Corporate security

Corporate security is the security of all the operations of a company. The purpose of corporate security measures is to secure the assets important to a company, such as personnel, reputation, property or the environment, against any risks.

The main task of corporate security is to promote and ensure the competitiveness of the company and boost its productivity. Safety and security management is part of the basic management of a company. It is not a separate security function but a way to ensure the company's business security, continuity and compliance in all situations and as a natural part of the company's overall risk management.

The corporate security framework is intended to be used by all kinds of companies, from large to small. Moreover, the principles can also be applied in governmental and non-governmental organisations.

1 Identify security threats, assess risks and take precautions

Dictionaries define a threat as a potentially unpleasant, frightening or harmful event. The internationally used ISO 31000 risk management standard defines risk as the effect of uncertainty on objectives.

A company should carry out a comprehensive survey of security threats and the risks that may arise from them to the company. Threat identification, risk assessment and risk management are key to defining and sizing the objectives and means of corporate security. Safety and vulnerability analyses are part or the identification of security threats, the assessment of their significance and taking precautions against them. A company's main stakeholders and partners should be engaged in the identification, assessment and management of risks. The risk environment of a company should be continuously monitored, since security is change management. The purpose of security and risk management is not only to eliminate or reduce risks, but also to enable a company to take risks – business is based on risk-taking, but it is important that systematic efforts are made to identify, assess and manage risks. When realised, an unidentified risk can often become a disaster.

2 Increase awareness, provide training and encouragement

Areas or security improvement can be identified, for example, by looking at statistics on incidents, accidents and damage, by investigating occurred incidents and accidents and by learning from their root causes. It pays to invest in the development and implementation of high-quality security guidelines.

Personnel training, increasing security awareness and the creation of a good security culture are paramount. A company also needs a security management and communication system to ensure business continuity in all situations. Personnel and stakeholders should receive feedback on security matters and be encouraged to consider security in everything they do. Monitoring changes in both the internal and external operating environment is essential for improving security. Situation reports from and studies carried out by the authorities can be useful for understanding external changes, for example.

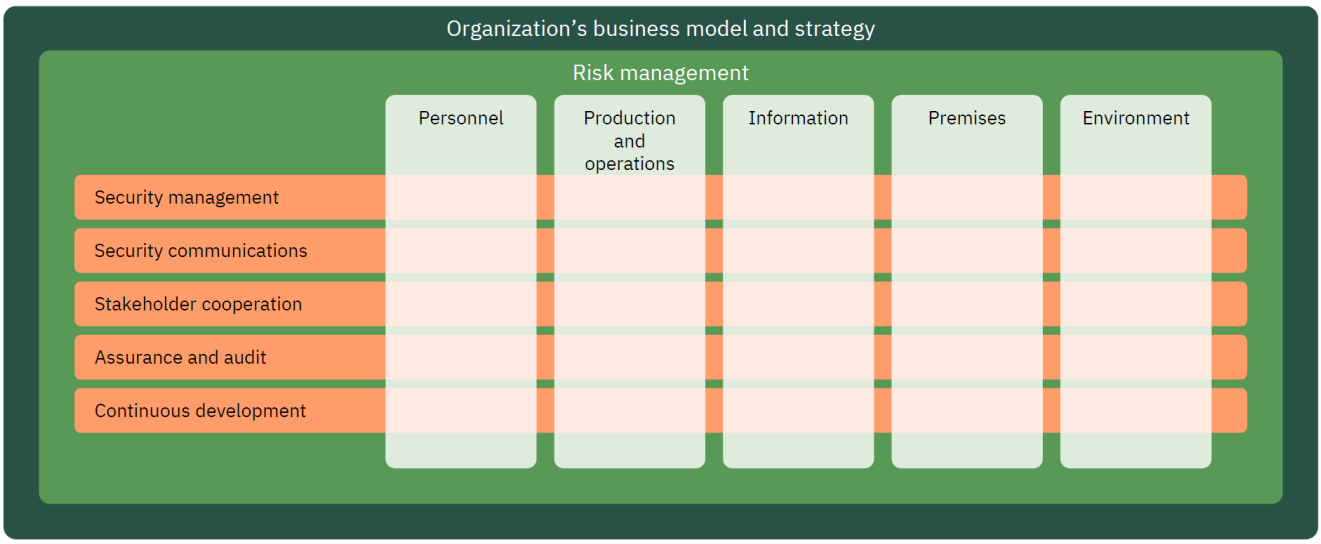
3 Aim for high quality, consult standards and collaborate with others

