it is being applied.

The level at which these documents will need sign-off will vary between organisations and it will be for the governance group to decide the appropriate level. Figure 5 illustrates a flow from a policy to standards and guidance.

Figure 5 – Example of the relationship between a policy, standards and guidance documents



Maintain secure ICS architecture and systems on all assets

Implement stateful firewalls between ICS and corporate networks

How to implement, configure and monitor ICS perimeter firewalls

3.3 Reference standards and guidance

There are a number of sources of guidance to support the development of ICS security standards and which will help define the required expectations to achieve the desired level of security. The main sources are vendors, government institutions and industry regulators and some of the key providers are listed below:

- CPNI - Centre for the Protection of National Infrastructure
- CPNI Best Practice Guide - Firewall Deployment for SCADA and ICS 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 - Personnel Security Measures
- CESG Policy Portfolio
- IEC – International Electrotechnical Commission
- IEC 62443-2-1 Industrial communication networks - Network and system security Part 2-1: Establishing an industrial automation and control system security program (formerly ISA99)

- IEC 62443-3-3 Industrial communication networks - Network and system security Part 3-3: System security requirements and security levels
- IEEE – Institution of Electrical and Electronics Engineers
- ISO 27000 series - International Specification for Information Security Management Systems
- Industry – specific guidance from organisations such as API, NERC, AGA, OLF, CIGRE
- Vendor specific guidance
- US DHS - Cyber Security Procurement Language for Control Systems
- US DHS - Catalog of Control System Security Requirements
- US NERC - Critical Infrastructure Protection (CIP)
- US NIST - Cyber Security Framework
- US NIST - SP800-82 Guide to Industrial Control (ICS) Systems.

It is important to use this material as a starting point to capture the critical requirements but not simply write a wish list based on a specific supplier or piece of hardware / software or copy industry best practice. Organisations need to create their own specific set of documents based on their business requirements, characteristics and culture. It is this tailored application of good practice principles to an identified threat in the organisation that will best help mitigate the problem, in the line with the organisation's risk appetite.

4 MONITOR THE RISKS AND ENSURE COMPLIANCE

Ensuring compliance with policy and standards is vital to provide assurance that the appropriate actions are being taken to meet the right quality requirements. Monitoring the risks allows the organisation to verify that the desired risk mitigation is being achieved. This provides assurance that ICS are protected to the agreed level of business risk, avoids wasteful duplication of effort and ensures that consistent solutions are being deployed across the organisation.

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

- Ensure the security strategy remains appropriate through monitoring the risks
- Implement an assurance programme to ensure that the ICS security policy and standards are complied with on a continuous basis.

4.1 Monitor the risks

Monitoring risks effectively is fundamental to ensuring that security is maintained at the right level and organisations can improve security by measuring the efficiency of their risk reduction strategy.

Risk monitoring is performed through:

- Undertaking ongoing assessment of business risk (see SICS Framework element 'Manage the business risk')
- Learning from incidents through the identification of root causes and potential associated improvement actions (see SICS Framework element 'Manage the business risk')
- Maintaining an early warning system by keeping a close watch on the status of threats and emerging vulnerabilities (see SICS Framework element 'Manage vulnerabilities')
- Exchanging information on incidents and threats with industry peer groups
- Monitoring changes in the legal and regulatory environment
- Assessing the impact of changes in the infrastructure for example triggered by new projects or the decommissioning of old systems (see SICS Framework element 'Manage the Industrial Control Systems lifecycle')
- Detection of areas of non-compliance and the associated risks (see the section below for detail).

A good way to formalise the monitoring of risks is through the implementation of security Key Performance Indicators (KPIs) that evaluate the performance of the strategy and measure potential emerging risks.

Establishing KPIs is achieved by:

- Identifying the key objectives, benefits and parameters that are to be monitored
- Defining the associated KPI for each objective
- Measuring, reporting and analysing the KPIs on a regular basis.

The range of KPIs that an organisation chooses to monitor at a given point in time can vary depending on current priorities or if benefits have already been realised and do not require further monitoring.

4.2 Ensure compliance

There are a number of approaches to ensuring conformity with policy and standards and compliance with external standards. These approaches should be tailored to match the organisation’s culture, capabilities, and existing initiatives. Some organisations feel happier with detailed information about which areas are compliant and which are not. Others prefer to receive exception reports indicating where non-compliance has been recorded. In order to work out the best approach, three key points should be addressed:

- What information is required, in what detail and when and to whom will it be reported?
- 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?

