

6 SECURITY & COMPLIANCE MANAGEMENT

Learning objectives

In this chapter you will learn,

- what are the basic elements of risk management,
- what we understand by compliance management,
- what are the basic elements of information security management,
- what technology can do to make E-Commerce secure,
- what are the most important legal aspects of E-Commerce.

Recommended pre-reading

- Kimwele 2014.

6.1 FOUNDATIONS OF RISK MANAGEMENT

6.1.1 THREATS OF ICT SYSTEMS

ICT systems and the information, stored in these systems, can be attacked by software viruses, hackers or espionage. People (own employees, external people) can damage our ICT systems and destroy or damage information stored in these systems.

Also faults can lead to a damage or destruction of ICT systems or information stored in these systems. Typical faults are software bugs built in during first time development or maintenance of software, may it be our own software or may it be software packages from outside software suppliers, remote maintenance, where external organizations have access to our systems or information stored in these systems, spurious actions in operations, system administration or usage of systems.

6.1.2 THREATS CATALOGUE OF BSI

BSI (Bundesamt für Sicherheit in der Informationsverarbeitung; Federal Office for Information Security), a national German Authority, which has a high reputation, also internationally, has developed the “IT Grundschutz” catalogues. The complete documentation is available in the Internet at www.bsi.bund.de/grundschutz (as well in German as in English).

BSI has published a comprehensive list of threats for ICT (see table 12).

<ul style="list-style-type: none"> • Fire • Unfavourable climatic conditions • Water • Pollution, dust, corrosion • Natural or environmental disasters • Major events in the environment • Failure or disruption of power supply, communication networks, mains supply (power, telephone, cooling, heating or ventilation, water and sewage, supply of fire-fighting water, gas, alarm and control systems (e.g. for burglary, fire, housekeeping control engineering), intercoms) • Failure or disruption of service providers • Interfering Radiation (In Germany, regulations in this subject area are stated in the Act for the Electromagnetic Compatibility of Resources) • Intercepting of compromising emissions or information/espionage • Eavesdropping • Theft or loss of devices, storage media and documents • Bad planning or lack of adaption • Disclosure of sensitive information • Information or products from an unreliable source 	<ul style="list-style-type: none"> • Manipulation of hardware or software or information • Unauthorized access to ICT systems • Destruction of devices or storage media • Failure or malfunction of devices or systems • Lack of resources • Software vulnerabilities or errors • Violation of laws or regulations • Unauthorized/incorrect use or administration of devices and systems • Abuse of authorizations • Absence of personnel • Attack • Coercion, extortion or corruption • Identity theft • Reputation of actions • Abuse of personal data • Malicious software • Denial of service • Sabotage • Social engineering • Replaying messages • Unauthorized entry to premises • Data loss • Loss of integrity of sensitive information
---	---

Table 12: BSI threats catalogue

Each organization should build and maintain a list of specific threats. This list should be updated periodically. The discussion of threats is a major management issue.

6.1.3 DEFINITION OF RISK

We start with a definition:

A risk is the extent of loss, which may happen if a threat occurs.

Due to the British Information Security Breaches Survey 2015 the average cost of the worst single breach suffered by organizations surveyed has gone up sharply for all sizes of business. For companies employing over 500 people, the ‘starting point’ for breach costs – which includes elements such as business disruption, lost sales, recovery of assets, and fines & compensation – now commences at £1.46 million, up from £600,000 the previous year. The higher-end of the average range also more than doubles and is recorded as now costing £3.14 million (from £1.15 in 2014).

6.1.4 MEASUREMENT OF RISKS

Single risk

The standard approach (Ackermann 2013, p. 14) is, that the risk value is expressed by the product of the probability of occurrence and the expected amount of loss. The amount of loss is considered as a random variable. Thus it would be “more” correct to define the risk value as the expectation value of the random variable “amount of loss” with its underlying probability distribution.

The challenge of this definition is, that we have to find out the probability distribution of the amount of loss. Thus it is a good practice not to work with specific figures but just to list the identified risks and categorize them e.g. by low/medium/high.



“I studied English for 16 years but...
...I finally learned to speak it in just six lessons”
Jane, Chinese architect

ENGLISH OUT THERE

Click to hear me talking before and after my unique course download

Risk portfolio

A very naïve approach to value the total volume of risks of a management object (e.g. a total organization or a portfolio of specific objects or a specific E-Commerce system) is the number of identified risks. Many people think, that such an approach is too simple but it is much better to work with such a very simple list and to discuss about the risk situation than to ignore the risks.

A more “sophisticated” approach to value the total volume of risks is to build the sum of expectation values of the identified single risks. This assumes that the risks in the sense of probability theory are totally independent from each other, which obviously is not correct. However, otherwise we would have to have a model of the interdependencies between the different risks.