Security is part of a company's quality system and creates added value for its customers. A company should therefore commit to continuous development of its security measures. Security is not a permanent state but an ongoing process. The standards, quality and indicators of safety and security operations provide a company and its partners with a coherent picture of the status of the operations without a detailed presentation of the company's affairs.
Networking with others in safety and security matters is always advantageous. Cooperation with other companies, the authorities and security specialists will provide information about security threats and ensure effective action in abnormal situations, such as in accident, damage and crime prevention. Networks also often provide valuable information on which security measures work.

4 What does corporate security involve?

The Confederation of Finnish Industries (EK) has developed a corporate security framework the various sectors of which provide the means for forming an overall picture of a company's security matters and for their analysis. These sectors may overlap. Moreover, particular sectors may be more relevant than others on the basis of the industry in which a company operates and its business operations. In other words, not all the sectors are equally important to all companies. It is essential to select the areas and measures that are most relevant to your organisation. The significance of continuous development has also been considered in the framework. It is directly applicable to an international environment. However, local conditions, legislation and risks should always be analysed and taken into consideration.

Picture 1: The Corporate Security Framework



Picture 2: The Corporate Security Framework as a matrix

Personnel security

Personnel security is an integral part of corporate security. The purpose of personnel security is to guarantee the safety and capability of people by protecting them from crime and accidents. This will also safeguard the personnel resources critical to an organisation's operation.

Personnel security consists of factors such as the following:

1) Protecting employees, customers and key persons from crime and accidents	
• The safety of customers and visitors • Travel safety and working abroad	– Travel documents – Safety guidelines – Communications – Emergency services – Evacuation instructions – Insurance policies – Country and area risk classifications – Training required
• The safety of key persons	– Restricted access to contact information (e.g. personal data access restriction, address delivery restriction) – Use of safety technology – Personal protection in special cases – Threat and risk assessments and the planning and sizing of measures based on them
• The safety of home and family	– Working at home and abroad

2) Safeguarding personnel resources critical to operations	
• Deputy arrangements and substitutes • Reachability • Personal reserves for crisis periods, where possible	– Ensuring alert and communication procedures
3) Securing continuity of operations by preventing infiltration by criminals, for example	
• Careful and high-quality recruitment procedures • Security checks • Non-disclosure agreements and commitments • Drug tests • Mystery shopping (retail)	

Premises security

The offices and premises of an organisation should be protected in a cost-efficient way on the basis of risk assessments. The aim is to create an undisturbed and secure environment for working and conducting business as well as to prevent theft of information or material valuable to the organisation.

Premises security consists of factors such as the following:

1) Security classification of premises and their classification-based protection

- Creating security zones in accordance with the objects and activities to be protected (cyber and information security)
- Utilising the perimeter protection principle

- Also consider the surroundings of the target and the associated risks that affect your own activities

2) Structural security

- Environmental security planning (location, parking, loading and unloading)
- Feasibility of fencing, gates, barriers and lighting
- Locking and key management and access rights management procedures
- Intrusion protection and security structures
- Storage of high value items (safes, security and fire protection cabinets, vaults)
- Building services engineering
- Civil protection
- Accessibility

3) Security control

- Technical security surveillance (access control, crime detection/burglar alarm and camera surveillance systems)
- Control and supervision of personnel, visitors and vehicles on the site and in the premises
- Security and surveillance
- Security in meeting and conference rooms

4) Contract management

• Outsourcing and purchasing of services (including maintenance, cleaning, property and security services)
• Maintenance and service contracts, inspections
• Construction and renovation projects
• Liability and insurance

Rescue safety

Rescue safety means preventing fires and other accidents and responding rapidly and appropriately in the event of an accident.

The key is to manage accident risks through prevention, elimination and minimisation, and insurance. An organisation should also be aware of any planning and preparedness obligations and take into account rescue legislation and any instructions and regulations issued by the authorities. Furthermore, the creation of safety guidelines and regular training of personnel for dealing with accidents are paramount. Training should be provided in general civic skills such as the principles of first aid and first-aid firefighting.

