Protective Security Management Systems (PSeMS)

Guidance, Checklist, and Case Studies

mcclumpha
associates ltd

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. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in information, including all documents and their references, in this document or from any person acting, omitting to act or refraining from acting upon, otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

About McClumpha Associates Ltd

McClumpha Associates Ltd is a specialist SME company with extensive expertise in critical national infrastructure, transport, and civil aviation security systems. They have developed best practice guidance for governments, Crown corporations, security regulators and legislators, and the security industry to support operational effectiveness, performance efficiency, and workforce optimisation. This has included guidance on personnel recruitment and selection, training system design, operational performance management, security officer motivation, and Security Management Systems (SeMS).

Guidance Material

Checklist

Case Studies

Executive Summary

The target audience for this guidance is senior management and security representatives in all Critical National Infrastructure (CNI) sectors.

This guidance material is an introduction to Protective Security Management Systems (PSeMS) and covers background and information on PSeMS, a Checklist to help assess the maturity of an organisations security assurance, and a number of Case Studies that describe barriers, benefits and outcomes from implementation of PSeMS.

This guidance is intended to support existing initiatives and further raise awareness for:

• Organisations that are planning on adopting PSeMS, or are less mature with PSeMS and its benefits, can gain a comprehensive introduction to PSeMS and better understand how PSeMS can enhance their assurance of organisational security.

• Organisations that are familiar with PSeMS but wish to increase the level of PSeMS capability and want to understand potential gaps and weaknesses in their system and/or learn from PSeMS implementations in other CNI sectors.

• Organisations that class themselves as mature PSeMS organisations and can validate their understanding of PSeMS through this guidance material and can provide feedback and resources to enhance this guidance for the future benefit of the wider CNI community.

It is acknowledged that information resources on PSeMS in the form of international documents, ISO reference standards, regulatory frameworks, and accreditation schemes are available. Furthermore, it is expected that some CNI organisations may already be familiar with PSeMS as part of a regulated system or through an ISO standard.

What this section contains

The purpose of this section is to describe:

• the background to PSeMS;

• what a Protective Security Management System is and its major components;

• why an organisation should implement or enhance PSeMS;

• how an organisation sets out the framework for using PSeMS;

• variations of PSeMS across the CNI;

• what PSeMS is not;

• and finally a list of additional resources.

This document covers the the current range of PSeMS guidance products shown in figure 1, below.

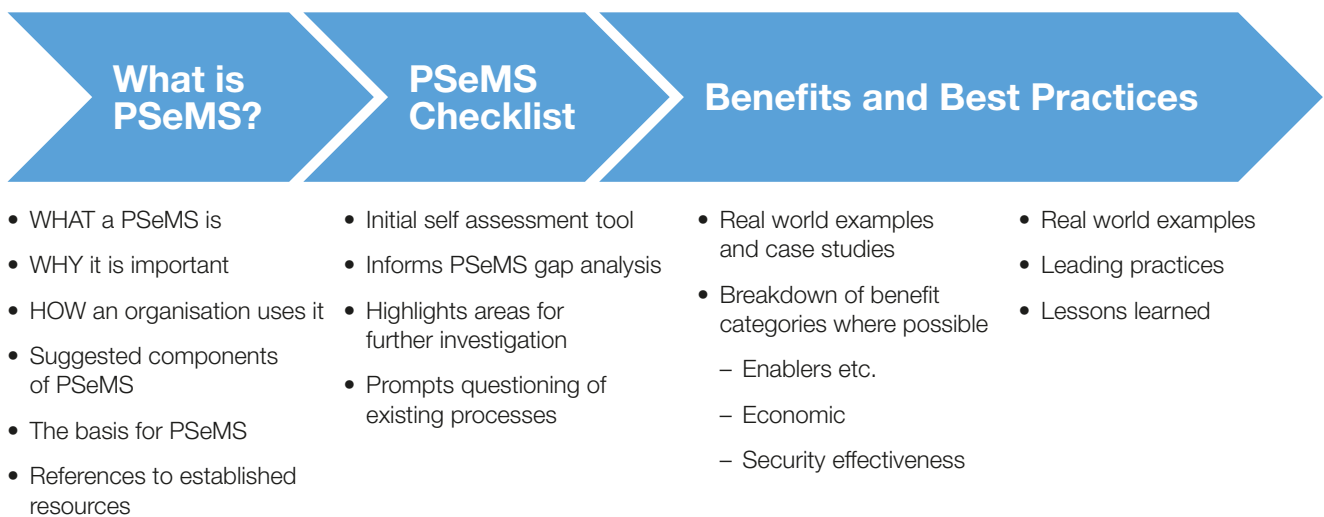| What is PSeMS?	PSeMS Checklist	Benefits and Best Practices	
• WHAT a PSeMS is	• Initial self assessment tool	• Real world examples and case studies	• Real world examples
• WHY it is important	• Informs PSeMS gap analysis	• Breakdown of benefit categories where possible	• Leading practices
• HOW an organisation uses it	• Highlights areas for further investigation	– Enablers etc.	• Lessons learned
• Suggested components of PSeMS	• Prompts questioning of existing processes	– Economic	
• The basis for PSeMS		– Security effectiveness	
• References to established resources			

Figure 1: Current CPNI PSeMS guidance materials

Background for PSeMS

PSeMS is an emerging management system approach and is derived from principles established under Quality Management Systems (QMS) and Safety Management Systems (SMS).

QMS originally started as a means to provide an organisation with a focus on savings and efficiency, and gaining additional revenue through the identification and reduction of errors in operational processes, products, and services offered to customers. The cost incurred by frequent small errors can be seen as minimal but over time will have a significant impact on costs to the business and its overall efficiency.
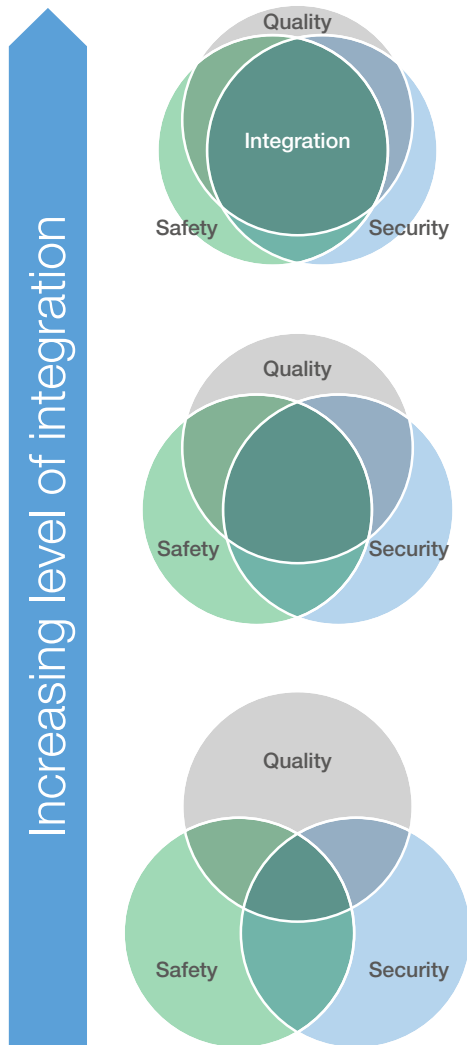
This quality principle resonates with safety and security where a number errors and lapses that may appear inconsequential on their own can, if unchecked, lead to more significant incidents over time.

Lack of compliance, 'cutting corners', skill fade, and failure to report incidents are but a few examples that can contribute to errors where safety and security is concerned.

The discipline created by QMS helps provide assurance to an organisation that all processes are performing to required levels and that new requirements are reflected in changes to processes.

Importantly, PSeMS shares many core principles with Safety and Quality Management Systems and should be integrated with these systems if they are implemented effectively and in use.

For example, a quality management process may already capture risks related to commercial, reputation, and other areas where these risks are made visible to the Board who also agree and set the policy and objectives for the organisation to mitigate those risks. Security should be an inherent part of this process.

This integration can help reduce the time taken to get PSeMS in place and provide a more integrated and cost effective approach when much of the required governance already exists.

What, Why, and How?

What

A PSeMS provides a structured and proactive approach for providing assurance for your organisation's security.