There are further methods to calculate the total value of a risk portfolio but they all need a lot of mathematics and probability theory (Ackermann 2013).

6.1.5 RISK ANALYSIS

A risk analysis according to ISO/IEC 27001 (IEC = International Electro-technical Commission, ISO = International Organization for Standardization) has to run through the following steps:

- Inventory of information assets,
- Determination of protection requirements,
- Identification and assignments of threats (e.g. supported by the BSI threats catalogue),
- Identification and assignment of weaknesses,
- Determination of potential extent of loss,
- Determination of probabilities of loss occurring,
- Determination of risks,
- Decision on acceptance of risk,
- Selection of safeguards,
- Documentation of residual risks,
- Documented approval of management.

6.1.6 BASIC RISK MANAGEMENT STRATEGIES

We see a lot of threats, which could lead to a damage or destruction of ICT systems. Management has to deal with it. Though the variety of threats and corresponding risks is extremely large there are only four basic risk management strategies:

- **Avoidance of threats**, which means that you are able to completely eliminate the threat of your management object. Normally you will not be able to completely avoid a threat.
- **Reduction of threats**, which means that you lower the risk resulting from that threat. In most cases you will be able to reduce the potential amount of loss. Whether you can change the probabilities of occurrence can only answered if the specific situation is known.
- **Transfer of risks** to a third party, e.g. insurance. This means that the third party will take over and pay the amount of loss if the risk occurs. You will have to pay a fee for that.
- **Acceptance of threats**, which is selected when you do not have any chance to change the situation.

6.1.7 BASIC RISK MANAGEMENT TASKS

Obviously it is not sufficient to know the risks. Management has to actively work on it. This does not only include the application of the risk management strategies listed above. They also have to be prepared for the situation when a risk occurs. This leads to the following elementary management tasks:

- Avoid, reduce or accept threats. Transfer risks, if this is the best strategy.
- Know what must be done when a risk occurs.

The latter leads to **business continuity management**, which has to supplement risk management.

6.1.8 BUSINESS CONTINUITY MANAGEMENT

The main question is: How good is business prepared to get back to work if some parts of the organization break down?

Main processes are:

- Prepare for emergency situation (provide documentation, train people, run emergency exercises),
- Initiate and build up emergency organization (alert management, disaster management team),
- Run emergency organization/processes (if a disaster occurs),
- Re-install regular organization/processes,
- Get back to regular organization/processes,
- Stop and break down emergency organization/processes.

Business continuity management includes **ICT continuity management**, of course. But it is much more than preparing the ICT systems for continual operation. Business may break down, even if no ICT system is damaged or out of operation (e.g. due to disease of employees). In many cases risks occur which lead to a breakdown of ICT systems as well as other business resources, e.g. fire in an office building.

This e-book
is made with
SetaPDF



PDF components for PHP developers

www.setasign.com

6.2 COMPLIANCE MANAGEMENT

We start with the definition of compliance:

In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations.

Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

6.2.1 RELEVANCE OF COMPLIANCE MANAGEMENT

The reason for the high attention of management towards compliance (management) is, that if any part of an organization is not compliant then there is a significant risk for that organization. Missing compliance can lead to punishment through governmental authorities and a loss of reputation in the business world.

6.2.2 INTEGRATION INTO GRC MANAGEMENT

Governance, Risk and Compliance (GRC) are three pillars that work together for the purpose of assuring that an organization meets its objectives....

Governance is the combination of processes established and executed by the board of directors that are reflected in the organization's structure and how it is managed and led towards achieving given objectives.

Risk management is predicting and managing risks that could hinder the organization to achieve its objectives.

Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered to be a key factor to an organization's success.

6.3 INFORMATION SECURITY MANAGEMENT (ISM)

Let us start with the definition of security:

Security is a status where a person, a resource or a process is protected against a threat or its negative consequences. Information security means the security of our information assets.

6.3.1 PROTECTION GOALS

With respect to information there are several common protection goals:

- **Authenticity:** Realness/credibility of an object/subject, which is verifiable,
- **Integrity:** Data cannot be manipulated unnoticed and without proper authorization,
- **Confidentiality:** Information retrieval not possible without proper authorisation,
- **Availability:** Authenticated and authorized subjects will not be restricted in their rights without proper authorization,
- **Obligation:** A transaction is binding if the executing subject is not able to disclaim the transaction afterwards,
- **Authorization:** Power and right to conduct an activity.

Information security management is not only an issue for the ICT department. It must be considered by all management areas and management levels.

