Information technology has already permeated large parts of our everyday life: whether it be a car, telephone or heating. Without the use of IT, the majority of devices and systems are almost inconceivable. Businesses in particular use IT systems to effectively design their working processes. The Fraunhofer Institute for Secure Information Technology focuses on protecting these systems against failures, attacks and manipulations.

The Institute works for companies in various industries. Many successful projects with international partners are impressive evidence of the faithful and reliable cooperation. Our customers include HP, Software AG, SAP, Lufthansa and the Federal Office for Information Security.
SECURITY MANAGEMENT
ASSESSMENT, MONITORING, TRAINING
MOTIVATION
The German Federal Office for Information Security talks about a continued and serious threat to information technology in businesses and public authorities. Targeted attacks, as well as technical or human errors, can threaten the existence of an institution on a long-term basis. It is also becoming increasingly apparent that the protection of one’s own internal information, through the utilization of technical solutions such as firewalls or antivirus software, is no longer sufficient.

»Practical experience has shown that optimizing information security management frequently improves information security more effectively and sustainably than investing in security technology.«, according to a principle in the BSI standard 100-1 on the management of information security. In order to achieve a suitable level of security, all resources and processes of an organization must be viewed holistically and taken into consideration when developing information security concepts. This means the subject of information security will become a field of action that must be managed from a strategic perspective.

CHALLENGES
An ever-increasing number of business processes now rely on information technologies that function smoothly and correctly. At the same time, the type and scope of connections between companies is on the increase. Their value-added processes are designed to extend beyond the borders of the organization, and they communicate internally as well as externally via IP-based networks. Due to the growing requirements being placed on information technology and the increasing complexity, appropriate risk defense measures must be taken to secure business processes. Such issues are, however, increasingly related to growing compliance requirements imposed by laws and other regulations. Companies can only meet these requirements nowadays with a risk and process-oriented security management system.

Therefore, the key issue is not the resolution of a technical problem. An appropriate information security management system requires a holistic approach, strategic planning, clearly defined security principles, security measures that are implemented across all processes, targeted awareness training, and the systematic control and further development of protective measures.
OUR OFFERINGS
- Analysis and management of risks
- Advice during the planning and design of an appropriate information security management system in accordance with established standards (for example, ISO 27001/02 and IT-Grundschutz)
- Support during the development and evaluation of security policies, the analysis of assets and the implementation of appropriate security measures
- Planning and implementation of incident and business continuity management systems
- Security audits
- Support during the implementation of performance measurement systems for internal control purposes
- Planning and realization of target-group oriented training measures and awareness campaigns

CUSTOMER BENEFIT
Cost reduction
- Speeding up of process flows
- Increase in process transparency
- Secure data management
- Utilization of tried-and-tested process models
- Methodical standardization and traceability
- Resource savings through continuity
- Interoperability

Implementation of an appropriate level of security
- Focus on the latest technologies and scientific findings
- Up-to-date security level
- Assistance in preparing for certification
- Improvement through cyclical analyses

Competitive advantages
- Fast implementation of compliance requirements
- Increased customer trust through secure communication and process flows
- Strengthening of legal certainty