Rescue safety consists of factors such as the following:

1) A contingency plan as a guiding document	
• Anticipation of dangerous situations • Workplace-specific arrangements • Outdoor areas (working or events) • Preparedness for major accidents • Threat prevention measures	– Guidelines – Structural measures – Nomination of responsible persons – Regular training – Security and access control – First aid – Rescue, repair, clearing and maintenance activities
2) Fire safety	
– Fire safety of buildings – Maintenance, regular inspections and servicing of rescue and firefighting equipment – Hot work safety	– Classification and compartmentation – Automated fire alarm system – Consideration of load-bearing structures – Rescue and firefighting arrangements – First-aid firefighting – Safety and signal lighting – Safety signs – Automated fire-extinguishing system

	– Smoke extraction – Arson prevention
3) Insurance policies	
• Property and business interruption insurance • Insurance companies' precautionary guidelines and safety clauses	

Security of production and operations

The purpose of the security of production and operations is to ensure that products and services are safe.

Security of production and operations consists of factors such as the following:

1) Product liability and safety
• Duty of care and duty to report • Supervisory bodies • Risk assessment • Marking (e.g. CE)
2) Security of services
3) Payment security
4) Safekeeping of valuable assets
5) Logistics safety (transport and storage)
• Delivery management • Specification of responsibilities
6) Networks
• Suppliers and service providers • Contract management
7) Insurance policies
• Liability insurance • Property insurance • Product insurance

- Business interruption insurance
- Project insurance
- Transport insurance

Environmental safety

The purpose of environmental safety measures is to consider ecological sustainability, and to meet and anticipate the environmental expectations of customers and society. This means taking responsibility for the environment, continuously developing processes and best practices, increasing personnel awareness, committing to the principles of legislation and standards and transparent communications.

Environmental safety consists of factors such as the following:

1) Principles of sustainability
2) Energy efficiency
3) Careful assessment of environmental impact
4) Notification and permit procedures
5) Handling and storage of dangerous substances
6) Environmental protection management system and action programme
7) Climate protection and emissions trading
8) Water and soil protection
9) Noise abatement and landscape protection
10) Chemical control
11) Waste management

Information and cyber security

Information and cyber security is an integral part of corporate security. Information and cyber security is understood broadly from a human, process and technological perspective, taking into account issues such as data confidentiality and integrity, continuity of information systems and services, physical security, supply chains and external requirements.

Technological development is rapid, and staying up to date requires constant monitoring of security methods and procedures and development of security measures. As it is impossible to achieve complete security, the best way to improve information and cyber security is to invest in ensuring the continuity of operations.

An organisation's information and cyber security consist of factors such as the following:

1) Evaluation of the significance of various information	
• Management of critical information and other assets and identification of safety-critical operations • Usability, integrity and confidentiality of information	– Certificates and verifiability
2) Classification and processing of information	
• Classification methods • Processing guidelines covering the whole life cycle of data	– Creation of a classification system – Consider all computing environments, both electronic and physical
3) Administrative information security	
• Management of user and access rights • Security checks • Security agreements • Non-disclosure agreements and commitments	
4) Data protection and privacy protection	

• Processing of personal data • Privacy protection in the workplace • Communications confidentiality	
5) Technical information security	
• Structural safety of the communication network • Detecting and preventing harmful traffic • Traceability and monitoring of operations • Regular software updates • Secure configuration of hardware and software • Network segmentation • Identity and access management • Improving user skills	– Services (email etc.) – Phones, mobile devices – Personnel competence
6) Securing the continuity of operation of systems and processes	
• Development of observation skills • Development of tolerance and resiliency • Physical security of the data processing environment • Technical and structural protection of critical physical equipment, including cross-connection cabinets • Back-ups • Recovery planning • Crisis management • Management of the continuity of other operations	– Continuous observation, log monitoring – Incident preparedness

Compliance control

With compliance control, an organisation can prevent and resolve misuse, crimes and other noncompliant behaviour that have an impact on its operation. It enables the organisation to protect its operations, personnel and assets against internal or external malicious actors.