6.3.2 OBJECTIVES OF ISM

The overall objective of information security management is to protect the information assets of the organization due to the above mentioned protection goals. This leads to specific ISM objectives:

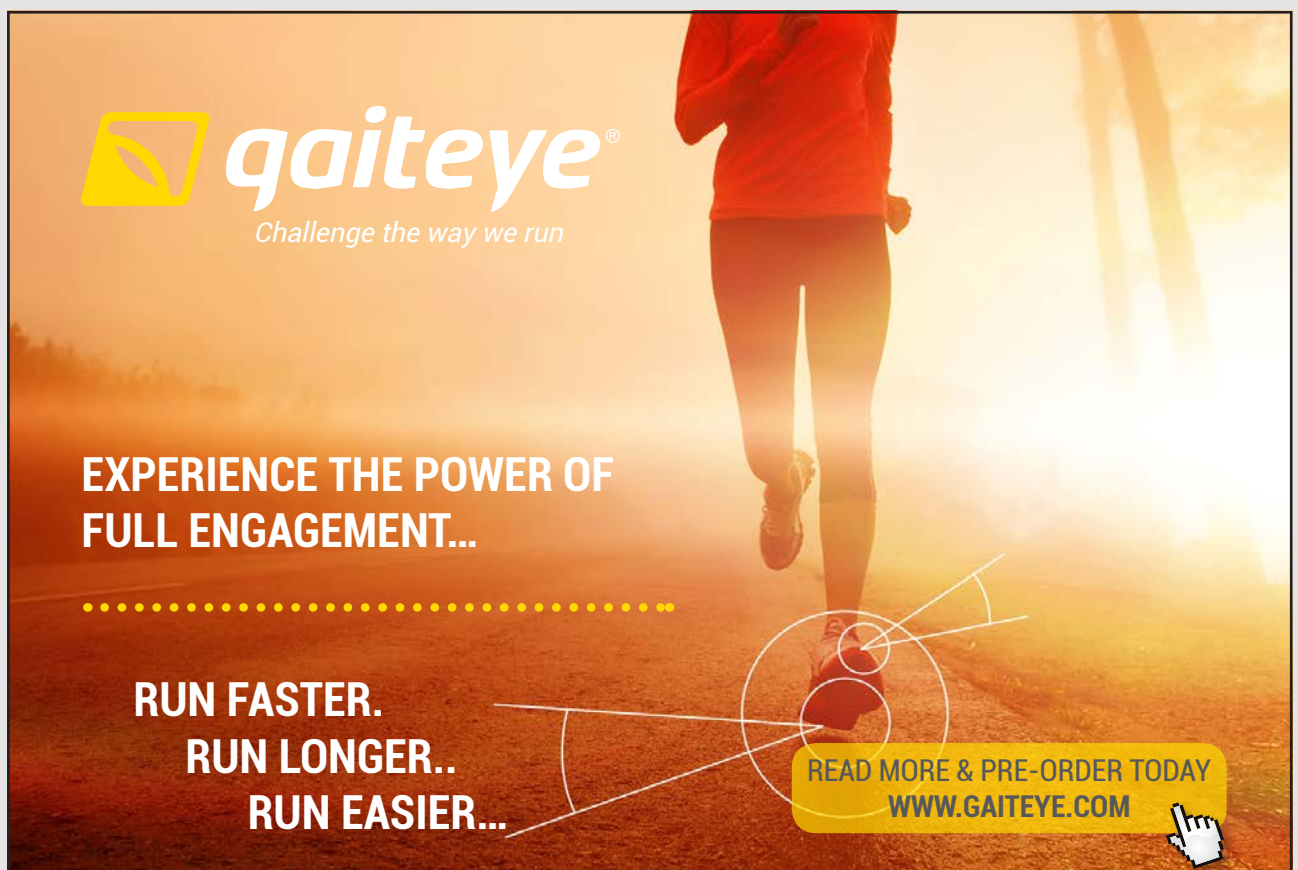
- Fulfil organizational duties: give precise, binding and complete orders to your people; select people carefully with respect to duties and responsibilities; check what your people do in the daily operation; inform your people about laws, rules and instructions they have to follow.
- Build an efficient and transparent organization.
- Build a professional security, continuity and risk management.
- Increase efficiency with general and unified rules and methods.
- Reduce time consumption and costs with security and security audits integrated into business processes.
- Run a continual improvement process to minimize risks and maximize economic efficiency.

- Have a good reputation at customers, shareholders, authorities and the public.
- Parry liability claims and plead the organization in criminal procedures.
- Be integrated into the corporate security management system.

6.3.3 THE ISM PROCESS

The information security management process has four major steps, which are subsequently described:

- **Initialize:**
 - Understand information security requirements,
 - Build information security policy to define overall security objectives,
 - Establish information security representative and organization,
- **Analyse and develop** information security strategy:
 - Determine protection needs,
 - Analyse threats,
 - Analyse risks,
 - Deduce information security requirements.



gaiteye[®]
Challenge the way we run

**EXPERIENCE THE POWER OF
FULL ENGAGEMENT...**

.....