PSeMS

- PSeMS is an assurance system for organisational security

- It provides the necessary organisational structure, accountabilities, policies and procedures to ensure effective oversight

- A PSeMS is an organisation's systematic approach to managing security risks incorporating security management into daily activities
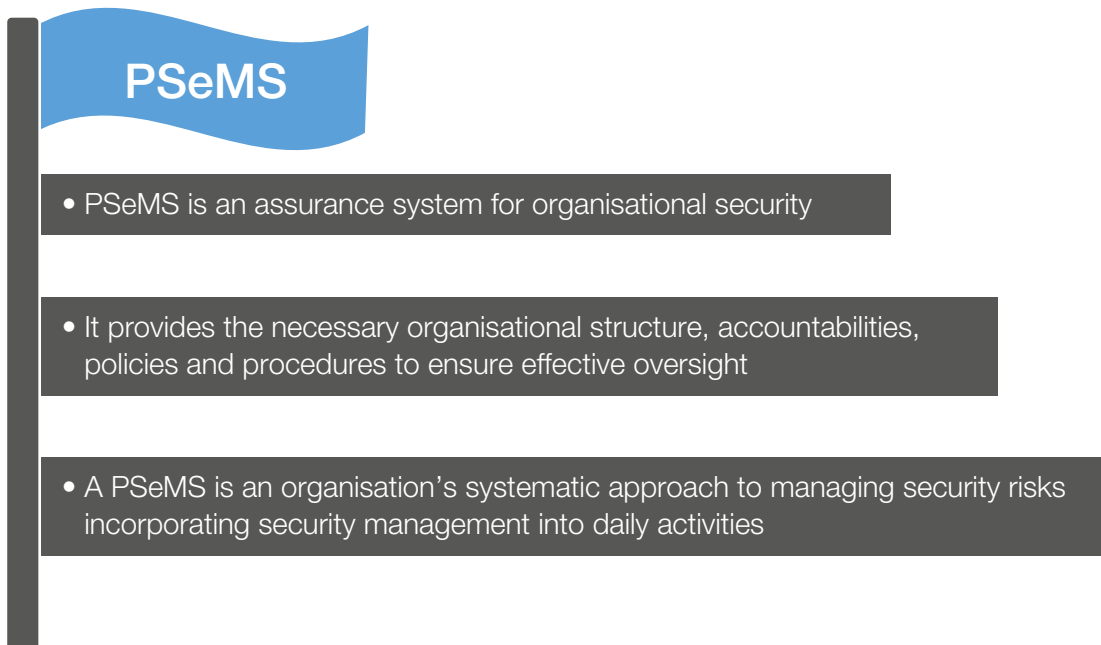
A PSeMS is a formal business practice that is part of the day to day activities of an organisation. It brings together a range of processes including governance, communication, risk management, and performance monitoring as part of daily operation.

The CPNI PSeMS Industry Working Group definition is shown below:

"A framework which helps coordinate processes and procedures covering governance, legal requirements, operating procedures, delivery, monitoring, review, and audit for security"

Suggested components of PSeMS and lifecycle

PSeMS can be best thought of as part of the ongoing life cycle of the organisation. A commonly accepted approach for this cycle is the Plan, Do, Check, Act (PDCA) cycle which is often used in Quality Management Systems.

The four step PDCA is an approach for managing the quality and control of processes, and ensuring a continued route to improvement. Each part of the cycle is explained below.
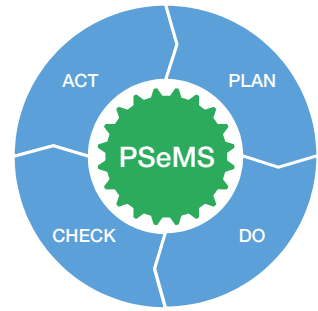
Plan

The organisation reviews it current status and identifies where it needs to be in the future. In order to do this it seeks to understand what needs to be achieved and how, who will be responsible for what, and the associated measures of success. This part of the process includes creating or updating a policy and plans to deliver the aims.

Do

During this phase of the cycle the organisation assesses and manages risks, organises and implements processes to deliver plans by communicating and involving personnel, and provides adequate resources and training.

Check

The organisation makes sure that plans have been implemented successfully and assesses how well risks are being controlled and if organisational aims are being achieved (for example through audit measures). As part of this process the organisation will investigate breaches or gaps in security and ensure corrective action is taken.

Act

The organisation reviews its performance enabling senior management to direct informed changes to policy and plans in response to lessons learned and data collected with respect to specific areas and the overall cycle.

The typical PSeMS components are shown in figure 2, below, and mapped to the PDCA approach. This image describes the flow of core processes moving clockwise starting from Plan through to Act.

The PSeMS components highlighted in this section are those that were given higher priority by the CNI industry stakeholders who helped inform this guidance. However, we recommend that additional resources such as the examples included later in this document are also consulted.
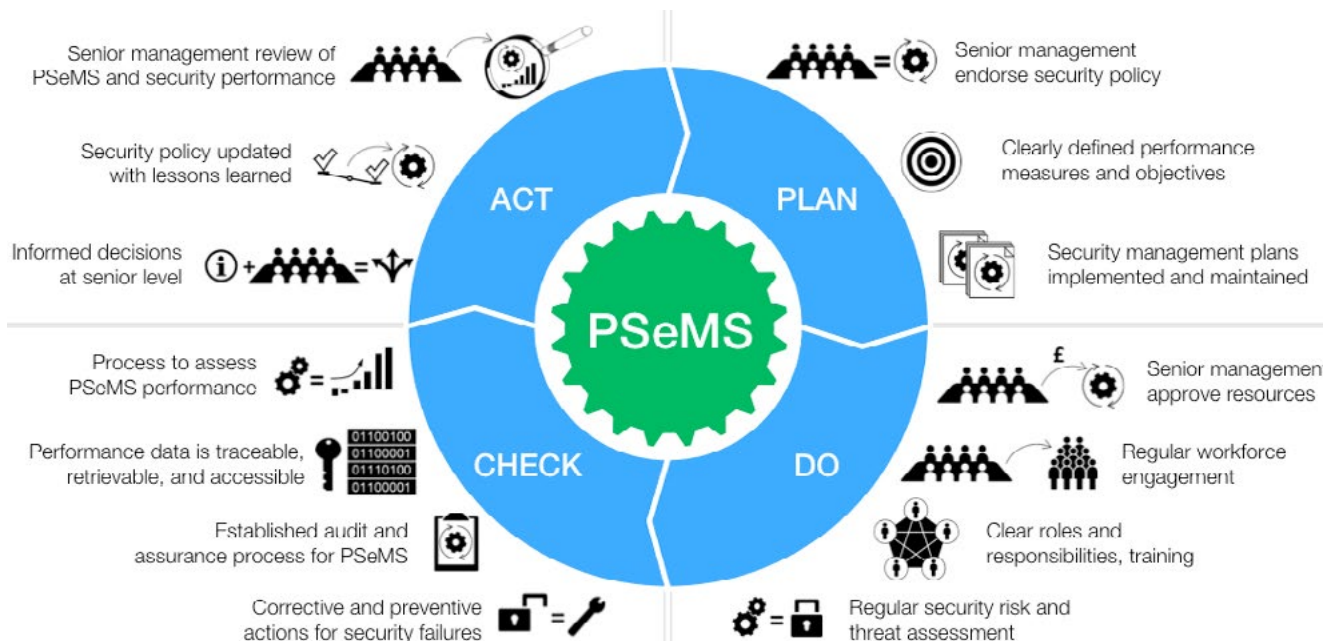

Figure 2: Organisational security assurance through tangible business practices and controls

Each of the PSeMS components under the PDCA approach is explained in figure 3, below.
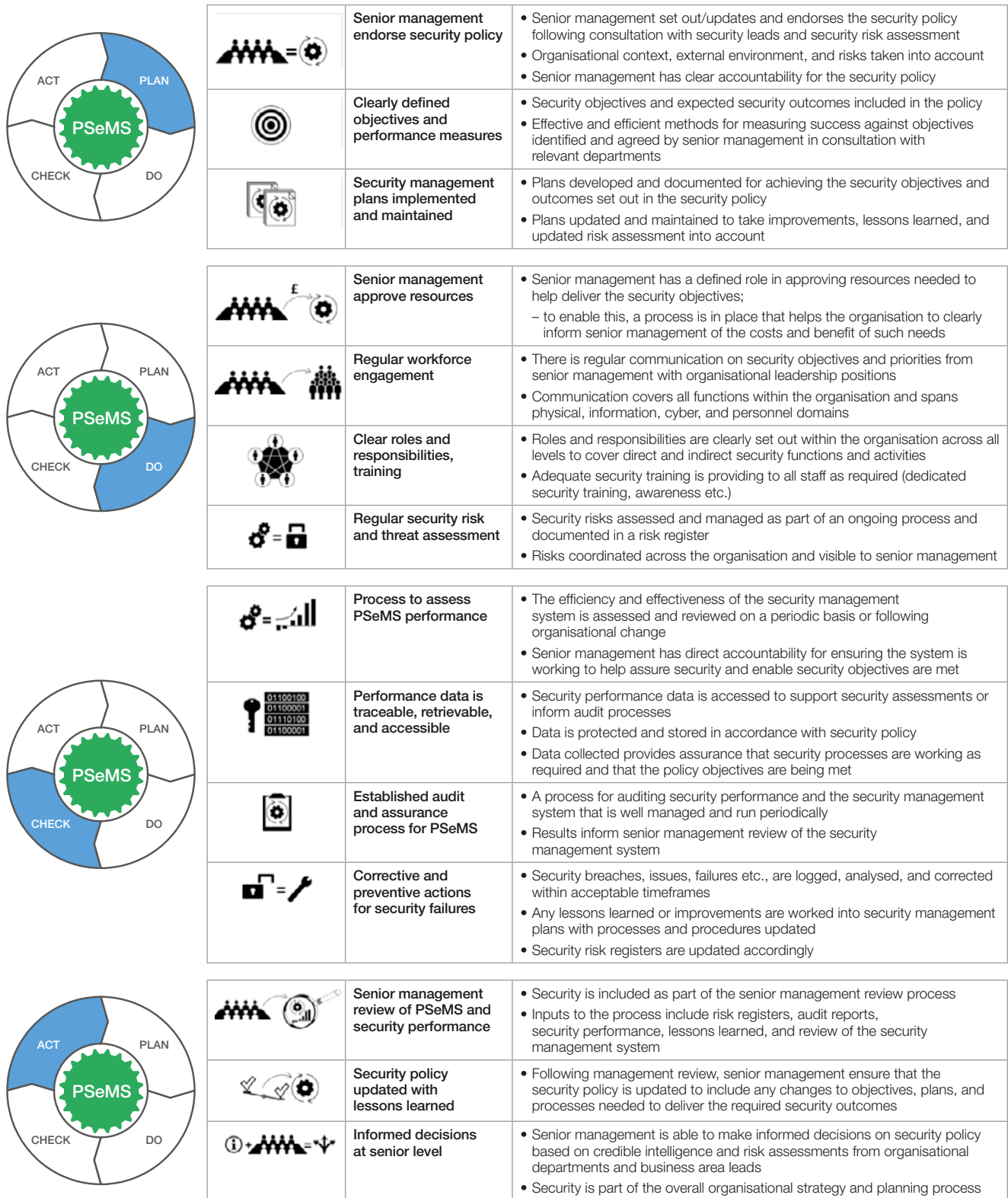
	Component	Description
	Senior management endorse security policy	• Senior management set out/updates and endorses the security policy following consultation with security leads and security risk assessment • Organisational context, external environment, and risks taken into account • Senior management has clear accountability for the security policy
	Clearly defined objectives and performance measures	• Security objectives and expected security outcomes included in the policy • Effective and efficient methods for measuring success against objectives identified and agreed by senior management in consultation with relevant departments
	Security management plans implemented and maintained	• Plans developed and documented for achieving the security objectives and outcomes set out in the security policy • Plans updated and maintained to take improvements, lessons learned, and updated risk assessment into account