4.2.1 Identify what information is required

Organisations need to decide what level of information is manageable while still providing enough detail to be of value in decision making. This will vary but should reflect the fact that too much information can be as bad as not enough and if people feel that the information they are submitting is not being read then the quality will soon decline. Equally if someone is trying to flag a problem with a policy or standard but does not have the scope to do so, then they may adopt their own practices and just pay lip-service to the organisation’s requirements, undermining compliance.

While approaches will vary there is some key information necessary for effective compliance reporting:

- Identification of the person responsible for implementing reporting and person responsible for implementation of resulting actions
- A single point of accountability for compliance assurance
- Relevant deviation from policy or standards
- Evidence to support the finding of the assessment
- Business impact implications
- Date of planned resolution
- Relevant circumstances (e.g. reasons for non-compliance).
- Update frequency as determined by the governance group based on time or significant changes.

4.2.2 Collect the information

Securing the capability and resources to ensure compliance can be achieved in a number of ways. An organisation can opt to resource the activity in-house through self-assessment, peer review or an internal audit department though this will depend on the quantity, quality and frequency of compliance monitoring. This approach has many benefits including creating a greater sense of ownership of any issues or excellent performance, but it can take up valuable time of specialist internal resources. Another approach is to outsource the task to a third party specialising in ICS security. This option provides more objective results and there is less chance of problems being hidden but it is likely to cost more. It also raises 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 non-compliance may have a regulatory impact and this needs to be identified.

Where external compliance is required, the use of independent third parties might be mandated but this is not always the case and it might still be possible to use more informal approaches like self-assessments.

Summary of options:

- **Self-assessment** – an assessment that is conducted by the accountable department
- **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 an ICS security specialist from an internal or external team
- **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 ICS Security'[2].

4.2.3 Assess the impact of non-compliance

The final key consideration is what, if any, additional business risk is posed, if a significant deviation from policy or standards has been reported.

There are many areas that can be assessed in relation to compliance but a balance needs to be struck between the effort required and the benefits that could be achieved. It is important to capture sufficient information about non-compliance to make an informed decision about the potential threat to feed into SICS Framework element 'Manage the business risk'. This means asking:

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

4.2.4 Monitor compliance

There are three areas that should always be carefully monitored: segregation, systems monitoring and detection and patching. For most organisations these present the largest threat to the business.

There are a number of activities that can be undertaken to monitor compliance. Typical activities include:

- Using automated tools or checklists based on the applicable (technical) standards, e.g. to check that deployed configuration or installed software is compliant
- Analysis of logs to look for compliance of operations / network traffic
- 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 other 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 ICS.

[2] http://csrc.nist.gov/publications/PubsSPs.html

5 MAINTAIN AND IMPROVE SECURITY

ICS technology, legislation, regulation and threats are continually changing and evolving. Therefore it is essential that security is maintained and improved continuously to respond effectively to these changes.

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

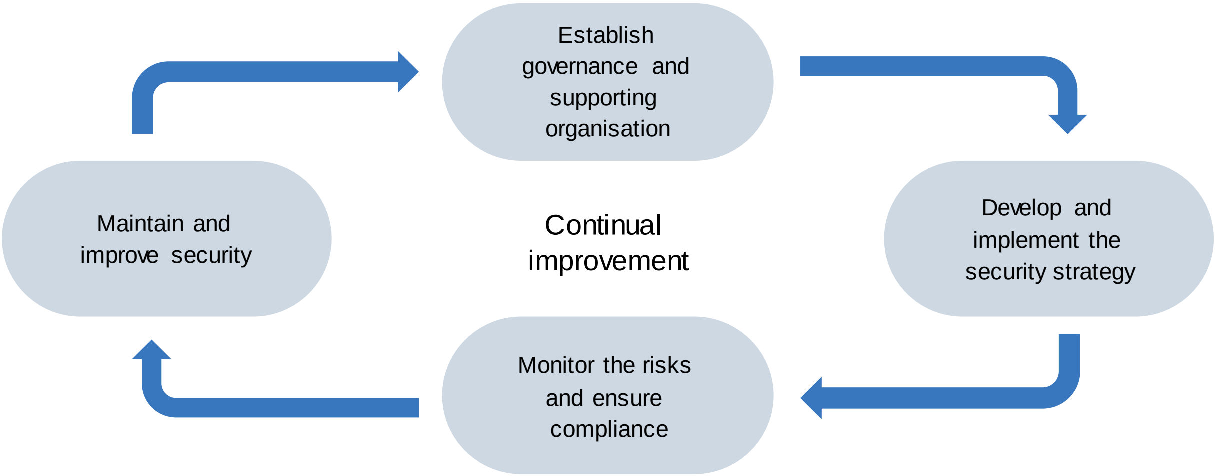
- Establish an ongoing programme to ensure that ICS security is maintained regularly and improved continually. This could take the form of annual reviews or a review prompted by changes:
  - In current threats
  - In legal and regulatory requirements
  - In the business requirements
  - In operational requirements
  - To operational equipment
  - To the strategy or long term plan.