**RUN FASTER.
RUN LONGER..
RUN EASIER...**

**READ MORE & PRE-ORDER TODAY
WWW.GAITEYE.COM**

- **Plan and implement:**
 - Define, what has to be regulated,
 - Define, how it should be regulated (comprehensively or detailed),
 - Prepare information security concepts,
 - Define policies and guidelines,
 - Prepare for implementation projects,
 - Run initial trainings,

- **Operation and monitoring:**
 - Administer activities and manage documentation,
 - Run trainings and increase security awareness,
 - Identify key performance indicators,
 - Conduct audits/assessments.

6.3.4 ISM ACTIONS

Information security management includes a great variety of activities, which can be categorized due to the focus of the different activities.

Organization:

- Establish access profiles.
- Provide and file task descriptions for IT administrators and information security representatives.
- Conduct administration of keys.
- Run evacuation and emergency exercises.

Technique:

- IT security: Implement and operate firewalls, virus scanner, spam filter, encryption software.
- Facility management: Install access control system, door locks, fire detection system, burglar alarm system, emergency power generator, uninterruptable power supply (UPS).
- Safety of buildings: Install fences, observation cameras.

People:

- Conduct a professional recruiting and include security aspects.
- Do a proper placement of employees (duties of employees).
- Ensure a careful adjustment to the job.
- Establish a continuous supervision: rising of awareness, training.
- Conduct a professional separation of employees.

6.3.5 ISM DOCUMENTS

A professional information security management will lead to several documents:

- Information Security Process Framework,
- Information Security Declaration:
 - Requirements to information security, continuity and risk management with respect to risk capacity, risk propensity und aspired security level: corporate principles, corporate objectives, requirements of stakeholders, requirements through laws, regulations and standards,
 - Description of ISM process with continual improvement process, organization and responsibilities,
 - Responsibility of top management,
 - Integrated, transparent and auditable process model: information security principles, processes and organization, technical resources, employees and external experts, life cycle, communication, training, motivation, raising of awareness, surveys,
 - Commitment of employees,
 - Penalties,
- Information security concepts (e.g. job safety, human resources, facility management, IT security),
- Subject oriented concepts (e.g. virus protection, network, E-Mail or IT processes),
- Policies/guidelines:
 - End user policy incl. password policy and Internet policy,
 - Communication policy incl. communication with external parties and E-Mail policy,
 - Access authorization for buildings and rooms (incl. request and authorization process),
 - Firewall policy,
 - Backup policy incl. off site storage of backup data,
 - Access authorization for IT systems and networks (incl. request and authorization process),
 - Access protection of data (incl. request and authorization process),
 - Encryption policy,
 - Emergency plan (incl. alerting, emergency operation, transformation to regular operation),
 - Configuration of security related facilities,
 - Fire protection,
 - Sourcing policy.

6.4 TECHNOLOGY

Important technologies for ISM are data encryption and smart cards.

6.4.1 DATA ENCRYPTION

Steganography

Objective is to hide the existence of a message. Specific applications of this technology are the transfer of messages or digital watermarking.

Examples of steganographic methods are special terms and phrases in text documents, sympathetic ink or hiding of information in image files through setting of single pixels.

A major problem with steganography is the vulnerability to changes of data, e.g. compression. Information saving data compression formats are GIF and BMP.

Symmetric encryption

The communication protocol runs as follows: A and B define a common secret key. Then A encrypts the message and sends the message to B. B receives and decrypts the message through applying the key.

wethrive.net

How to retain your top staff

FIND OUT NOW FOR FREE

DO YOU WANT TO KNOW:

- What your staff really want?
- The top issues troubling them?
- How to make staff assessments work for you & them, painlessly?

Get your free trial

Because happy staff get more done

Established methods are:

- DES = Data Encryption Standard,
- AES = Advanced Encryption Standard,
- IDEA = International Data Encryption Algorithm (Patents by Ascom AG, Switzerland).

The central problem with symmetric encryption is the secure exchange of the key between A and B.

Asymmetric encryption

The communication protocol runs as follows: A and B generate a pair of keys (each of them consisting of a public key and a private key. Both public keys are published and accessible by any third party. If now A wants to send a message to B, A encrypts his message with the public key of B and sends the message to B. B receives the message from A and decrypts it with his private key.

The actually used method is the RSA method (RSA = Ronald Rivest, Adi Shamir, Leonhard Adleman) named after the three gentlemen who published this method in 1978. Obviously 10 years earlier this method had already been developed by the British secret service.