	Component	Description
	Senior management approve resources	• Senior management has a defined role in approving resources needed to help deliver the security objectives; – to enable this, a process is in place that helps the organisation to clearly inform senior management of the costs and benefit of such needs
	Regular workforce engagement	• There is regular communication on security objectives and priorities from senior management with organisational leadership positions • Communication covers all functions within the organisation and spans physical, information, cyber, and personnel domains
	Clear roles and responsibilities, training	• Roles and responsibilities are clearly set out within the organisation across all levels to cover direct and indirect security functions and activities • Adequate security training is providing to all staff as required (dedicated security training, awareness etc.)
	Regular security risk and threat assessment	• Security risks assessed and managed as part of an ongoing process and documented in a risk register • Risks coordinated across the organisation and visible to senior management

	Component	Description
	Process to assess PSeMS performance	• The efficiency and effectiveness of the security management system is assessed and reviewed on a periodic basis or following organisational change • Senior management has direct accountability for ensuring the system is working to help assure security and enable security objectives are met
	Performance data is traceable, retrievable, and accessible	• Security performance data is accessed to support security assessments or inform audit processes • Data is protected and stored in accordance with security policy • Data collected provides assurance that security processes are working as required and that the policy objectives are being met
	Established audit and assurance process for PSeMS	• A process for auditing security performance and the security management system that is well managed and run periodically • Results inform senior management review of the security management system
	Corrective and preventive actions for security failures	• Security breaches, issues, failures etc., are logged, analysed, and corrected within acceptable timeframes • Any lessons learned or improvements are worked into security management plans with processes and procedures updated • Security risk registers are updated accordingly

	Component	Description
	Senior management review of PSeMS and security performance	• Security is included as part of the senior management review process • Inputs to the process include risk registers, audit reports, security performance, lessons learned, and review of the security management system
	Security policy updated with lessons learned	• Following management review, senior management ensure that the security policy is updated to include any changes to objectives, plans, and processes needed to deliver the required security outcomes
	Informed decisions at senior level	• Senior management is able to make informed decisions on security policy based on credible intelligence and risk assessments from organisational departments and business area leads • Security is part of the overall organisational strategy and planning process

Figure 3: Typical PSeMS components within PDCA

To better understand the readiness of your organisation in relation to the PSeMS components we suggest you use the CPNI PSeMS checklist (p16).

Application of PSeMS across the security domains

PSeMS principles apply to all applicable security domains such as physical, cyber, and personnel security and it is recommended that it should be integrated across these domains.
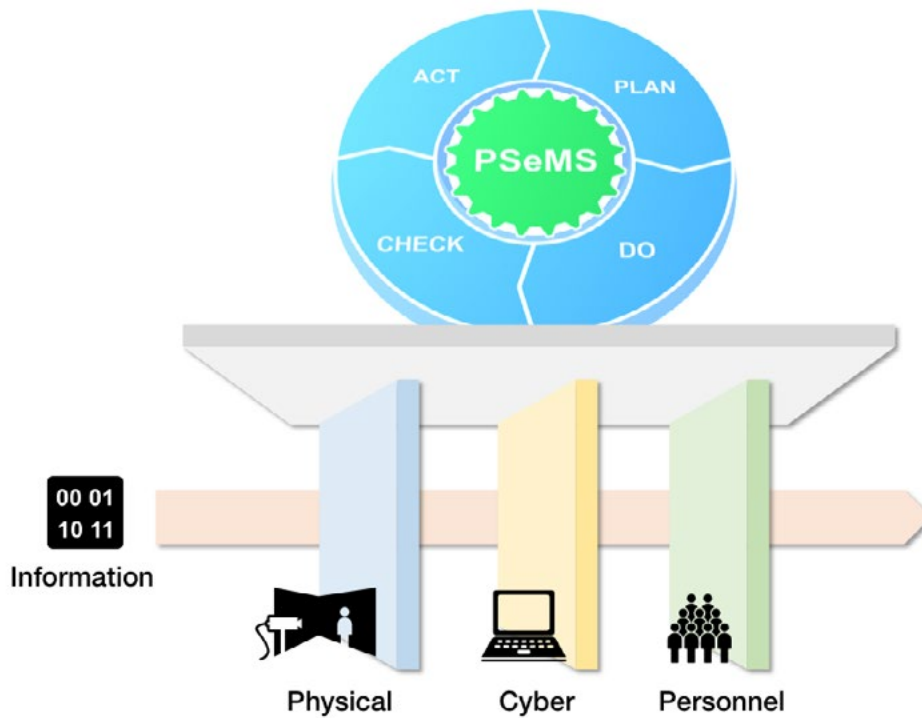
Why?

CNI organisations that have worked with CPNI as part of the PSeMS Working Group have shared their experience of the organisational challenges and benefits provided by PSeMS. An indication of the challenges most often reported are shown in figure 4, below:
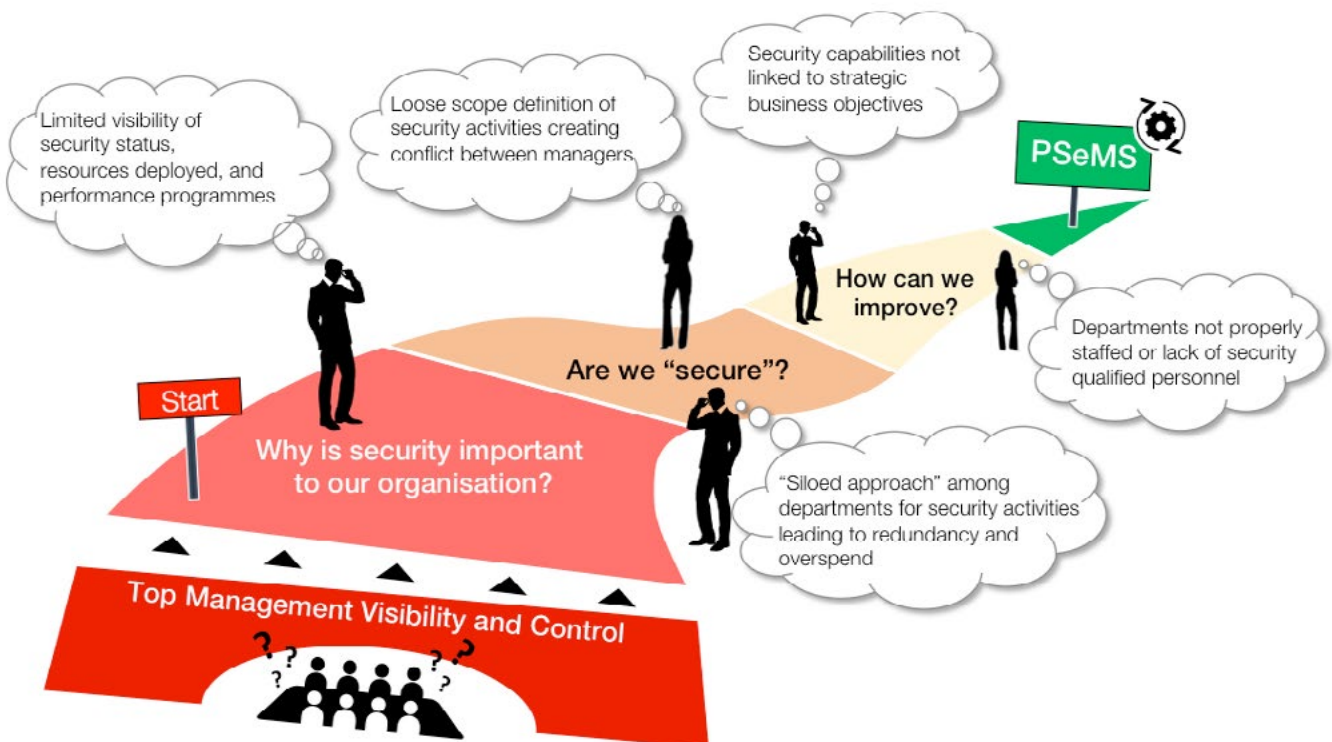