5.1 Implement a continual improvement capability

The threat profile of an organisation is not static. As shown as shown in Figure 6, an organisation's ability to make continual improvements in security is a key factor in managing its risk successfully and sustainably.

"SECURITY IS NOT A DESTINATION, IT IS A JOURNEY"

Figure 6 – 'Establish ongoing governance' continual improvement cycle


Establish governance and supporting organisation
Develop and implement the security strategy
Monitor the risks and ensure compliance
Maintain and improve security
Continual improvement

5.2 Maintain security and updating policies and standards

There needs to be a balance between constantly adapting the strategy and ensuring that it is always optimal and between updating documents and ensuring that the documents are relevant. This makes it important that the structure and detail covered in policies and standards are carefully written. By investing time in constructing good quality, flexible, but unambiguous policies and standards an organisation should be able to amend only specific sections, rather than having to completely rewrite them.

Another key principle when writing policy and standards is to consider what the expected lifespan will be before it will need to be updated. While this kind of scheduling cannot accommodate unexpected threats or regulatory changes, it should be able to factor in anticipated 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 provide review and comment and the impacts on ICS 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 to involve can vary however the following categories can be used:

- 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 disseminated appropriately even if the policy or standards updates have a limited stakeholder sign-off.

The optimum position within an organisation would be to build the updating of policy and standards into 'business as usual' procedures such as change management.

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

6 CASE STUDY: LECTRIC DISTRIBUTION

6.1 Lectric Distribution: summary of previous developments

In the face of security incidents the Plant Manager of Lectric Distribution commissioned a risk assessment to evaluate the state of security of the ICS of this electricity distribution network operator.

The Director of Enterprise Risk integrated the assessment results into the company risk register and put ICS security on the agenda of the next board meeting to which the Head of ICS was invited to attend.

6.2 Lectric Distribution: on the way towards a new security strategy and governance framework

During the board meeting, many senior managers become aware of the exposure of their ICS and that the lack of security could jeopardise the business objectives and even the company itself.

As a result the board decided to create a task force to establish a strategy to address the risks. The board mandate the Plant Manager to create this task force.

She decided to restrict the size of the task force in order to keep an agile and focused group but she made sure that all the skills she needed were represented. The members were:

- Plant Manager in her role of Task Force leader and for her ICS expertise
- Information Systems security manager for his expertise in cyber security
- The Head of risk and compliance for his experience in deploying governance frameworks and risk management
- The deputy director of operations for his understanding of the business needs and constraints.

