

Introducing a Security Risk Management System (SRMS) at your facility requires a level of time, resource and effort.

By introducing an SRMS, you will be initiating positive change that will result in a range of benefits associated with engagement, efficiency, transparency and assurance. To be successful, you will need the engagement of those responsible for security at your facility. This is normally found at board level, though the specific role of the individual(s) responsible may vary from one facility to the next.

This infographic guides you through the basic stages of setting up an SRMS. Further detail can be found in the SABRE scheme document (SD0229 v1.1).

Examples of where SABRE assessment and certification relates to the process, and how the standard can support you in achieving your objectives, are contained in this infographic.

SABRE is owned by the Building Research Establishment (BRE, incorporating LPCB) and operated by The Security Institute.

For further details contact us at sabre@security-institute.org or visit www.security-institute.org/sabre

Stage

What's required?



Commitment

This stage involves establishing the presence of commitment to improve security arrangements at the facility. Change can entail, but is not limited to:

- *Improving effectiveness*
- *Managing and reducing risk*
- *Improving procurement, ROI & CSR*
- *Better marketability*
- *Greater assurance for stakeholders*



Gap Analysis

This part of the process involves establishing an understanding of the current approach to facility security and setting clear targets for future performance.

Areas to review include:

- *A review of policies and procedures*
- *Existing risk assessment procedures*
- *The strategic approach to security*
- *Documentation of security measures*



Plan & Improve

Set a realistic plan that will:

- *Address any critical gaps identified in Stage 2.*
- *Identify technical/organisational support that may be required.*

Set a realistic budget and timescale for implementation that meets management's expectations, and which offers a clear value proposition to the organisation.



Implement

This phase involves putting into action the plans devised in Stage 3 and documenting the various components of the Security Risk Management System (SRMS).

Effective implementation requires appropriate provision of technical and operational resources, and where necessary, the involvement of suitably qualified professionals.



Operate

The System is operated and maintained by The Security Manager. Non-conformances are recorded and addressed during regular updates to the SRMS.

The person(s) responsible for security regularly reviews performance and effectiveness of the SRMS, communicating review findings to The Security Manager.



Assurance

Much like enterprise management systems, the facility SRMS may be independently assessed and certified by a third-party certification body.

This helps to robustly communicate achievements to interested parties such as: *the C-suite, investors, prospective occupiers, insurers, local authorities and more.*

SABRE

An informal conversation with a SABRE Assessor or The Security Institute can help you determine whether you are ready to proceed.

A SABRE Registered Assessor can carry out a pre-assessment with you and your stakeholders to identify gaps and associated areas for improvement.

SABRE Registered Professionals can assist you in developing a plan to suit your operating requirements and fill critical gaps identified in Stage 2.

SABRE Registered Professionals can assist you in implementing your SRMS and producing key documentation upon which the SRMS relies.

Your system will need maintaining to make sure it is up to date and fit for purpose. SABRE Registered Professionals can assist with this activity.

A SABRE Assessor will conduct an assessment and submit a formal application to BRE for LPCB certification and Red Book Listing of the facility.