Figure 4: Typical organisational challenges with security management and its assurance

Figure 4 shows the typical challenges associated with organisational security assurance starting with senior management and filtering down the organisation. Oftentimes organisations will have 'siloed' departmental structures leading to possessive ownership of ideas and initiatives that are not shared or dealt with for the benefit of the organisation. This can result in a failure to identify all risks to the organisation. Senior management can demonstrate a strong commitment to security but fail to adequately resource security departments. This can result in security departments lacking the resource to adequately address emerging or new challenges. Finally, security requirements can also be seen as a barrier to effective working unless staff awareness and training is delivered in a way that supports the organisations strategic objectives.

PSeMS can help to reduce gaps in the organisation's security assurance and is a fundamental building block for effective management of security and will have a range of direct and indirect benefits. A selection of PSeMS benefits identified by CNI organisations is shown in figure 5, below. Further real world examples of benefits can be found in the Case Studies section, pp28–41.

Creates Board level accountability for security	PSeMS provides for an Accountable Manager at Board level to ensure the organisation's security activities are appropriately governed, resourced and managed.
Encourages collaborative approaches	PSeMS helps remove silo approaches ensuring that security risk management is an integral part of all business activities, with key stakeholders willing to share 'near misses', best practices and learning.
Encourages transparent and verifiable security	PSeMS enables organisations to demonstrate they are discharging their accountability and responsibilities for security and delivers clear compliance and assurance visibility.
Creates business efficiencies	PSeMS is about integrating security into existing business management systems and processes as opposed to creating something new.
Supports threat assessment methodology	PSeMS helps ensure security performance information is current, readily available, and easily retrievable to support security risk assessments, audits etc.
Empowers and promotes pro-active reporting	A PSeMS approach encourages a healthy security culture where the pro-active reporting of security-related matters forms part of the organisation's inherent behaviour.
Drives a more assurance-based regime	PSeMS performance measures will provide a richer assurance picture, beyond regulatory compliance.
Builds on existing best practices	PSeMS builds on the best practices and various risk management and assurance frameworks, standards and guidance applicable across the Critical National Infrastructure and other organisations.

Figure 5: Reported benefits of PSeMS benefits identified through industry engagement

How?

In order to help achieve the benefits of PSeMS, an understanding of security risks and accountability for them should be visible at the most senior levels in the organisation. This enables an organisation's leadership to establish and formally endorse security policies and outcomes to be achieved by the organisation.

A PSeMS provides a framework to help an organisation develop and assimilate the security policy and objectives such that it is reflected in behaviours, processes, and risk mitigations that are integral with the way all employees carry out their jobs and their daily tasks.

As with all management systems, a PSeMS provides for goal setting, planning and measuring performance, and focuses on maximising opportunities to continuously improve security and the management system itself.

PSeMS is not necessarily about implementing new processes, but about ensuring that the current ones are fit for purpose and brought together to provide an optimised and holistic approach to security assurance.

PSeMS approaches will vary

CNI organisations differ in terms of what they do and their operational environment. This context often shapes and determines the requirements for PSeMS and can include one or more of the following factors which are shown in figure 6, below.

Figure 6: Factors that can inform the scope and manner of PSeMS implementation

The implementation and scope of PSeMS will not be the same for all CNI organisations or even organisations in the same CNI sector due to the above factors. PSeMS is likely to vary according to the unique requirements of each organisation and it is normal for some of the PSeMS components shown in Figure 3 to vary in terms of priority, maturity, and ease of implementation.

What PSeMS is not

Within the scope of this guidance material, PSeMS is not any of the following:

PSeMS is not:					
A set of documents on file or a shelf	A technology or software solution	A rigid process		A substitute for QMS or SMS	A 'silver bullet' or miraculous solution
A significant cost	Reinventing the wheel or creating new processes	A replacement for security regulation	A one-size-fits-all approach		An additional burden
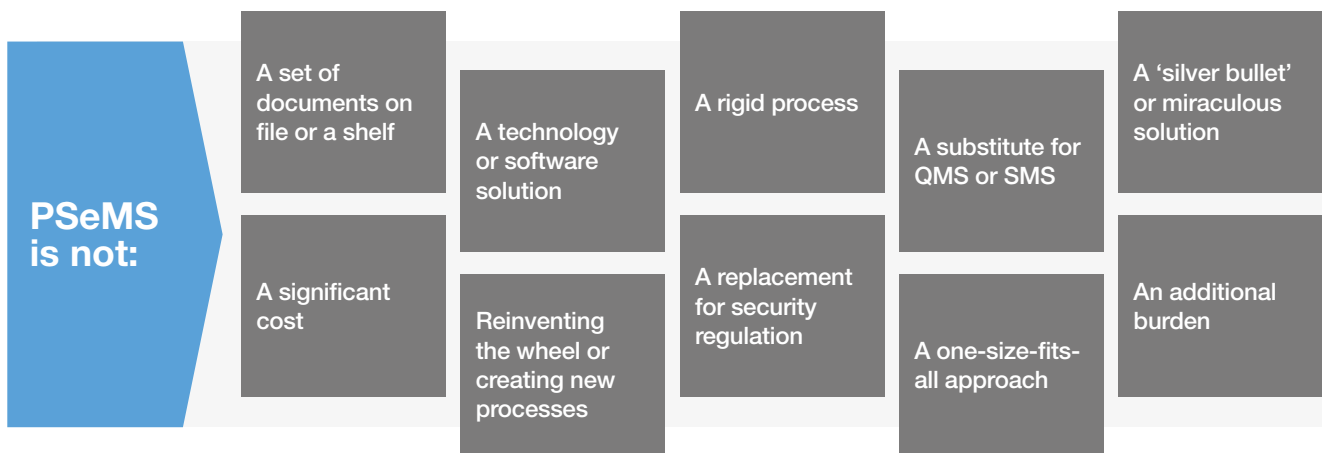
Figure 7: Typical false assumptions about SeMS

Like Safety and Quality Management Systems, PSeMS is susceptible to misconceptions – some of the more popular ones are shown in figure 7, above. Typical reasons for why Management Systems fail to gain recognition and traction are due to the perception that they are part of a periodic 'box ticking exercise'. Although elements of a PSeMS such as security procedures and the security policy will be captured in many documents this does not constitute an effective PSeMS. An effective PSeMS becomes part of the day to day business process of the organisation and its components are shown in Figure 3.

Useful references

Document Type	Title	Date published	CNI Domain specificity	Notes
ISO Standard	Quality Management Systems: **ISO 9001, 2015**	2015	All CNI domains	• Although not security related, set outs principles that underpin Safety and Security Management systems • Details above principles under the Plan, Do, Check, and Act cycle
ISO Standard	Specification for security management system for supply chain: **ISO 28000, 2007**	2007	All CNI domains	• Provides a detailed overview of PSeMS in relation to Plan, Do, Check, and Act • Applies the framework set out in ISO 9001 (quality management) to supply chain security
ISO Standard	Information Technology: Information Security Management Systems: **ISO/IEC 27001, 2013**	2013	Information Security Cyber Security	• Provides an overview of PSeMS in relation to Plan, Do, Check, and Act • Applies the framework set out in ISO 9001 (quality management) to cyber security • The main difference when compared to ISO 28000 (2007) above is that this has a focus on Cyber Security but many of the principles are similar
Guidance	HMG Security Policy Framework, Security Policy **Framework 5:** April 2014	2014	Government	• Less prescriptive than the ISO standards • Provides more of a framework with key principles to adhere to • Suits a more outcome-based environment
Guidance	Framework for an Aviation Security Management System (SeMS)	2014	Transport: Aviation	• Covers PSeMS components in isolation from Plan, Do, Check, Act • Emphasises importance of Accountable Manager for security • Covers regulated components of Aviation Security

Introduction

- This section assists an organisation in understanding its strengths and weaknesses with respect to organisational security assurance

- The assessment includes the most important and critical elements of a PSeMS and is a good starting place especially for organisations that are less familiar with respect to PSeMS
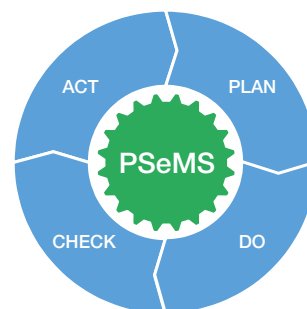
Who should complete the assessment

- Security managers responsible for the organisation's security in consultation with organisational stakeholders who directly or indirectly impact security