There are two weaknesses. The first: The public key must be authentic. This can or must be ensured by appropriate organizational elements. The second: Asymmetric encryption could be knocked out if the attacker placed his key as the public key of another person or organization. So the sender would think that he uses the public key of his addressee. He encrypts the message and the attacker could decrypt it with his own private key.

Hash function

Hash functions are considered to be one step towards an electronic signature. By using specific algorithms a hash function generates a document specific hash value. That is a high-value number assigned to the actual document. If the document is modified later on it gets another hash value. However, because the hash function concentrates the document in one single number though it is a very big number, there is a residual probability, that the hash value of the changed document is identical to the hash value of the document before the modification or manipulation. There is also a residual probability that two different documents get an identical hash value.

But these residual probabilities are very low, if the length of the hash value is great enough (The hash function must be collision resistant). The SHA-1 (Secure Hash Algorithm) generates 160 bit hash values. Since 2007 the NIST recommends the use of one of the SHA-2 methods, which generate hash values of 256, 384, or 512 bits. An alternative hash function is MD5 (Message Digest) with a hash value of 128 bits. However, this method is not longer recommended, because it is relatively easy to find different messages having the same hash value.

Electronic signature

There are some requirements for an electronic signature, which have their origin in traditional signatures, of course. First it has to proof the identity of the signer doubtlessly. The signature shall be applied once only and valid only in connection with the original document. The signed document must not be changed afterwards; a change must be visible. The signature must not be rejected. The signer must not deny that he has signed the document.

However, there are some advantages of the electronic signature against the traditional signature. The content of the document can be kept secret. The document can be better protected against later manipulation through the use of hash functions. The validity of the signature can be limited in time with time stamps. And finally signatures can be stored at a trustworthy organization so that the signer can be identified reliably.

The communication protocol runs as follows: The signer of a document creates a pair of keys and stores the public key in a public database. He encrypts the document with his private key and sends the document to the receiver. The receiver gets the public key from the public database and decrypts the documents (he “verifies” the signature).

The reader should be aware of the fact that the mathematical algorithms for electronic signatures are the same as for asymmetric encryption. But they are used in a different way.

The German law on electronic signatures differentiates between three levels of electronic signatures:

- **Basic electronic signature:** The signature is added to the document and is used to authenticate it. The provider of the signature is not liable for correctness and completeness of certificate data. An injured party has to prove that there is damage.

- **Advanced electronic signature:** This signature is only assigned to the owner of the signature key. It facilitates the identification of the owner of the signature key. The advanced electronic signature is generated by means, which are under full control of the owner of the signature key. It must be tied to the document in a way so that a later change of the document is recognized.
- **Qualified electronic signature:** This signature is based on a qualified certificate, which is valid at the time of generation of the signature. It has been generated with a so-called secure signature generation unit. The certificate assigns a signature check key to a specific person and confirms his/her identity. The certificate only is a qualified certificate if it has been provided by an accredited trust centre, has been electronically and qualified signed and contains some specific information, which is defined in the law. To store signature keys and to generate qualified electronic signatures secure signature generation units have to be used. The used technical components have to be accredited by specific German authorities.



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

How do those technologies work together, if you want to send a message to your partner? First you have to sign the message. Secondly you apply a hash function to the signed document so that the receiver can check, whether the document he has got is the one you have sent. And thirdly you encrypt the signed and hashed document so that no third party can read the document.

Public Key Infrastructure (PKI)

A PKI is built and operated for a secure generation, distribution, certification, storage/archiving and deletion of (encryption) keys.

The most important term is the certificate. This is a digital confirmation that a public signature key is assigned to a specific person or organization. There is a world wide standard for certificates: X.509v3. Thus a PKI is an infrastructure to generate and manage certificates. There is a business standard for PKI. It is PKCS (Public Key Cryptography Standard), which is provided of the company RSA who are the owners of the RSA encryption method.

Elements of a PKI are:

- CA (Certification Authority): Publication and call-back of certificates,
- RA (Registration Authority): links key and person,
- CPS (Certification Practice Standard): rules for issuing and managing of certificates,
- CRL (Certification Revocation List): list of blocked keys,
- Directory of issued certificates.

However, there are some problems and challenges in building and operating a PKI. First significant costs occur and several organizational issues have to be solved. Secondly a cooperation of different PKI's is a real challenge. But how can two communication partners verify their certificates if they do not operate within the same CA?

6.4.2 SMART CARDS

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Usually smart cards are made of plastic. The application focus is the proof of identity.

Smart cards can provide identification, authentication, data storage and application processing. They may provide strong security authentication for single sign-on (SSO) within large organizations.

Smart cards contain a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provide security services (e.g., protects in-memory information). They communicate with external services via card-reading devices, such as ticket readers, ATMs, DIP readers (to “dip” the card into a chip-enabled reader), etc.

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RFID (at data rates of 106–848 kbit/s). These cards require only proximity to an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card’s electronics.