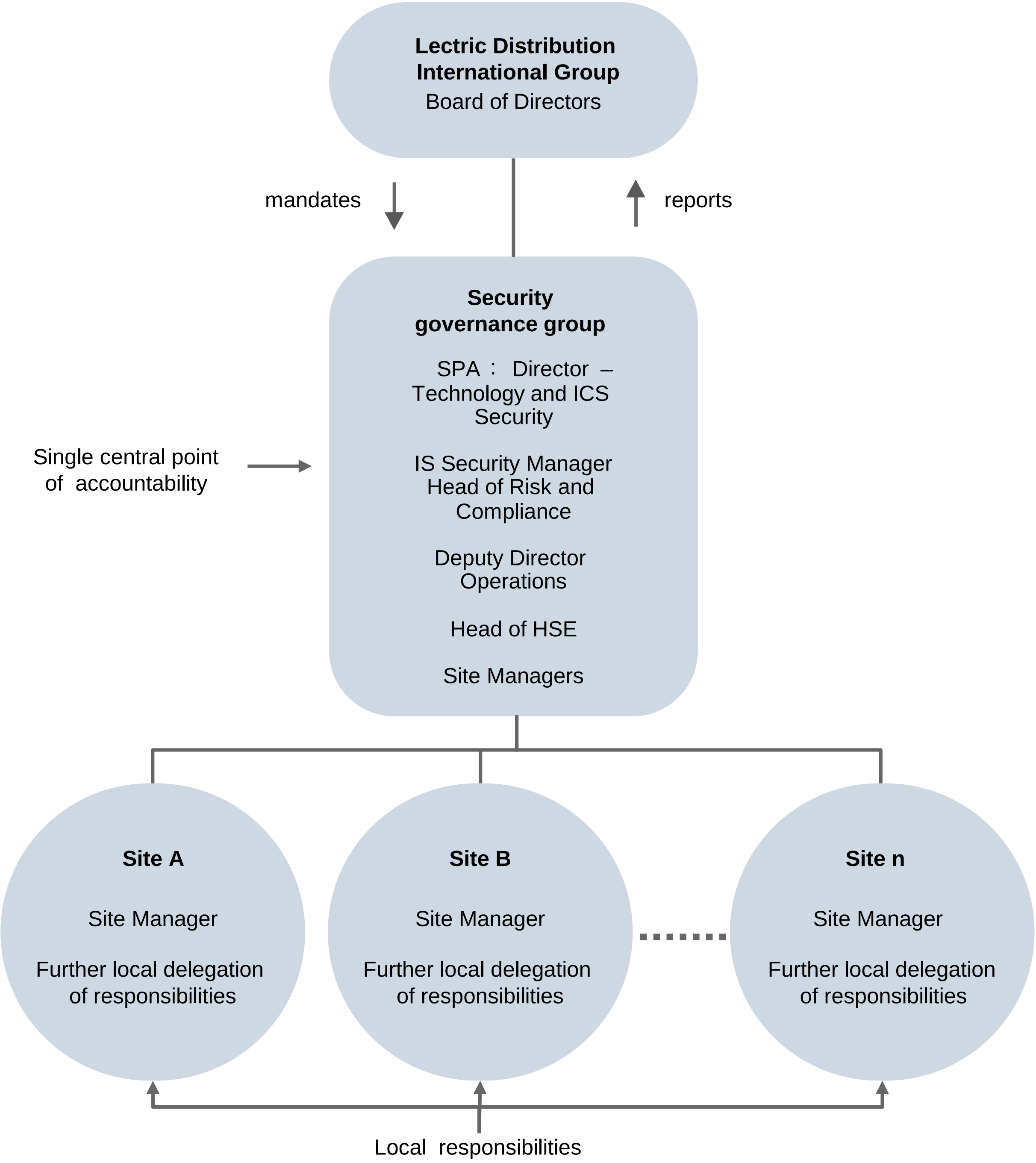
They submitted the following strategy for the board's approval, it was based on:

- Short term quick wins through:
  - Creation of an incident response team to address the risk of an incident resulting from the current poor state of ICS security
  - Engagement of all ongoing technology projects to ensure that newly commissioned infrastructure would embed a minimum set of security features.
- A longer term improvement strategy through:
  - A company-wide initiative for raising the level of skills required to implement the security programme
  - Selection of a pilot site for evaluating potential options for implementation of the strategy
  - Establishment of a company-wide policy and set of standards to roll out the agreed strategy to all sites

The board approved the strategy and designated a security governance group to drive this strategy. It was constituted of:

- The original task force members
- The Head of HSE (Heath, Safety and Environmental), as it became clear that cyber security incidents could also impact this area
- The site managers who were made responsible for the implementation of the security strategy on their respective sites
- The Plant Manager was promoted to Director level in charge of Technology and ICS Security. She was mandated as the Single Point of Accountability for ICS security for the whole organisation.

Figure 7 - Lectric Distribution - Security governance organisation


Lectric Distribution International Group
Board of Directors
mandates
reports
Security governance group
SPA : Director – Technology and ICS Security
IS Security Manager
Head of Risk and Compliance
Deputy Director Operations
Head of HSE
Site Managers
Single central point of accountability
Site A
Site Manager
Further local delegation of responsibilities
Site B
Site Manager
Further local delegation of responsibilities
Site n
Site Manager
Further local delegation of responsibilities
Local responsibilities