- The initial assessment should be reviewed and validated with senior management and Board level management

How to use the checklist section

- This section contains a number of indicators of good practice (statements). Use these to assess your current status and record any required actions

- Next to each of these statements record one of the following responses:
  Yes – processes described in the statement are in place
  In part – processes described in the statement are partly in place
  No – processes described in the statement are not in place
  Not sure – investigation required
  Not applicable – does not apply

- Use the comment boxes to record evidence and rationale in relation to each response and consider gaps in evidence that can be addressed by your action plans

About this section

- This checklist is an additional approach to other assessments which may also cover PSeMS and its maturity

  – It is not a replacement for existing processes or a formal requirement

- It is not expected that organisations will excel or achieve all of the indicators immediately, but you should consider them as prompts for future action

- Some organisations may consider that certain indicators are not suitable for them or do not apply

  – In this event it is recommended you seek to thoroughly understand the opportunities and benefits that may be missed by excluding them

Security Assurance – Assessment of organisational readiness

ACT

Management Review and Improvement

Performance Monitoring

Corrective and Preventative Actions

CHECK

PSeMS

PLAN

Security Management Policy

Security Planning

Implement and Operate

Training, Awareness and Preparedness

DO
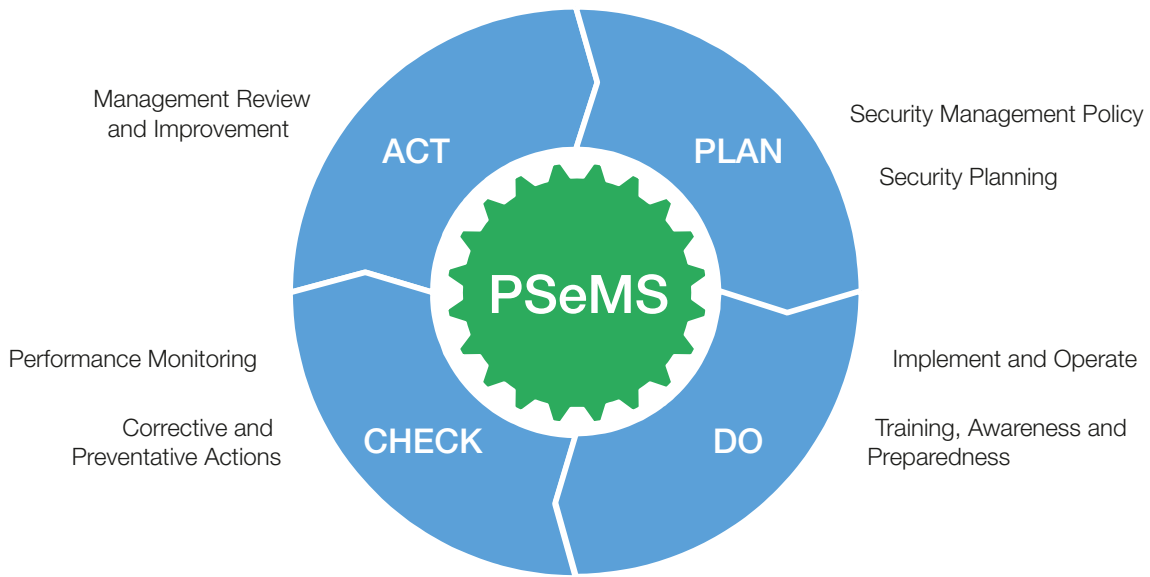
Protective Security Management Systems (PSeMS)

Security Assurance – Assessment of organisational readiness

Recommended steps

The following steps are recommended for an organisation to follow when completing this assessment to ensure the responses to the assessment are valid and any required organisational actions are endorsed at senior level.

1 Complete first iteration of assessment	**2** Validate initial assessment	**3** Validate with top management	**4** Manage and maintain action plan	**5** Repeat assessment as required
• The security manager/lead completes an initial assessment – Ideally, this should be completed in consultation with peers and organisational stakeholders • Rationale, evidence and actions are recorded for each response	• Seek to close out 'not sure' responses • Seek to validate recorded responses and rationale with stakeholders, peers and applicable departments as far as possible	• Validate findings with top management/board level – Obtain agreement on status of responses and actions to address any concerns raised • Ensure impacts for not completing actions are understood by senior management and stakeholders	• Ensure there is a clear plan, roles, and responsibilities for discharging any actions identified • Ensure appropriate timescales are assigned to each action • Actions can include (but not limited to): – Further investigation – Improving processes – Validating rationale and evidence • Actions and risks identified should be included as part of the company-wide risk register	• Agree with senior management and stakeholders the frequency at which the assessment should be repeated

Example Checklist

Sub-topic under 'Plan, Do, Check, or Act'

Content guide: shows Section heading (in blue) in relation to Plan, Do, Check, or Act. In this example it is 'Plan'

PLAN – Security Management Policy

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
1. Senior management endorse and thereby approve the security management policy		X				Check one box per row
2. The policy is based on a credible assessment of security risks to the overall business			X			
3. Security management policy enables specification of security objectives, performance measures, and mitigation requirements		X				Use this space to: • Note evidence/rationale for answer provided • Record actions for further investigation or follow up • Ensure that there is clear plan for following up
4. Security management policy takes regulatory, legal, and statutory requirements into account	X					
5. Security management policy is regularly maintained and updated in conjunction with senior management				X		Not sure! We think security is on the Exec's quarterly review agenda but we never quite know what is discussed or the outcome. Policy is updated but not sure what has been changed and why. Need to check at next Senior Managers' meeting.

Yes — **Yes** (processes described in the statement are in place)

In part — **In part** (processes described in the statement are partly in place)

No — **No** (processes described in the statement are not in place)

Not sure — **Not sure** (further investigation required)

N/A — **Not Applicable (N/A)** (this practice is not applicable to my organisation)

Checklist Template
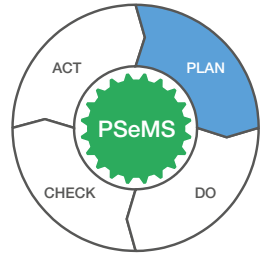
COMMERCIALLY SENSITIVE WHEN COMPLETE

PLAN – Security Management Policy

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
1. Senior management endorse and thereby approve the security management policy						
2. The policy is based on a credible assessment of security risks to the overall business						
3. Security management policy enables specification of security objectives, performance measures, and mitigation requirements						
4. Security management policy takes regulatory, legal, and statutory requirements into account						
5. Security management policy is regularly maintained and updated in conjunction with senior management						
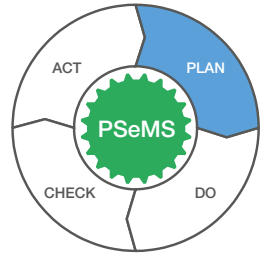
PLAN – Security Planning

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
6. Security objectives and targets are communicated and understood throughout the organisation and applicable third parties, suppliers, etc.						
7. There is an established process for ongoing security risk identification, assessment, and management						
8. Security risk assessments include physical, information, cyber, and personnel domains						
9. Security risk assessments include issues related to technology, people, processes, and environment						
10. The output from security risk assessments informs the design, management, and control of operational security processes						
11. Security management plans for achieving objectives and targets are implemented and maintained						
12. All security processes and procedures set out in management plans have clearly defined performance measures						
13. Security performance measures are specific, measurable, achievable, and relevant						
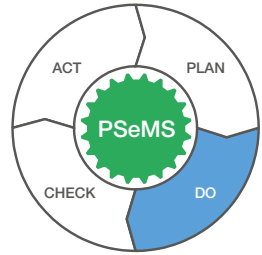
DO – Implement and Operate

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
14. Senior management is formally accountable for the design, maintenance, documentation, and improvement of the organisation's Security Management System						
15. The Security Management System is reviewed and updated in relation to any significant organisational change						
16. Changes to the organisation are documented and reflected as part of the security risk assessment process						
17. Senior management provide agreed financial resources in support of organisational security management plan(s)						
18. Clear roles and responsibilities are defined in relation to security management throughout the organisation						
19. Organisational operations that are necessary for achieving the security policy, objectives, and plans are identified and controlled						
20. A documentation system is established and maintained that includes the security policy, targets, risk management data, plans and procedures, and performance records						
21. Plans and procedures are established and maintained for detailing the responses and mitigations for security incidents and emergencies						
22. Controls are in place to ensure facilities, equipment, and supporting services are effective in achieving the security objectives						
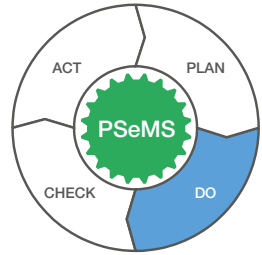
DO – Awareness and Operate

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
23. The security policy is communicated to all staff, third parties, and suppliers						
24. Senior management regularly communicates the importance of meeting security management requirements related to the policy to all relevant stakeholders						
25. Security matters are communicated regularly with effective senior management and staff involvement						
26. Security awareness training is provided to all staff, relevant third parties, and suppliers						
27. Specific security training requirements are assessed in accordance with security roles and responsibilities						
28. Security training provides all relevant personnel with the necessary operational skills, knowledge, and abilities						
29. Exercises and training for emergency preparedness are completed regularly						
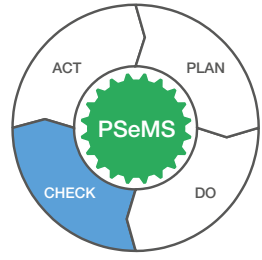
CHECK – Performance Monitoring

