DIGITALIZATION – PLANNING

BORUT JEREB
University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

E-business plays a crucial role in the modern digital environment, transforming business practices and opening new possibilities. The model of the e-business value chain is presented, encompassing supporting processes, the value chain, and technological solutions. Additionally, various e-business approaches are addressed, including e-marketing, e-documentation, e-payments, and e-customer management. The importance of information and cyber security in the contemporary business environment is emphasized. Safeguarding the digital landscape becomes crucial, with information security covering the protection of information, while cyber security addresses the protection of digital systems from cyber threats. Both disciplines are essential for maintaining trust and security in e-business. The article concludes with the presentation of IT risk management using the ISO/IEC 27005 standard.

DOI
https://doi.org/10.18690/um.fl.2.2026.1

ISBN
978-961-299-074-9

Keywords:
digitalization,
e-business,
information security,
cyber security,
IT risks

University of Maribor Press

1 Introduction

In the rapidly changing environment of the digital age, electronic business or e-business has emerged as a paradigm that is changing the way organizations conduct their operations and communicate with stakeholders. For businesses, e-business refers to the use of digital technologies and the Internet to simplify and improve various business processes from buying and selling goods and services to managing internal operations and collaborating with partners. In commerce, unlike traditional business models, e-business transcends geographical and time constraints by providing a global platform for trade.

E-business encompasses a wide range of online activities, including e-commerce, e-marketing, e-supply chain management, and e-procurement. The integration of technology not only enables more efficient and cost-effective business practices but also opens up new opportunities for innovation and market adaptation.

Key elements of e-business include establishing an online presence, conducting secure electronic transactions, leveraging data analytics for informed decision-making, and adapting to an ever-changing digital environment. A company's success in an e-business environment depends on its ability to create seamless and engaging customer experiences, to establish trust and security in online transactions, and to leverage insights gleaned from (often massive) data to stay competitive in a dynamically changing marketplace.

As technology continues to advance and change, e-business will play an increasingly important role in shaping the future of business within and between companies – especially when it comes to supply chains. Whether you're a startup or an established multinational, understanding and harnessing the power of e-business is key to succeeding in the digital economy. In doing so, companies must not only overcome technological challenges but also the changing expectations of connecting with digitally savvy employees and customers inside and outside the company.

In the following, we want to guide the reader on a path to becoming able to:

- review and analyze that part of the business in its environment that would make sense to digitize,

- recognize the importance of information and cybersecurity security and be able to plan them in the role of the middle management
- critically evaluate IT risks in the role of the middle management.

2 E-business

E-business is a comprehensive approach to conducting business processes using electronic means. This also applies to the implementation of business processes that support the implementation of logistics processes. E-business encompasses a wide range of activities that leverage digital technologies to optimize operations, improve customer experience, and increase overall business efficiency. E-business also encompasses both the internal and external interactions of organizations and seeks to transform traditional business practices by connecting electronic systems and communication channels. The concept of e-business is changing the way organizations conduct their operations, communicate with customers, and create value. It constitutes a comprehensive shift toward conducting business processes using electronic means, ultimately driving efficiency, innovation, and global reach.

The origins of e-business date back to the early days of the Internet. With the emergence of e-business (e-commerce), the idea of buying and selling products online emerged. However, over time, the idea of e-business has also evolved to encompass a multitude of activities that extend far beyond digital stores.

E-business thus consists of business that relies on information and communication technologies (ICT). Some of the key areas of such business are:

- **E-marketing**: The use of digital channels such as: social media, email marketing, search engine optimization (SEO), and online advertising to promote products or services and reach a wider audience.
- **E-commerce**: As mentioned above, e-commerce is an important part of e-business. It involves the online buying and selling of goods and services and encompasses various business models and platforms.
- **E-customer relationship management (e-CRM)**: The management and nurturing of customer relationships using digital tools and platforms. This includes tracking customer interactions, analyzing data to customize customer experience, and providing effective online customer support.

- **E-Supply Chain Management (e-SCM)**: The use of digital technologies to optimize supply chain processes: from procurement and inventory management to order fulfilment and distribution.
- **E-Procurement**: The use of electronic systems to manage the procurement of goods and services, including supplier selection, order placement, and supplier relationship management.
- **E-Collaboration**: Enabling collaboration between employees and partners through digital platforms, videoconferencing, and cloud-based tools.
- **E-Knowledge Management**: Managing and sharing organizational knowledge electronically to improve decision-making, problem-solving, and innovation.
- **E-Data Analytics and Business Intelligence**: The use of data analytics tools to extract insights from large data sets, enabling data-driven decision-making.
- **E-Payments and Financial Transactions**: Processing electronic payments, online invoicing, and securely managing financial transactions through digital platforms.

