Security Risk Management

Statement of Capability

Many large companies are finding their facilities, operations and sensitive information is under increasing security threat, whether located in developing countries or Western urban centres. As a result, identifying and protecting against threats such as political instability, terrorist attacks, natural disasters, insider sabotage, cyber hacking or information theft is a priority for many organisations.

Risktec helps organisations to identify, understand, assess and manage their security risks. Our systematic yet flexible approach develops a comprehensive security plan, covering physical and procedural defences.

Our services encompass:

Physical Security

- Security vulnerability assessment
- Vital area assessment
- Crown jewel assessment
- Governance and process consultancy

Information Security

- Security governance and process consultancy
- ISO27001 gap analysis
- NCSC / HMG GSC gap analysis
- Maturity assessment
- Virtual information security management (CISO/ISM)
- Secure information facility design

Cyber Security

- Cyber HAZOP risk assessment
- Cyber LOPA risk assessment
- Gap and compliance analysis to a wide variety of UK and international standards (IEC62443, IoTSAF, OG -0086)
- IoT risk assessment
- Design assessment and analysis
- ICS / OT security governance and process consultancy.

Personnel Security

- BPSS security screening processes
- Insider threat assessment

BUSINESS FOCUSSED SECURITY

Risktec operates in all risk management disciplines, allowing us to draw on knowledge from other industries to assess the complete picture. Our solution oriented approach is focussed on identifying an applying the most effective methods to produce the required results.

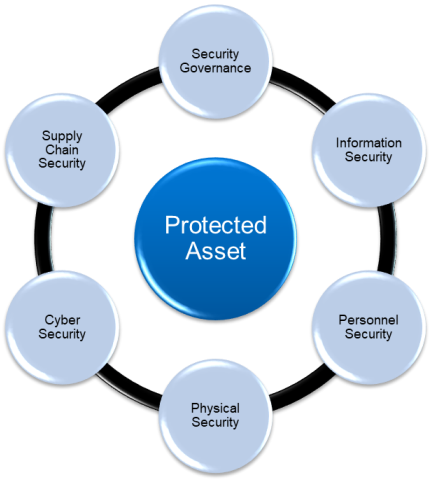
For facilities and operations to remain viable, it is vital that there is an effective and integrated approach to managing risks. Risktec use a pragmatic approach to help organisations set security objectives that support business goals, and in turn that any security controls recommended or implemented help to achieve these objectives.

AREAS OF EXPERTISE

- Industrial control systems
- Oil and gas installations
- Power stations
- Business security risk
- Building and asset security
- Supply chain security
- Personnel security
- Physical security
- UK, EU and International standards and security legislation
- Independent security assessment

SECURITY DOMAINS

Security can be divided into many different sub-domains, however for assets to be protected, and controls effective, each domain needs to be in place for every asset to create a holistic security solution.



Security Governance

This is all about the organisations approach to security, it's security culture and it's processes and procedures. It's most important functions are to ensure that security aligns with business objectives, and controls are effectively mitigating identified risks.

Information Security

Loss of information can significantly affect the viability of a business, both from loss of records to loss of competitive advantage. Risks may arise from external actions as well as insider threats.

Personnel Security

Covering security around the human resources involved in an organisations activities. Risks from insider threats, whether accidental or malicious can be some of the most frequent, and most damaging of security incidents.

Physical Security

Considering hostile actions against fixed and mobile assets as well against personnel; ranging from low-level theft, occupation by protestors, physical plant and infrastructure damage, to assault and kidnapping of personnel.

Cyber Security

As well as the risks posed by damage to IT systems and loss of data, business interruption from viruses and hacking attacks, there is also the possibility for poor cyber security to allow external parties access to asset Operational Technology (OT) systems with potentially catastrophic results.

Supply Chain

The security of supply chains, whether in physical assets, information or infrastructure, may be a significant risk to the business.

RISK MANAGEMENT

Key steps for security risk management apply irrespective of the specific aspect being considered.

Assets

Considering for example their functions, relationships to other assets, potential adverse consequences of events, to identify those assets requiring detailed assessment.

Threats

Who, why and how might assets be attacked; what are the scenarios that require managing?

