ISMS-Governance – edited by Dr. Bernard Bowitz , 2018

1. Rollen -Verankerung in der Organisation: Die Verantwortlichkeiten und Befugnisse für den Informationssicherheitsprozess werden vom obersten Management eindeutig und widerspruchsfrei zugewiesen. Insbesondere wird ein Mitarbeiter bestimmt, der umfassend verantwortlich für das Informationssicherheitsmanagementsystem ist (in der Regel Informationssicherheitsbeauftragter oder kurz ISB genannt)
2. Verbindliche Ziele: Die durch den Informationssicherheitsprozess zu erreichenden Ziele werden durch das Topmanagement vorgegeben.
3. Richtlinien: Verabschiedung von Sicherheitsrichtlinien, die sich mit der IT-Infrastruktur und den Informationen durch das oberste Management befassen.
4. Personalmanagement: Bei Einstellung, Bearbeitung und Abschluss der Umstellung der Mitarbeiter werden die Anforderungen der Informationssicherheit berücksichtigt.
5. Aktuality of the Knowledge: Es wird sichergestellt, dass das Unternehmen über aktuelle Erkenntnisse in Bezug auf Informationssicherheit verfügt.
6. Qualifizierung und Fortbildung: Es wird gesichert, dass das Personal seine persönlichen Fähigkeiten und Kompetenzen für seine Aufgaben qualifiziert und qualifiziert.
7. Adaptive Sicherheit: Das angestaute Niveau der Informationssicherheit wird definiert, umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst.
8. Zugänge und Zugriffsrechte werden strukturiert verwaltet.
9. Es ist eine strukturierte Datensicherung vorhanden.
10. Vorbereitung: Das Unternehmen ist in der elektronischen Datenverarbeitung vorbereitet.

In practice, the characteristics and goals of an ISMS can be defined as follows:

1. Anchoring in the organization: The responsibilities and powers for the information security process are assigned unambiguously and consistently by senior management. In particular, an employee is identified who is fully responsible for the information security management system (usually called Information Security Officer or ISB for short).
2. Binding goals: The goals to be achieved by the information security process are set by the top management.
3. Guidelines: Security Policy Approval, which defines the secure management of the IT infrastructure and information by senior management.
4. Personnel management: The requirements of information security are taken into account when hiring, training, terminating or changing the employment of employees.
5. Up-to-dateness of knowledge: It ensures that the company has up-to-date knowledge of information security.
6. Qualification and training: It is ensured that the staff understands its responsibilities and that it is suitable and qualified for its tasks.
7. Adaptive security: The desired level of information security is defined, implemented and continuously adapted to current needs and the threat situation.
8. Additions and access rights are managed in a structured way.
9. There is a structured backup available.
10. Preparation: The company is prepared for failures, failures and security incidents in electronic data processing.