The following are some of the benefits that are conditioned by the characteristics of e-business. The key components and impacts of e-business are:

- **Digital transformation:** e-business has accelerated the process of digital transformation across industries. Organizations have moved from traditional businesses to integrated digital ecosystems that streamline processes, improve customer experience, and increase overall efficiency.
- **Global reach:** e-business allows companies to reach a global audience without the constraints of geographical boundaries.
- **Cost-effectiveness:** Digital processes can reduce operational costs such as paper-based documentation and physical infrastructure. We are witnessing new economic models and employment opportunities. Startups and entrepreneurs can enter into and participate in global markets with minimal barriers to entry, which stimulates economic growth.
- **Customer/Partner Focus:** e-business enables personalized interactions, rapid responses, and convenient access to information, which increases customer satisfaction. Customers and/or partners are at the center of (business) operations. With the help of data driven analytics, organizations understand the

desires, behaviors, and needs of customers and partners, which leads to personalized interactions and offerings.

- **Optimized Processes:** Automation of tasks and processes leads to greater efficiency and reduced human error. Automation, integration and digitalization of processes increase operational efficiency. From supply chain management to inventory control and order processing, e-business optimizes resource utilization and reduces costs.
- **Big Data Insights and Data-Driven Decision Making:** e-business generates valuable data that can be analyzed to gain insights into customer behavior, market trends, and business performance.
- **Competitive advantage:** Organizations that adopt e-business strategies are better positioned to adapt to changing market conditions and outperform the competition.
- **Innovation and agility:** E-business fosters an environment of innovation. Organizations quickly adapt to changing market dynamics, introduce new services and products, and test new business models without delay, quickly and in near real time.

Thus, e-business encompasses various aspects of modern business operations that leverage digital technologies to improve efficiency, customer engagement, and overall competitiveness. It is about adopting a holistic approach to managing business in the digital age.

While e-business offers numerous advantages, such as greater reach, cost savings, and convenience, it also has several negative aspects that companies need to consider and address to ensure sustainable and successful online business. This includes investing in robust security measures, efficient logistics management, ensuring compliance with legal regulations, and building customer trust and satisfaction with reliable services and secure transactions.

Some of the key negative aspects of e-business that need to be addressed with particular care in e-business are:

- **Security challenges**: E-business involves the transfer of sensitive data, including financial transactions and personal information. This means that e-business is a target for cyber-attacks such as hacking, phishing, and malware.

Businesses need to invest heavily in cybersecurity to protect data, which can be expensive and complex.

- **Privacy challenge:** With the collection of vast amounts of consumer data, serious privacy concerns arise. Companies need to ensure that they comply with data protection regulations such as GDPR. Failure to comply with these regulations can result in legal consequences and loss of customer trust.
- **Technical issues:** E-business is heavily technology driven. Technical issues such as website downtime, software bugs or slow loading can disrupt business, leading to lost sales and dissatisfied customers.
- **High start-up costs:** Setting up a robust e-business infrastructure can be expensive. This includes the cost of developing a user-friendly website, operating secure payment systems and integrating the necessary back-end systems. These initial investments can be a barrier for small businesses.
- **Intense competition:** In many business segments, the internet has leveled the playing field for companies large and small. Increased competition makes it harder for companies to stand out and attract customers, often requiring significant investments in marketing and differentiation strategies.
- **Logistics challenges:** E-business businesses need to pay extra attention to managing their logistics processes. This includes warehousing, inventory management, shipping, and returns processing. Poor logistics management can lead to delivery delays and increased costs, which negatively impacts customer satisfaction.
- **Technology dependency:** In e-business, businesses are highly dependent on technology, meaning that any technological failure can bring their business to a standstill. Businesses need to have robust IT support and disaster recovery plans in place to mitigate IT risks.
- **Customer trust and satisfaction:** Building trust with customers is more challenging online than in brick-and-mortar stores. Issues such as the inability to physically inspect products before purchase, concerns about payment security, and delays in responding to customer inquiries can all reduce customer satisfaction.
- **Legal and regulatory compliance:** In e-business, businesses must contend with a complex web of regulations that vary by region and industry. These include consumer protection laws, e-business regulations, and international trade laws. Non-compliance can lead to fines and other difficulties in meeting legal norms.

- **Lack of personal interaction:** The lack of personal interaction in e-business makes it difficult to build deeper relationships with customers. Personalized service and the human touch often play a key role in customer loyalty and satisfaction.
- **Returns and refund management:** Managing returns and refunds in e-business can be more complex and expensive than in traditional retail. The process involves handling reverse logistics, restocking, and dealing with possible loss or damage to returned items.
- **Digital divide:** Not all potential customers have equal access to the internet or digital devices, leading to a digital divide. This limits the reach of e-business businesses, especially in regions with low internet penetration or among demographic groups with lower levels of technological literacy.

2.1 E-business model

Figure 2.1 shows the e-business value chain model from Meier & Stormer (2009). The figure shows the three essential components of e-business, which are:

- support processes for implementing e-business,
- e-business value chain,
- technical and technological solutions to support the implementation of e-business.

The supporting processes consist of: strategic planning, organizational and human resources, information and cybersecurity management, control, and cultural diversity management. All of these processes are conditional and related to e-business. We assume that knowledge about these processes is already present or needs to be acquired from management literature.