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
30. Procedures to monitor and measure organisational security performance are established and maintained*						
31. Procedures to monitor and measure the performance of the security management system are established and maintained*						
32. The frequency for measuring and monitoring the performance measures is proportional to security risks and threats						
33. Performance monitoring and measurement is sufficient to facilitate subsequent corrective and preventive action analysis						
34. Security data is traceable, retrievable, and accessible (i.e., can be interpreted by relevant staff)						
35. There are controls in place to ensure the quality of the performance data is assured						

* For questions 30 and 31, please refer to Annex A for additional prompts to help you better respond to these statements
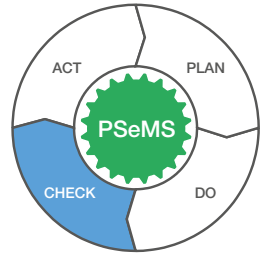
CHECK – Corrective and Preventative actions

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
36. There is an established audit process to help ensure the Security Management System is efficient and effective						
37. Security related failures, non-conformances, incidents, and audit findings are reviewed in a timely fashion						
38. Security and corporate risk registers are reviewed and updated following security related failures, non-conformances, incidents and audit findings						
39. Proposed corrective and preventive actions are assessed and implemented in a timely manner						
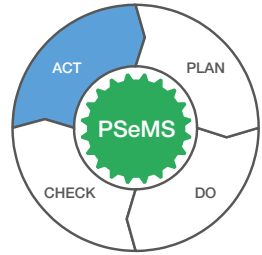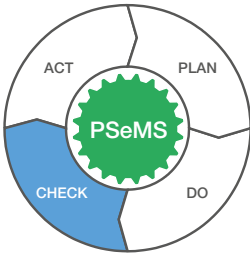
ACT – Management Review and Improvement
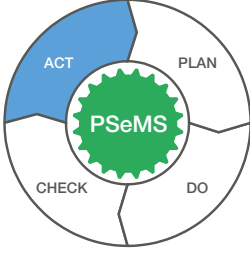
Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
40. Senior management has a defined role and accountability for reviewing and approving the organisation's security management system at defined intervals						
41. Records of senior management reviews are retained as part of the security system documentation system						
42. Lessons learned are captured and taken into account by the organisation upon review, resulting in changes to the security policy where required						
43. Senior management has the information needed to make informed decisions on any changes to security management policy						
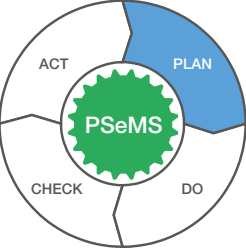
Annex A

The table below provides further information and prompts to inform the assessment of statements 30 and 31. The purpose of the questions below is to help prompt you to think about how your organisation selects, develops and uses metrics and measures to help understand the effectiveness of your Security Management System and the measures you capture to assess its effectiveness.

Component	Prompts
	Are security responsibilities included in role profiles including those outside of the security team?
	Who is responsible for developing the metrics/performance measure?
	How is the data collected?
	Who is responsible for analysing the metrics?
	How is risk assessed in your organisation?
	How often are the metrics reviewed?
	How quickly could security performance metrics be changed in the event of a change to risk or threat level?
	How does the organisation communicate the value of the secirity metric(s)?
	How are the details of the metrics communicated to key stakeholders?
	Does the organisation have an incident reporting programme in place (either confidential or anonymous)?
	Are security awareness training records kept?

Component	Prompts
	What data analysis is carried out on the security performance metrics?
	How are the analyses and results displayed? For example are the results displayed in a dashboard format for review or sharing?
	Who is the information presented to?
	How often are the metrics shared with relevant shareholders?
	How often are the metrics reviewed?
	Who reviews them and where?

| Component	Prompts
	How easy is it to adapt security performance metrics if they are not adding value?
	How quickly could security performance metrics be changed?
	Is the organisation able to advise of any Enablers (processes and interventions) that have been beneficial at an organisational, operational and tactical level?
	Is the organisation able to give examples of how their PSeMS and security performance metrics have helped improve security and risk management?
	Have there been any financial benefits identified following the analysis of security performance metrics or from the development of your PSeMS?
	Have any other benefits been noted following your organisation's development of PSeMS, e.g. reduction in security incidents, increased levels of reporting by staff, improved staff morale, greater confidence in risk management and assessment due to the quality and integrity of security performance metrics available?
	Do your metrics include measurement of the time taken to resolve security issues?
	Has your Security Performance data/metrics (and SeMS) helped inprove your organisation's ability to influence senior decision makers within the business?

| Component	Prompts
	How are performance metrics established at board level?
	Which metrics does the Board/key stakeholders place most value on or see as more important?
	To what extent does security performance assessment form part of objective-setting processes within the business?
	Are the metrics included in the Security Plan or its equivalent?
	Is there an approval process when metrics are being set, and if so, at what level, e.g. Accountable Manager, Board-level Responsible Officer, or equivalent?
	Have you used Return on Investment (ROI) data as a tool to harness management attention and action with regards to security performance metrics?
	Which aspects of the organisation's security programme are measured to determine current performance levels or program effectiveness?
	Are the organisation's security performance metrics compared to external benchmarks?
	Are the metrics applicable to third parties?
	Why did the organisation select these particular metrics?
	How are the metrics generated (by which sources)?
	Do you score your metrics against an evaluation process?
	Are the metrics linked to, aligned with, or form part of the organisational risk process or organisational objectives?
	Are the metrics focused on cost, risk management, or other aspect of the organisational requirements?
	Are the metrics based on legal or policy requirements?

Protective Security Management Systems (PSeMS)
Case Study – Transport Sector – Airport

Applicable PSeMS components

- Senior management endorse security policy

- Security management plans implemented and maintained

- Clearly defined performance measures and objectives
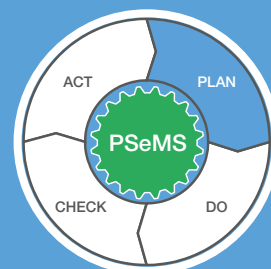
Challenges

- The greatest challenge was ensuring cohesion between organisational stakeholders such that they were all signatories to the Security Master Plan which helps provide confidence in security assurance.

- Gap analysis alone would not help the organisation to resolve the gaps, and there was no guidance material for them to refer to.

- Other constraints were caused by the prescriptive approach taken in relation to regulatory compliance – often taking a quantitative approach rather than a qualitative one. It needed to be recognised that PSeMS supports compliance and is not just a project being imposed by the regulator.

What was done

- A greater focus was placed on security communication and the development of a Security Master Plan. This document helped consolidate the various PSeMS components and documented them in single source. For example, the organisation's security meetings were well established, but the Security Master Plan helped articulate the information and decision flow, by integrating them to demonstrate that the organisation had a solid governance structure with clear roles and responsibilities.

- The CAA's PSeMS Assessment Tool was used for completing the gap analysis and identifying where compliance improvement areas were required. It helped identify areas of consistency and conformity that can be developed within industry.

- Compliance was renamed 'Protection' as the organisation believed that regulatory compliance alone was simply not enough to cover the wider business continuity interests.

Benefits

- The organisation's Accountable Manager (Board level) now has a much clearer understanding of the role accountabilities and is more security focused.

- The Security Master Plan enables the organisation to provide a high-level holistic view of their security arrangements, obligations, and assurance. This informs key stakeholders, internal and external, encouraging a unified and collaborative approach to security delivery.

Case Study – Transport Sector – Airport

continuation (2 of 2)

Applicable PSeMS components

- Senior management endorse security policy

- Clear roles and responsibilities, training

- Regular security risk and threat assessment
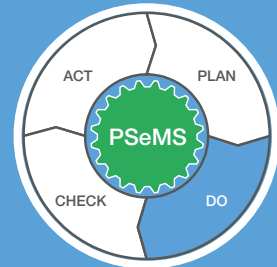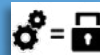
Challenges

- The security compliance team was small and operating at capacity. There were no additional resources assigned, nor was it clear what benefits a PSeMS would bring, particularly as the Airport already had a comprehensive Aviation Security Programme, which met regulatory requirements.

- The Security team worked in a reactive environment, often having to take a fire-fighting approach which created challenges in terms of PSeMS implementation as there was limited time and resources available and these were depleted when a significant event occurred.

- The desire to be more collaborative was faced with the challenge of balancing stakeholder needs for information sharing versus the commercial challenges of 'showing your hand' in security.

What was done

- The five-year plan, included in the Security Master Plan, outlined the path the organisation wanted to fulfil and provided information about how the organisation was evolving how they do things.

- The organisation created a dedicated Security Intelligence team to ensure their risk picture is the best it can be. This has been achieved following a comprehensive review of the RAG, ensuring that the right stakeholders are present, and that the risk register is kept under constant review.

