Achieving secure Physical Security Systems

1. Identify a senior risk owner

at board level who can help and support the process.

2. Ensure that physical security and IT security teams collaborate

to define the demands of the PSS environment and achieve a workable secure solution.

3. Request that developers demonstrate compliance with CAPSS

when inviting tenders for the supply of equipment and systems. This should include evidence of a publicly stated vulnerability disclosure policy.

4. Identify the systems and environment

into which you have the physical security installed, and ensure they are suitably audited and documented.

5. Assess the risks

that are inherent in your PSS environment and identify whether further action is needed to deal with issues identified in step 4.

6. Assess the systems and environments using the NCSC CAF.

The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done.

7. Identify the locations

in which your systems and devices are deployed, as defined in this document (i.e. non-secure area, secure area, secure enclave).

8. Identify where gaps exist

between the controls identified in this document and the environment you are operating.

9. Devise and implement a plan

to close gaps to ensure long-term management of any risks associated with the system. Repeat this in line with security best practice.

10. On-going monitoring

Include the Physical Security Systems within the scope of your Information Assurance processes and systems, and ensure they are continually monitored.