

## Management

Senior managers need to be aware of the importance of information risk management. Practical management tools include security procedures to control access to information, the use of expertise and integrating information security and quality systems.

### Are your risks under control in these areas?

Yes No N/A

- Managers' awareness of the significance of information risks
- Identifying the most important information
- Identifying the greatest risks
- Information security policy and practice
- Information security as part of the quality system
- Access to specialist expertise
- Developing information security activities
- Other

Yes = satisfactory  
No = action or more investigation is needed  
N/A = not applicable

## Activities of personnel

Information risks are either managed or caused by the actions of people. Expertise and procedures create a foundation for success. You should provide employees with training, as well as effective tools for managing information risks, for example anti-virus software that updates computer systems automatically.

### Are your risks under control in these areas?

Yes No N/A

- Training
- Information security policy
- Clear instructions
- Procedures for staff who leave your business
- Managing user rights
- Preparing for failures and accidents
- Protecting individual computers
- Other

## Premises

Accidents and theft are key information security risks. Basic control measures include controlling access to certain areas.

### Are your risks under control in these areas?

Yes No N/A

- Exposure to accidents
- Shared occupancy of premises
- Access control
- Guarding and security against break-ins
- Partitioning of premises and access rights
- Archiving and document handling
- Access to fax machines, photocopiers and printers
- Customer areas
- Other

## Protecting information systems

Protecting electronic and paper-based information systems is one of the main challenges of information risk management.

### Are your risks under control in these areas?

**Yes**   **No**   **N/A**

- Systems management
- User rights
- Remote working
- Monitoring computer use
- Archiving and handling documents
- Managing change
- Procuring software
- Backing-up data
- Passwords
- Intranet and internet use
- Other

---

## Business relationships

Information risks in business relationships are increased by networking (linking your computer systems with those of business partners or customers and subcontractors). You should assess how secure the information security systems of third parties are, make sure there are no weak links in the network, and provide employees with training.

### Are your risks under control in these areas?

**Yes**   **No**   **N/A**

- Security of your network partners' systems
- Common rules
- Contracts
- System user rights
- Information security during negotiations
- Protecting shared information
- Other