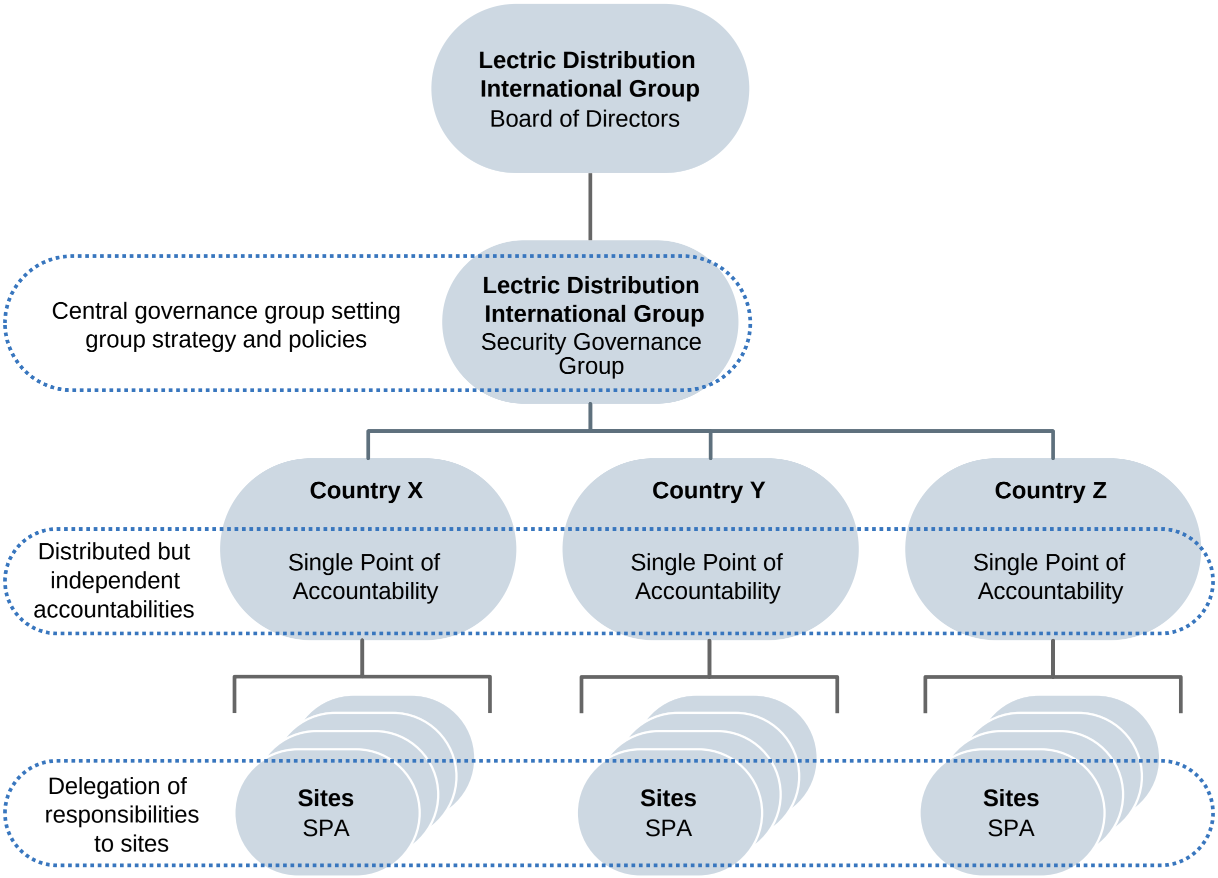
6.3 Fast Forward: Three years later: Lectric Distribution International Group

During the past three years Lectric Distribution has been busy implementing security measures under the direction of their Security Governance Group. It has not prevented the organisation from suffering several moderate incidents that have highlighted some unidentified weaknesses. But the decision to invest in Incident Response Capabilities had allowed Lectric Distribution to limit the impact of those incidents and after structured lessons learnt exercises they have managed to improve the infrastructure to avoid those incidents reoccurring.

In the meantime, Lectric Distribution acquired several businesses in line with a new overseas expansion strategy, this triggered:

- **A change of governance model**. It was decided to adopt a model which devolved accountability to reflect the increase in size and the relative geographical separation of the different national businesses. This resulted in breaking down the SPA role to one per country and the retention of a central governance function responsible for setting the policies and strategies.
- **A move to a more flexible strategy** with a minimum baseline mandated at Group level and local variations (i.e. additional measures) to reflect the varying local contexts in the different countries of operations (e.g. different threat environment, different legacy architecture choices).

Figure 8 – Lectric Distribution International Group - Security governance organisation


Lectric Distribution International Group
Board of Directors
Central governance group setting group strategy and policies
Lectric Distribution International Group
Security Governance Group
Country X
Country Y
Country Z
Distributed but independent accountabilities
Single Point of Accountability
Single Point of Accountability
Single Point of Accountability
Delegation of responsibilities to sites
Sites
SPA
Sites
SPA
Sites
SPA

A TERMINOLOGY RELEVANT TO THIS GUIDE

Accountability	Assigned to someone who is required or expected to justify actions or decisions. Accountability cannot be shared.
Governance	The structure and processes by which organisations are directed and controlled.
Programme	A set of related measures or activities with a particular long-term aim.
Responsibility	Having an obligation to do something as part of a role. Responsibility can be shared.
Strategy	A plan of action designed to achieve a long-term or overall aim.

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/