- The organisation uses risk registers throughout their business areas, e.g. security, finance, commercial, security operations, and environment. The process applied for oversight and governance was kept the same regardless of the business area. By consolidating and explaining this method in the Security Master Plan the organisation demonstrated an integrated risk management approach.

Benefits

- Reduction in the organisation's vulnerability to an 'abundance of caution' approach and the resulting additional costs this can bring.

- The Security Master Plan enables the organisation to ensure that security is a constant organisation priority, with appropriate resources, investment and ways of working in place to respond systematically to the threats they face.

- A benefit under 'Check': CAA inspections and visits are easier due to the PSeMS work undertaken within the organisation making it easier to demonstrate compliance and oversight. Performance data is traceable, retrievable, and accessible.
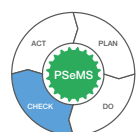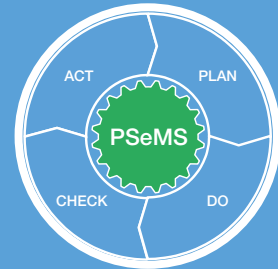
Protective Security Management Systems (PSeMS)

Case Study – Energy Sector – Energy Terminal

Applicable PSeMS components

- This organisation has a broad range of challenges across all areas e.g. Plan, Do, Check, and Act (PDCA)

- SeMS Components are broken down on the following pages for PDCA under 'What was done' and 'Benefits'

Challenges

- This facility identified the requirement for an effective and efficient PSeMS implementation. The principal challenge was how to create this and deliver a security provision that was deemed 'mature' with effective integration of all security and operational stakeholders, clear monthly reporting, Board level accountability, and processes for continual improvement and its monitoring and review. An 'early adopter' version of PSeMS was already established at this site.

- Industrial and operational growth at this site also resulted in a need for the organisation to increase and integrate the security manpower. The organisation had two providers; one subsidiary provider managing site security only (perimeter security) and the other delivering a wider range of both site, maritime, and facilities security. It was decided to establish a single provider with all responsibilities passed to one security provider. The challenge was how to ensure integration was effective with no increase in security breaches.

  – The security team previously providing perimeter security only was identified as operating to a less effective standard than the main security team.

  – The principal challenge was to address how best to merge the two entities that are both operating under PSeMS guidance on the same facility. The challenge to address was whether the more mature PSeMS entity would lead to the less mature entity increasing its standards or whether the less mature entity would adversely impact the more mature entity.
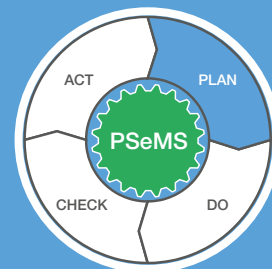
Case Study – Energy Sector – Energy Terminal
continuation (2 of 4)

Applicable PSeMS components

- Senior management endorse security policy

- Clearly defined performance measures and objectives

What was done

- At the start of each financial year the organisation prepared its corporate vision. The security function aligned itself with this by providing best value and evaluating how security could be better managed. For example, if new security policies were introduced they would create an additional cost to the business and if so the security team would demonstrate a corresponding reduction in security risk.

- Safety and security related policies, procedures, and requirements were included in procurement documentation supplied to the organisation's third-party suppliers.

- Extensive metrics were put in place covering people, performance, and continuous improvement. Some notable elements from the organisation's performance measures were a 100-day plan/security roadmap and a Success Register so that positive security news could be shared. Other tools used to engage with stakeholders for problem resolution were SIPOC (Supplier, Input, Process, Output and Customer).

- Additional security performance metrics were implemented to cover the serviceability of the organisation's physical security equipment. They used a red, amber, green approach to enable them to see the status of the security equipment on site, particularly the CCTV and provide an early indication that remedial measures to mitigate risk may be needed.

Benefits

- The Head of Security is required to present to the organisation's insurers every two years. Premiums have been reduced due to confidence in the security management system and oversight in place.

Case Study – Energy Sector – Energy Terminal
continuation (3 of 4)

Applicable PSeMS components

- Regular workforce engagement

- Clear roles and responsibilities, training

- Regular security risk and threat assessment
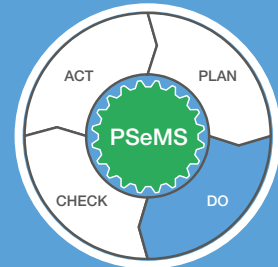
What was done

- The organisation nurtured a strong security culture by placing confidence and trust in the security teams and focusing on developing effective relationships across the business.

- The organisation ensured that security was seen as an enabler and not a barrier to business activities by providing valid examples and successes – such as the reduction in insurance premium.

- All security activities, including those of the contract security team, were integrated into the organisation's normal business activities to avoid 'silo' approaches.

Benefits

- The organisation's people-focused approach has helped create a positive security culture within their business, particularly with regard to security reporting.

- Risk management processes are more robust with appropriate accountability in place.

Case Study – Energy Sector – Energy Terminal

continuation (4 of 4)

Applicable PSeMS components

- Established audit and assurance process for PSeMS

- Corrective and preventive actions for security failures
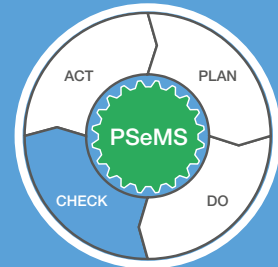
What was done

- A self-audit program was implemented and the organisation adhered to the International Ship and Port Facility code, a guiding document covering policy relating to tactical aspects of maritime security and response.

- A zero tolerance approach was taken with contractors' compliance breaches.

- Contract security personnel were empowered to deal with incidents without needing authorisation from the organisation's Security Management team who did not want to constrain their contractors to Assignment Instructions as there was a need for a flexible approach.

Benefits

- The organisation's positive organisational security culture, effective communications, robust response measures and embedded metrics helps them to routinely manage incidents and is a good example of 'learn, review, and improve'. This helps support continuous improvement of the organisation's PSeMS.

- An example of the organisation's security performance and oversight measures being used to good effect followed an incident involving an individual who gained unauthorised access to the site. The intruder was rapidly spotted by two non-security employees who immediately notified the security control room. Armed police officers and the contract security team were deployed to the scene and the intruder was subsequently arrested. Details of the event were recorded on the organisation's Threat Calendar Log which forms part of their performance and excellence metrics, and a '3C' form generated to show the Concern, Cause, and Countermeasures. An immediate review of the incident revealed the cause of the event to be a failure in the CCTV patrol strategy. The frequency of patrols on vulnerable points was not sufficient and was increased, along with the full site patrols. The organisation provided a resolution to the event within 2 hours of it occurring. Security policies were updated with the lessons learned. The security metrics in place ensured a timely review and implementation of effective countermeasures.

Protective Security Management Systems (PSeMS)
Case Study – Financial Sector – Financial Institution

Applicable PSeMS components

- Senior management endorse security policy

- Security management plans implemented and maintained
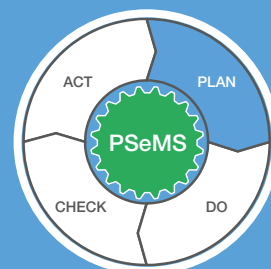
Challenges

- The security department lacked the ability to describe why particular security processes are necessary.

- Security policies were either incomplete, difficult to implement, or absent. The policies often did not have a sound operational rationale for their implementation.

- Security processes were perceived as a barrier to achieving business goals and the importance of security procedures was not appreciated by senior management. It was therefore a priority to show how security could be an enabler and be of benefit to all staff and all business areas.

What was done

- Recognising the importance of senior level engagement the security management team took advantage of the requirement to conduct home security visits with members of the leadership team (due to prior intelligence that they could be potential 'targets' of external threat actors). This made security personal to these individuals and brought home the importance of the security function within the organisation.

- The security team helped to positively change the attitude of the leadership team to security within the context of the wider organisation.

- Presenting security risk analysis and recommendations in a format similar to financial analysis (which the Board is used to working with) is helping to demonstrate security benefits.

Benefits

- By targeting the senior leadership team via one to one engagement, created high-level advocacy and corrected entrenched misperceptions of security.

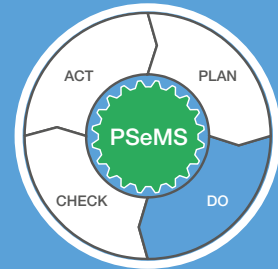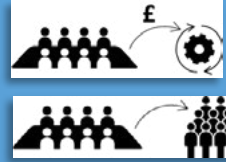- Increased ability to demonstrate organisational security benefits.

Case Study – Financial Sector – Financial Institution
continuation (2 of 3)

Applicable PSeMS components

- Senior management approve resources

- Regular workforce engagement

Challenges

- Minimal resources were available to enable the organisation to focus properly on threat, policy, training, and risk management. However, there were adequate resources devoted to aspects of physical security.

- The organisation lacked the resources to assess security intelligence and emerging risks to help inform decision-making and policy across the organisation.

What was done

- New security roles were established with the express purpose of providing an integrated focus on threat, policy, training, and risk management. The organisation formalised the role of Chief Security Officer with clearly defined roles and responsibilities. A Senior Security Risk Manager was appointed with qualifications in threat intelligence analysis, policy development, and security training and education.

