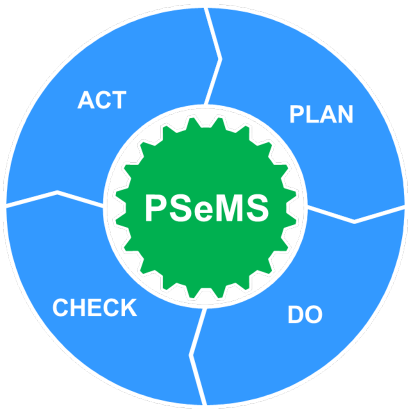
CPNI

Centre for the Protection of National Infrastructure

Protective Security Management Systems (PSeMS)

Pandemic Self-Assessment Checklist

Protective Security Management Systems (PSeMS) – Pandemic Self-Assessment Checklist



About this document

- This Pandemic 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 during the period of the Pandemic, 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.*

Introduction

- This document assists an organisation in understanding its strengths and weaknesses with respect to organisational security assurance during a Pandemic such as COVID-19.
- 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 this document?

- This document contains a number of indicators of good practice (statements) which are particularly relevant to managing protective security during a Pandemic. 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 or in the process of being put in place

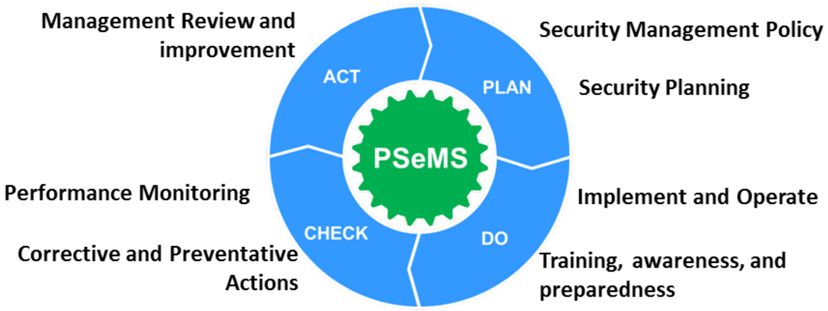
  No – processes described in the statement are not in place

  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.

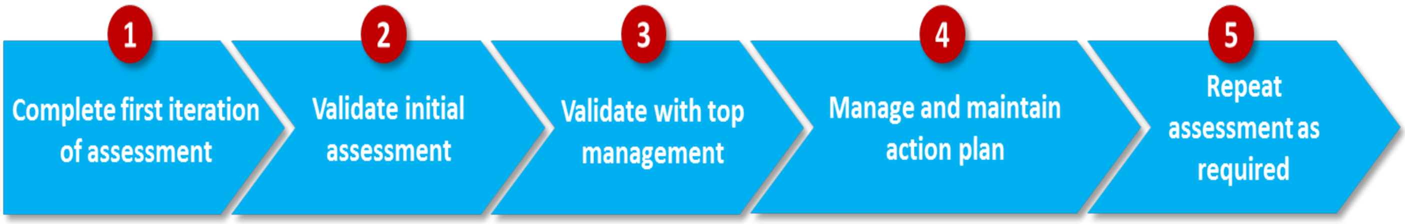
Security Assurance

Assessment of organisational readiness


Management Review and improvement
Security Management Policy
ACT
PLAN
Security Planning
PSeMS
Performance Monitoring
Implement and Operate
CHECK
DO
Corrective and Preventative Actions
Training, awareness, and preparedness

Protective Security Management Systems (PSeMS)

- **https://www.cpni.gov.uk/protective-security-management-systems-psems**



1 Complete first iteration of assessment

- 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

2 Validate initial assessment

- Seek to close out ‘not sure’ responses
- Seek to validate recorded responses and rationale with stakeholders, peers and applicable departments as far as possible

3 Validate with top management

- 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

4 Manage and maintain action plan

- 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

5 Repeat assessment as required

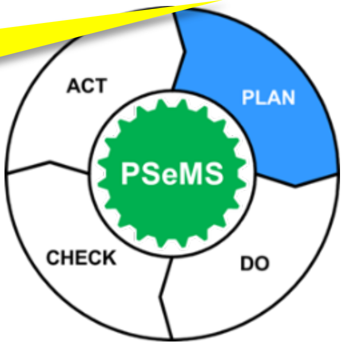
- Agree with senior management and stakeholders the frequency at which the assessment should be repeated