Compliance control consists of factors such as the following:

1) Harmful events directed at operation, personnel and property	
• Observation, analysis and prevention of harmful events • Solutions and recovery • Reporting and learning	– External events – Internal events
2) Management of misdemeanour	
• Preventive actions • Exposure • Internal inspections and detections • Cooperation with the authorities • Action in the event of crime	– Planning, strategies and technical solutions – Preliminary reports – Crime cases leading to preliminary investigation – Complainant offences – Offences subject to public prosecution
3) Insurance policies	
• Crime risks	

Contingency and crisis management

Through contingency and crisis management, an organisation seeks to identify and anticipate unexpected situations and protect itself against them as efficiently as possible. Abnormal situations often come as a surprise and require quick decisions. It is therefore important that action plans exist and that the action is rehearsed.

It is important for an organisation to retain its capacity to operate and recover as soon as possible. This way an organisation can secure the continuity of its operations in all situations. Consequently, crisis management interacts closely with business continuity management.

Contingency planning as defined in emergency powers legislation is based on securing economic defence and the security of supply in extraordinary circumstances. Contingency planning is particularly important for security-critical businesses that produce services and goods critical to society as a whole, even in exceptional circumstances. However, all organisations should consider ensuring the continuity of their operations during a crisis.

1) Business continuity planning	
• Assessment of business risks and alternative plans • Production disruption or stoppage • Planning and development of resiliency	– Profitability – Agreements
2) Crisis management	
• Prevention and assessment • Action in crises • Recovery plans • Learning	– Preparedness – Acute crises – Developing crises – Timely and correct response – Communications
3) Contingency planning (preparing for extraordinary circumstances)	
• Identification of responsibilities • Planning of production and operations	– Exclusion of personnel from call to military service – Energy management

	– Stockpiling – Raw materials, machinery and equipment - Vehicle reservations if necessary – Repairs and maintenance, spare parts – Outsourcing and services

Industrial safety (including occupational health and safety)

The purpose of occupational safety and health is safe work, personnel wellbeing and, as a result, a good and responsible corporate image.

Our operations are governed by occupational safety legislation, which defines a minimum level of occupational safety practices. Occupational safety and health is based on a target-oriented action plan that lists concrete measures for the prevention of occupational health hazards.

<table>
<tr><td colspan="2">1) Safe work and personnel wellbeing – risk prevention and a good corporate image</td></tr>
<tr><td>• Workplace safety management and cooperation
• Occupational safety responsibilities
• Occupational safety and health in the workplace
• Safety of machinery, equipment and tools
• Internal traffic in the workplace
• Physical factors
• Psychosocial stress factors
• Handling of hazardous substances
• Chemical contaminants
• Personal protective equipment
• Violence and facing the threat of violence
• Occupational wellbeing
• Occupational safety and health in a workplace with multiple companies</td><td>– Employer’s occupational safety duties
– Employees’ occupational safety duties
– Employer/employee cooperation for occupational safety and health
– Occupational health services
– Functionality of the workplace community
– Competence improving activities</td></tr>
<tr><td colspan="2">2) Occupational safety organisation</td></tr>
<tr><td>• Occupational safety committee, head of occupational safety and health, health and safety representatives, labour protection ombudsmen</td><td></td></tr>
</table>

3) Action programme	
• Goals	- Continuous improvement of occupational health and safety as a matter for the whole work community – Development of working methods, conditions and tools – Engagement of collaboration partners – Developing site and workplace-specific activities – Workforce management as part of strategic management – Improvement of working capacity and environment through preventive occupational health care – Increasing safety awareness
• Training	– Induction and orientation, occupational safety cards, special tasks, activities abroad
• Indicators	– Quantitative and qualitative indicators
• Statistics	– Accident statistics – Incident reports (near misses) – Sickness absence statistics

Standards for corporate security

Standard / series of standards		
Quality management standard series	ISO 9000	
Risk management	ISO 31000 ISO 31010	
Supply chain security management system	ISO 28000	
Security and crisis resilience Environmental management standard series	ISO 22301 ISO 14000	
Information security management	ISO/IEC 27000	
Asset management standard series	ISO 55000	
Occupational health and safety management	ISO 45001	
Social responsibility	ISO 26000	
Energy management	ISO 50001	