- A conscious effort was made to use consistent language to describe security risk and avoid using jargon. A common taxonomy for risk was established so that all departments see the measurement of risk in the same way.

- A deliberate effort was made to recognise and celebrate good security practices and behaviours across the organisation. This helped to associate good security with a positive experience. This was done through media campaigns and emails of thanks to staff who showed the right approach (with details copied to their line management).

Benefits

- Senior management approval of increased resources has enabled the organisation to take a more structured and risk proportionate approach to security that helps in inform threat intelligence analysis, policy development, security training and education.

- Increased recognition of the security team's role and capabilities has helped to influence and build trust across the organisation. Therefore, success stories related to security are more visible across the organisation and with greater traction with senior management. The security team expect the value of this type of benefit to increase as PSeMS develops and matures within the organisation.

- Personalising security delivery has helped with engagement at the leadership level and has created a positive impression that 'security is looking out for me, and my family'.

Case Study – Financial Sector – Financial Institution
continuation (3 of 3)

Applicable PSeMS components

- Informed decisions at senior level

- Improvement: Security policy updated with lessons learned
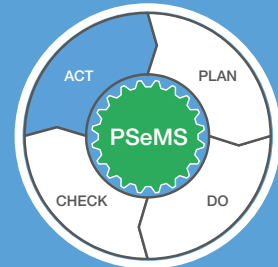
Challenges

- The organisation lacked an understanding of how to improve the existing physical security systems despite extensive experience in maintaining standards of security.

What was done

- More focus and structure was obtained to risk and threat intelligence as a result of implementing a formal PSeMS process supported by appointment of a Senior Security Risk Manager.

Benefits

- The intelligence/threat picture the organisation is now able to present to stakeholders creates business opportunities and drives a more pro-active response with informed security decisions being made at a senior level.

- An unexpected benefit for the organisation was that a security risk assessment conducted on invited participants prior to a high profile communications event revealed factors about individuals that whilst not security related, enabled the speakers to target their presentations and prepare for likely challenges and questions. This target audience analysis was a real non-security benefit from a security activity. This clearly demonstrated that security can not only add value but can, if done correctly, be an investment and not a cost.
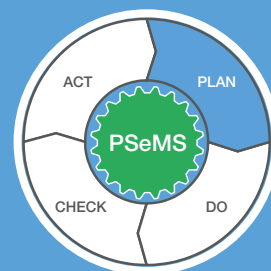
Protective Security Management Systems (PSeMS)
Case Study – Transport Sector – Train Operating Company

Applicable PSeMS components

- Senior management endorse security policy

- Clearly defined performance measures and objectives

Challenges

- The organisation wanted to achieve a level of corporate security and risk assurance beyond the mandated requirements of the National Rail Security Programme.

- Identifying and understanding the 'triggers' for the Board and speaking their language was a challenge for the security team as there was a tendency for a reactive rather than pro-active approach to be taken.

What was done

- Security surveys were developed and distributed across the business to determined where barriers and negative behaviours toward security were most present and why.

- An appropriate PSeMS was aligned such that it reflected the organisation's values which was key in terms of achieving traction with the Board.

- Much work was done to identify metrics already used within the business and linking them to Security. Linking security to a metric that was regarded as a sector staple such as 'disruption minutes' helped achieve greater focus from senior management as it was identified as an 'attention trigger'.

- A cost versus benefit approach was used to help inform discussions on the benefits of security.

- The organisation's PSeMS enablers included using common language and aligning processes with existing models e.g. the National Decision-Making Model and the Secure Stations Accreditation Scheme which encouraged the organisation to be holistic in their approach.

- Linking company security awareness initiatives to external campaigns such as the UK's NCT Week helped magnify the importance.

Benefits

- Obtaining Board level attention and representation for the security function helped influence senior management decision making and has put security on the same foundation as safety in terms of importance and decision making.
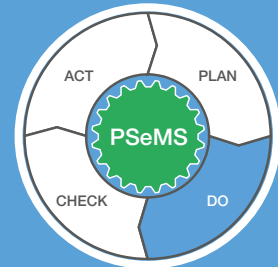
Case Study – Transport Sector – Train Operating Company
continuation (2 of 2)

Applicable PSeMS components

- Regular workforce engagement

- Clear roles and responsibilities, training

Challenges

- Security was initially seen as the poor relation of safety and there was a need for greater security influence and integration throughout the organisation.

- Awareness of security needed to be increased across the business. Buy-in from all departments was problematic with some areas holding the view that security was not their responsibility.

- Security communication across the organisation needed enhancing. Aligning PSeMS with those of station owners and other TOCs was challenging, due to their reluctance to collaborate.

What was done

- The use of in-house messaging tools, such as Yammer to brief staff ensured widespread coverage with minimal impact to business operations.

- Security Awareness training was provided to the Revenue and Security Managers (RSMs) and now included PSeMS in addition to Security and regulatory requirements under the National Rail Security Programme. This was done on a train the trainer basis, with the RSMs then acting as ambassadors for the business.

Benefits

- Much greater focus on security, particularly in relation to communication and employees' understanding of station security plans and the response to threat level changes.

- Enhanced communications channels for security resulted in a noticeable improvement in security incident reporting and greater buy-in to security requests. Security is now in the main agenda as opposed to 'AOB'.

- Helped reduce headcount by making more effective use of existing resources.

- Ensured that the resource used was effective in merging 'operational needs' and 'security requirements' as the business knowledge was present and the messaging and communications were consistent.
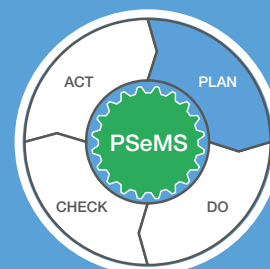
Protective Security Management Systems (PSeMS)
Case Study – Transport Sector – Multimodal Transport Operator

Applicable PSeMS components

- Senior management endorse security policy

- Security management plans implemented and maintained

Challenges

- It was recognised that there were opportunities for security to become more systemised with a requirement for better standardisation in security management approaches throughout the organisation.

- The organisation wanted to develop a flexible approach to achieving security assurance based on the organisation's overall objectives, with measures being developed centrally and empowerment for delivery firmly embedded locally and with those responsible.

- The organisation had many of the PSeMS components in place, but certain processes such as risk management, security resilience, and security performance management needed developing and optimising.

- Safety had traditionally had a far greater focus than security and held greater attention at senior management level.

What was done

- Some elements are still work in progress, but the organisation has achieved the following in relation to the above challenges:

  – A change in senior leadership within the organisation resulted in a new vision, purpose, and supporting pillars for the business. For the first time security was included as one of the supporting pillars (Safety and Security, Assurance and Compliance).

  – The alignment of security within safety was key, and the organisation's established Steering Groups were now used to deal with the respective security focus areas: workplace violence and suicides (Health and Wellbeing) and terrorism and trespass (Customer Safety).

  – The organisation changed its perception and emphasis of security recognising that robust risk controls often come from other areas of the business e.g. safety, customer services.

Benefits

- The alignment of security with safety has helped to improve the status of security, as safety had always enjoyed a greater focus within the organisation.
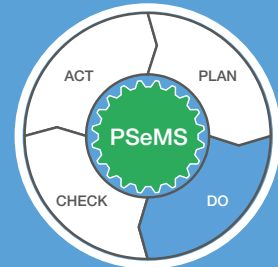
Case Study – Transport Sector – Multimodal Transport Operator
continuation (2 of 3)

Applicable PSeMS components

- Regular security risk and threat assessment

Challenges

- Senior management level support is good but the organisation needs to also focus on longer-term risks rather than immediate challenges.

- The security team had finite resources.

What was done

- The PSeMS approach adopted by the organisation encouraged a collaborative approach with key stakeholders to inform intelligence gathering and security risk assessment. The organisation is policed by the British Transport Police (BTP) and strong, collaborative relationships exist between the two organisations. A Performance and Stakeholder Engagement Plan is in place between the two entities and good levels of collaboration are also maintained with the Department for Transport (DfT). These relationships are based on mutual trust, confidence and a shared understanding that the organisations are seeking to achieve the same objectives.

Benefits

- Improved collaboration with external stakeholders has helped ensure the security risk assessment process is well informed while leveraging external resources.
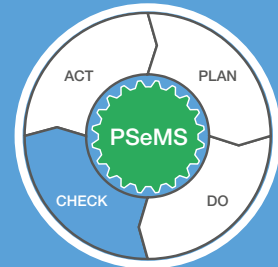
Case Study – Transport Sector – Multimodal Transport Operator
continuation (3 of 3)

Applicable PSeMS components

- Performance data is traceable, retrievable, and accessible

ACT   PLAN

PSeMS

CHECK   DO

Challenges

- The organisation did not have the capability to view the network-wide compliance picture and were examining security performance data site by site. This tended to create a risk-averse approach where one relatively small problem identified could result in a wrong assumption that the issue was more widespread.

What was done

- Covert tests are now being performed in conjunction with the regulator. Local management teams have been empowered to conduct their own tests. Work is underway within the Light Railway to develop their systems to achieve a more complete view of performance data.

Benefits

- More informed assurance picture and credibility with regulator.

- The focus on PSeMS/security assurance has helped to move the organisation from a reactive stance to one that is pro-active and risk-based.