Recommended steps

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

Example Checklist

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



Sub Topic under 'Plan, Do, Check, or Act'

Security Management policy

Best practice indicators	Yes	In part	No	Not sure	N/A	Evidence/Actions
1. A security risk assessment related to the changed circumstances of the pandemic has been carried out covering: • Personnel issues (availability, home working, furloughing, redundancies, etc.) • Changes to working practices • Changes to technical security controls Availability of maintenance, repair, installation and support services.				X		Not sure all changed areas listed here have been covered. Need to check with HR and Cyber stakeholders and report back to the Senior Security Managers' meeting.

Check one box per row

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 actions

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)

PANDEMIC PSeMS CHECKLIST - TEMPLATE

PLAN – Security Management Policy

Best practice indicators	**Yes**	**In part**	**No**	**Not sure**	**N/A**	**Evidence /Actions**
1. A security risk assessment related to the changed circumstances of the pandemic has been carried out covering: • Personnel issues (availability, home working, furloughing, redundancies, etc.) • Changes to working practices • Changes to technical security controls • Availability of maintenance, repair, installation and support services						
2. Security policies have been adjusted where necessary, for example, for: • Rules for use of communications devices (e.g. cameras, microphones, conferencing software, etc.) • Monitoring of suspicious security related behaviours (e.g. hostile reconnaissance, indications of insider activity, etc.) • Use of third-party suppliers • Suspension of or changes to usual security practices						
3. Changes in security practices have been communicated to staff and support and guidance is in place.						
4. The organisation's security posture and risk appetite has been explicitly reviewed, and decisions made about what reductions in security would be tolerable.						

DO – Implement and Operate

Best practice indicators	**Yes**	**In part**	**No**	**Not sure**	**N/A**	**Evidence /Actions**
5. The need for new services (e.g. for holding remote meetings), new software, new IT controls, etc., has been evaluated and requirements decided upon with security in mind.						
6. Action has been taken to increase awareness and capability amongst all personnel, including suppliers, of the changing security landscape and to educate them about required changes in behaviour? (e.g. increased risk of email scams, how to use personal IT devices securely working from home, how to report problems that arise during home working, etc.)						
7. Additional or alternative protective security measures have been identified and implemented where usual security practices are no longer adequate? (e.g. increased use of technology for monitoring of security behaviours, enhanced controls to ensure operational services are secure, etc.)						
8. Effective processes have been introduced for maintaining contact with and supporting personnel working at home.						
9. Effective policies and procedures have been introduced for managing personnel who are being furloughed or made redundant.						

CHECK – Performance Monitoring and Response

Best practice indicators	**Yes**	**In part**	**No**	**Not sure**	**N/A**	**Evidence /Actions**
10. Ways of collecting, analysing and evaluating data from new or revised monitoring activities have been introduced and are being used to inform decisions on preventive security measures.						
11. The effectiveness of new or revised corrective, preventative or response activities is being evaluated and the results used to inform decisions on enhancing security measures.						
12. Checks that personnel are coping with the changes to their working practices are being undertaken and support provided where necessary. *						
13. Fair and proportional procedures are in place for dealing with behaviours or performance which does not conform to new or revised working practices. *						

*Further advice on specific personnel security risks associated with your workforce during a Pandemic can be found at: https://www.cpni.gov.uk/system/files/documents/13/31/Guidance%20to%20Insider%20Threat%20during%20a%20Pandemic-PW.pdf.

ACT – Management Review and Improvement

Best practice indicators	**Yes**	**In part**	**No**	**Not sure**	**N/A**	**Evidence /Actions**
14. Review of new or revised security practices has been included as a standard item in Board / SMT meetings.						
15. Lessons learned about the success or failure of new or revised security practices are captured and taken into account in any changes required to the security policy or practice.						

Further advice and guidance

Further advice and guidance on how to maintain a robust protective security system during a Pandemic can be found at https://www.cpni.gov.uk/staying-secure-during-covid-19-0.

CPNI 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.