Dimensions of smart cards are similar to those of credit cards. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters (3.370 in × 2.125 in). Another popular size is ID-000, which is nominally 25 by 15 millimeters (0.984 in × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimeters (0.030 in) thick.

PCI Data Security Standard (Payment Card Industry)

Mandatory regulations for the applying firms are:

- Installation and periodic updates of a firewall to protect data,
- No use of pre-given values for system passwords and other security parameters,
- Protection of stored credit card data, card and transaction data shall not be stored needlessly, e.g. complete credit card number or card number check digit,
- Encrypted transfer of cardholder data and other sensitive data in open networks,
- Use and periodic update of anti virus software,
- Development and use of secure systems and applications,
- Restriction of access to cardholder data to pure business reasons,
- Assignment of a unique identification code to each person who has access to the computer system,
- Restriction of physical access to cardholder data,
- Monitoring and documentation of all accesses to network resources and cardholder data,
- Periodic checks and assignments of the security systems and processes,
- Providing a company guideline for information security and ensuring, that it is practiced by employees and business partners.

The steps of the **certification process** for merchants are:

- Registration of merchant at credit card organization,
- Self assessment with respect to the compliance with the PCI rules and standards (questionnaire),
- Security scan (external security inspection conducting attacks to the systems of the merchant),
- Security audit (inspection of the merchant facilities and assessment on-site of the compliance with security rules and standards).

Certifying organizations have to be accredited. A list of accredited organizations is available at www.pcisecuritystandards.org. Registration is free. However, the costs of inspections are several thousands of EUR.

SET (Secure Electronic Transaction)

SET is a credit card based online payment system developed by Visa and Microsoft, supported by MasterCard, IBM, Netscape und CyberCash. The first official version was launched in May 1997. SET aims at enabling a secure electronic payment. It is an expensive system and has low acceptance in the markets.

© 2013 Accenture. All rights reserved.

be > your degree

Bring your talent and passion to a global organization at the forefront of business, technology and innovation. Discover how great you can be.

Visit accenture.com/bookboon

Be greater than.
consulting | technology | outsourcing

accenture
High performance. Delivered.

Requirements:

- Ensure confidentiality of order and payment information,
- Ensure integrity of transferred data,
- Authentication whether card holder is true owner of credit card account,
- Authentication whether customer communicates with an authentic merchant,
- Use of a secure protocol, which is independent from the security services of the communication protocols.

Process:

- Ordering/purchase request:
 - Customer sends an initial message (initiate request),
 - Request is answered by the supplier through sending a signed answer and also the certificate of the supplier and the certification of the supplier's bank (initiate response),
 - Customer checks both certificates and the supplier's signature at the certification office,
 - Customer creates the order and the order to pay and creates from both messages a dual signature,
 - The order to pay is additionally encrypted with the public key of the supplier's bank so that the supplier is not able to read it,
 - Finally all messages are sent to the supplier together with the certificate of the customer,
- Acceptance of the order to pay (payment authorization):
 - The supplier sends a request to his bank,
 - This request is signed and encrypted by the supplier. Certificates of supplier and customer as well as customer's order to pay are added,
 - The bank of the supplier checks all certificates and sends a corresponding request to the customer's bank via the bank's network,
 - The answer is signed by the supplier's bank and encrypted with the public key of the supplier,
 - Furthermore a so-called "capture token" is created for the subsequent clearance. This is encrypted with the public key of the supplier's bank and can only be read by this bank later on,
 - The encrypted answer and capture token are transferred to the supplier. He checks the certificates and the answer of the customer's bank, stores the capture token and delivers the goods or services to the customer,

- Clearance (payment capture):
 - The supplier sends the capture request to his bank complemented with his certificates and the payment amount,
 - This request is checked by the supplier's bank and a corresponding message is sent to the customer's bank (clearing request),
 - Subsequently a signed and encrypted acknowledgement is forwarded to the supplier (capture response), who can store it for his purposes.

6.5 LEGAL ASPECTS OF E-COMMERCE

The following considerations are made on the background of the situation in Germany resp. in European Union. Many questions will be the same or similar in other legal environments. However, some issues may be considered differently in other legal environments.

6.5.1 RELEVANT LAWS

In the European Union an E-Commerce-recommendation (Recommendation 2000/31/EG; ECRL) has been provided as of 08.06.2000. This had to be transferred to national laws in the European Union.

In Germany there are several other laws being relevant for E-Commerce:

- Telecommunications Act (Telekommunikationsgesetz (TKG)),
- Telemedia Act (Telemediengesetz (TMG)),
- Data privacy laws (on federal and state level),
- Signature law (with a Signature Act, a Signature Policy and a Signature By-Law),
- Administrative procedures laws (e.g. notification reform act, Formal requirements adjustment act, justice communications act),
- Antitrust and public procurement laws (with contracting rules and a law against restraints on competition).