Vulnerabilities

For each scenario identified, what are the existing control measures – both prevention and mitigation, and how effective are they?

Analysis

Given the likelihood, consequences and quality of the control measures, are the risks tolerable?

Mitigation

Can or should, additional measures be employed?

Monitoring

As baselines are established, assurance is required that risks continue to be managed, e.g. establishing KPIs to monitor control effectiveness, monitoring for changes e.g. to threat nature, type, etc.

APPROACHES

Adapting a structured approach allows for an objective assessment of the risks faced, maximising of business outcomes whilst prioritising expenditure to the most vulnerable or highest risks areas.

The value of experience and expert judgement should never be underestimated in assessing risks and its efficacy can be significantly increased by using appropriate risk tools to bring structure to the analysis.

The selection of a tool to assist will be influenced by several factors such as the level of risk, the desired outputs and the familiarity/certainty of the scenario. Risktec's experience allows for efficiency gains based on our knowledge of what tools work where, and what adaptions are required to allow repurposing of existing tools to new areas.

Example approaches that Risktec utilise

Gap analysis / audit

A gap analysis / audit allows you to see where your business / product meets, or falls short of recommended good practice and National / International standards. A gap analysis will allow you to prioritise improvements needed to meet your compliance objectives.

Crown Jewels

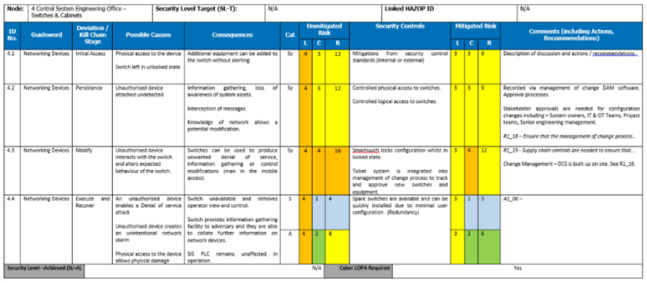
The Crown Jewels assessment aims to identify those assets that are most critical to an organisations operations. This assessment if often the start of a wider risk management process, and allows organisations to better understand their risk profile.

Maturity Assessment

As businesses grow, so does the complexity of managing information and physical security. A maturity assessment will compare your processes and procedures with recommended good practice, established maturity models and provide an understanding of your current maturity in terms of security.

Vital Area Identification

The VAI aims to identify physical areas on sites that are critical for operation, and safety of people both on site and off site. VAI is based on the methodology we use within the civil nuclear industry.



Information Security Risk Assessment:

Selecting from a variety of approaches dependent on the client (Such as ISO27005, Octave Allegro, NIST SP800-30). The Information security risk assessment is designed to give a complete picture of risks and required security controls for a wide range of information assets.

CyHAZOP

The CyHAZOP is a Risktec designed assessment methodology based on the traditional HAZOP techniques used in the safety arena. Combining the strength of this well tested technique, and tailoring it to security enables a fast, cost-effective risk cyber security risk assessment.

CyLOPA

The CyLOPA (Layers of Protection Analysis) is another Risktec designed assessment method, and takes cyber security risk assessment to the next level of detail. Utilising the outputs from the CyHAZOP process, the CyLOPA applies specific threats and scenario's against the current security mitigations to ensure they are effective against the identified threats.

Security Governance and Process Consultancy

Risk assessments on their own will not create a secure business. Risktec can also provide security governance and process consultancy across the full range of security domains (information, cyber, physical, personnel and supply chain).

Virtual Security Manager

Many small organisations do not need, or have the budget to employ dedicated security or information security managers. Risktec can offer experienced security professionals to assist organisations to set up, maintain and review their security processes, and provide guidance to the business in dealing with all aspects of security.

UK Principal Office
Wilderspool Park
Greenall's Avenue
Warrington WA4 6HL
United Kingdom
Tel +44 (0)1925 611200

Europe
Aberdeen
Derby
Edinburgh
Glasgow
London
Nottingham
Rijswijk

Middle East
Dammam
Dubai
Muscat

North America
Calgary
Houston

South East Asia
Kuala Lumpur

TÜVRheinland®
Risktec

risktec.tuv.com
enquiries@risktec.tuv.com