In general there is the question which national law has to be applied when making E-Commerce. Basically there is a free selection of the law system, which is chosen as the basis for contracts. However, there is one exception (in Germany): Contracts with consumers. The protection of the consumer's state of residence cannot be revoked.

In the European Union the freedom to offer professional services in other countries (of the union) is protected by law.

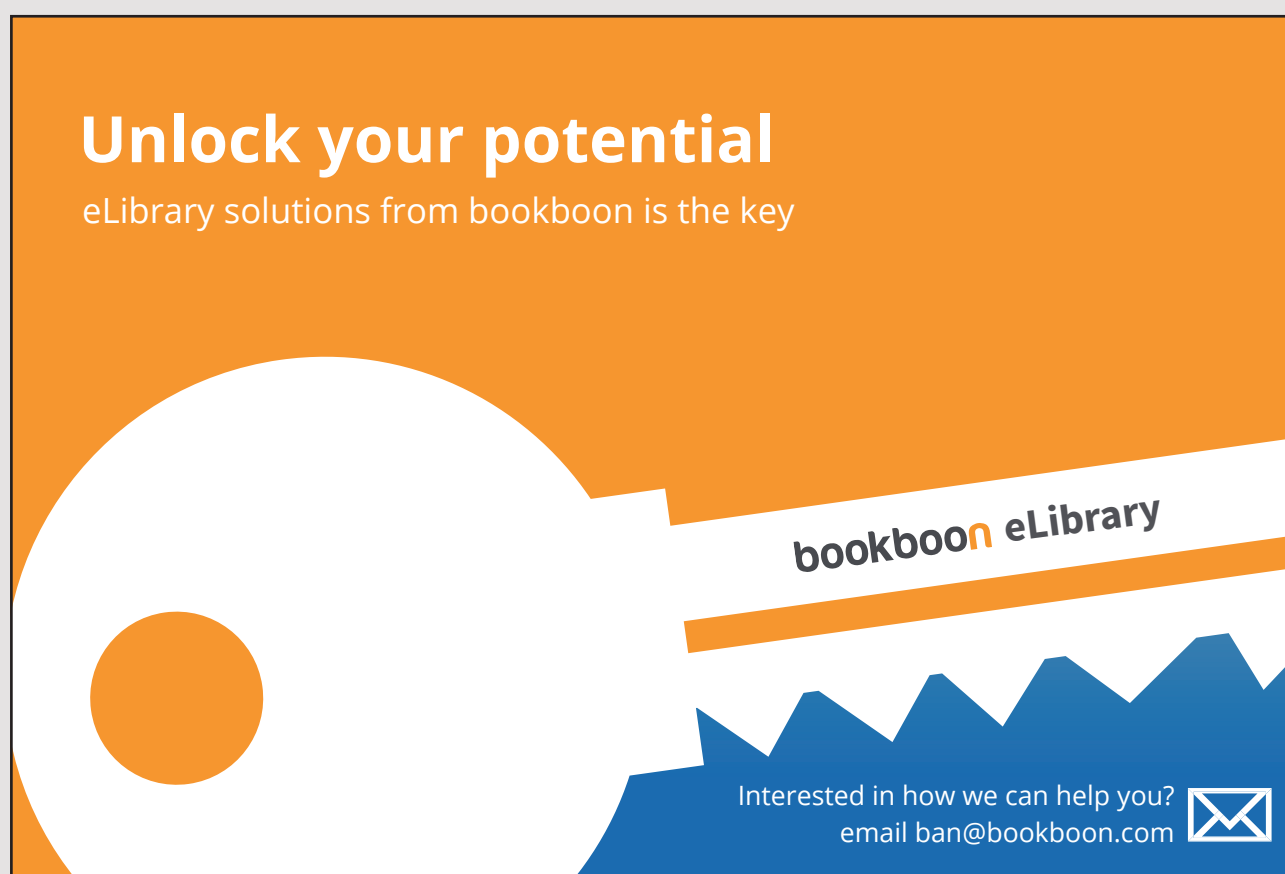
6.5.2 DOMAIN RIGHT

Domains are assigned via ICANN (Internet Corporation for Assigned Names and Numbers) and subsidiaries.

The domain **.eu** was started in 2005. In the beginning it was only available for owners of registered trademarks. The assignment follows the first-come-first-serve-principle. Strong formal procedures have been established.

The highest reconciliation instance is the Czech court of arbitration. An applicant is not only obliged to present his own judicial position but also has to expose that the opposite party does not have a reasonable interest in the considered domain or has registered it in bad faith (Bad faith is assumed if the domain has not been used for at least 2 years). No dispute action is accepted (if a third party claims a stronger interest in the considered domain).

The domain **.de** has been assigned since 1996 through DENIC e.G., the German chapter of ICANN.

The advertisement features a large white key shape on an orange background. The key's shaft is a white banner with the text 'bookboon eLibrary' in black and orange. The key's head is a white circle with an orange circle inside. Below the key, a blue jagged line represents a mountain range. At the bottom right, there is a white envelope icon and the text 'Interested in how we can help you? email ban@bookboon.com'.

Unlock your potential
eLibrary solutions from bookboon is the key

bookboon eLibrary

Interested in how we can help you?
email ban@bookboon.com

Only civil law settlements are accepted. There is no trademark verification at registration. Dispute actions are not possible. The domain assignment is fixed for at least one year (to avoid domain grabbing).

6.5.3 IDENTIFICATION OF PROVIDER/IMPRESSUM

In Germany there is a clear legal obligation for all (!) providers of websites (organizations as well as individuals) to identify themselves in a specific way. The obliged elements of provider identification are:

- Complete name and address (no P.O.Box allowed),
- Telephone number,
- E-Mail address,
- Inspecting authority if business needs a state licence,
- Value added tax identification number (if given),
- Business identification number, if given,
- Commercial register number, if provider runs a registered business,
- Similarly for registered cooperatives and registered associations.

For organizations the top representatives must be reported. There are specific obligations for specific businesses.

6.5.4 LIABILITY FOR DISTURBANCE

A disrupter is a person or organization being involved in causing damage (see BGB § 1004; BGB = German Civil Code). His specific contribution is not relevant. Accountability is assumed even if you let a third party cause damage though you would have been able to prohibit it. This accountability is always given even if you are not aware of an illegal activity.

However, auditing duties have to be reasonable. Preventive auditing is requested but not clear. In 2016 pure conveyance of information has been allowed by the German Telemedia Act, if just the technical capability is provided, e.g. WLAN services in a public area are provided.

6.5.5 CRIMINAL LAW

Due to German criminal law (StGB § 9) an action has been conducted where the actor did it or where he wanted to do it or where the result of his action occurred or was expected by him to occur.

What does this mean? If somebody provides racist content in German via a server running in a foreign country then the German prosecutor and German police have to become active because of the German language they assume that the actor wanted to address his ideologies to a German audience and wanted to have an effect in Germany.

6.5.6 RIGHTS OF EMPLOYEES

In Germany the employer is the owner of his Web and mail system. An employee is not allowed to use it for private reasons if there is not an explicit permission of the organization.

If the private use is permitted then the employer is considered to be a professional telecommunication services provider. He is not longer allowed to check mails because the privacy of correspondence, posts and telecommunications dominates the employer's right to check the activities of his employees. Therefore the explicit prohibition of private use of any system of the organization is strongly recommended.

6.6 EXERCISES

6.6.1 QUESTIONS FOR YOUR SELF-STUDY

Q6.01: Why is the access provider not able to guarantee successful access to any computer attached to the Internet?

Q6.02: Why could we see the criminal liability of search engine operators differently from access providers?

Q6.03: Review the threat catalogue of German BSI. Which threats are especially relevant for E-Commerce? Do you see further threats, which are not listed here?

Q6.04: List internal rules of a firm, which have to be followed in running the firm's online shop.

6.6.2 PREPARATION FOR FINAL EXAMINATION

T6.01: Please define the term “security”.

T6.02: Please list the four risk management strategies!

T6.03: Some people tell, that employees are one of the greatest threats of every organization. Why do they come to that opinion?

T6.04: Let two organizations have an encrypted data exchange. Describe the communication protocol if they decide to use asymmetric encryption.

T6.05: Describe the communication protocol if an electronic signature is used.

T6.06: What is the objective of business continuity management?

6.6.3 HOMEWORK

Find out specific risks within E-Commerce. Do all participants have similar risks? Which risk management strategies do they need?

ie
BUSINESS SCHOOL

CHARLES
FINANCIAL SERVICES

MARIA
CONSULTING

NICK
TECHNOLOGY

MATTHEW
MANUFACTURING

SARAH
RETAIL

AFTER GRADUATION, MIM STUDENTS
WORK IN A VARIETY OF SECTORS

MASTER IN MANAGEMENT

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS
Av. Experience: 1 YEAR
Language: ENGLISH / SPANISH
Format: FULL-TIME
Intakes: SEPT / FEB

5 SPECIALIZATIONS
PERSONALIZE YOUR PROGRAM

INTERNATIONAL
FACULTY PROFILE

55 NATIONALITIES
IN CLASS

www.ie.edu/master-management | mim.admissions@ie.edu | [f](#) [t](#) [i](#) Follow us on IE MIM Experience