The value chain consists of seven different approaches, which complement each other. Within each of the aforementioned approaches, it is possible to find other approaches. However, on the left side of this value chain, approaches that require lower inputs, as a rule, also produce lower value results. The further we go to the right, the greater the inputs for the realization of the solution and the greater the expected benefits.

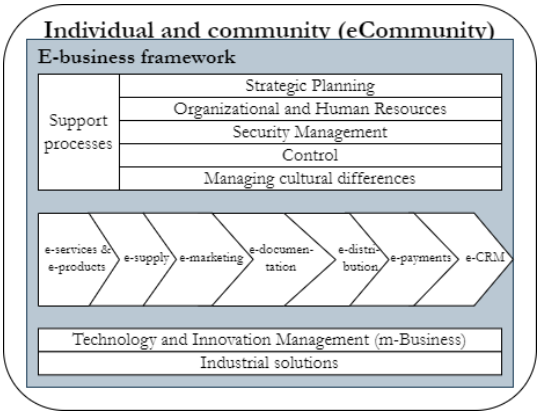

Figure 1.1: E-business model
Source: Summarized by Meier & Stormer, 2009.

In the organization of electronic products and services, the organization is required to find an appropriate form of cooperation using a business model. Such forms of cooperation between organizations and potential buyers range from simple and informative presentation of goods, open markets with goods and their values, to more closed systems where the stakeholders of such a market cooperate with each other.

The next approach in e-business is intended for electronically supported purchasing processes. In principle, there are a number of solutions for e-procurement. Solutions differ from each other depending on whether product and service catalogs for the selection and purchase of products are available on the buyer's side (buy side) or on the supplier's side (sell side). In the third variant (electronic market), a third party provides software solutions and catalogs for purchasing. This allows comparisons and evaluation of products and services. Catalog management presents a special challenge.

E-marketing (or online marketing) works by exploiting market potential and nurturing business relationships through electronic means of obtaining information and communication. Segmenting online »customers« into categories enables the implementation of a diverse marketing process and immediate adaptation of online marketing services. The first successful global example of this type of e-business was Google, with Facebook and others following. With appropriate key indicators, they enable the measurement of the effectiveness of online offers (for example, using a

web browser), can calculate interaction rates (if we say that the other side is an online consumer), encourage online customers to create their (possibly virtual) values, carry out business transactions (online customer) and maintain connections with the customer (online key customer). Of course, in this process, it is necessary to study and analyze the specifics of online advertising.

The next approach deals with the concept of e-documentation. Here, an electronic document is considered a legally valid document. To achieve this, it is necessary to establish trusted centers that register real persons, issue digital certificates and provide a pair of electronic keys for digital signatures. Asymmetric cryptographic procedures using private and public keys are a basic requirement for the use of such certificates and signatures. Electronic documents can be electronically signed on the one hand while digital signature authentication can be performed on the other. Documents can also be appropriately converted into an electronic cryptogram, which protects the document relatively well from unwanted views.

In the case of the electronically supported distribution of a product or service, which can be in physical or electronic form, we encounter the next level of complexity of electronic commerce. If the consumer has a mobile device with an Internet connection at hand for the service, he can take advantage of a time- and location-independent purchase or service (online distribution). Of course, products in electronic form can also be distributed in a classic way - that is, not electronically, since offline distribution on the World Wide Web also has its advantages. In addition, hybrid distribution forms can be presented that combine online distribution with a version of offline distribution. Distribution is only part of the complete supply chain. In e-delivery, it is necessary to coordinate the steps of planning, purchasing, production and delivery of products and services using a reference model.

Electronic payments (e-payments) allow for the payment of small amounts involving only a few cents (picopayment), medium amounts of a few euros (micropayment) and larger amounts (macropayment). To ensure that the transaction costs for picopayments and micropayments are low enough to be worthwhile, methods based on the use of electronic coins have been developed. In addition, there are several accounting and proprietary procedures for electronic payments. In order to ensure the security of electronic payment procedures, cryptographic procedures and digital signatures must be used. For example, the SET (Secure Electronic Transaction)

protocol requires the use of a double signature procedure so that both the order data (regarding the merchant) and the payment methods (regarding the bank) are protected.

In e-Customer Relationship Management, the focus shifts from the products themselves to customer management. In addition to the usual key financial indicators, what becomes especially important is that customers, buyers or stakeholders in general need to be captured and evaluated. Relevant data is stored in a customer data warehouse, which allows for a comprehensive analysis of customer behavior. In addition to analytical customer relationship management, we also use multi-channel management, which presents a special challenge, as it is necessary to evaluate different communication channels with customers and determine which ones are suitable for use. This e-business approach requires the highest investment in implementation but can also provide the highest returns. These returns can be measured in money or in other ways - for example, in knowledge of behavior. Recently, great efforts have been made in the EU especially to limit the collection of data/information on individuals (customers) by both individual companies and other organizations (for example, intelligence services).

3 Information and cybersecurity

Securing the digital landscape in a rapidly changing digital age, where information and data are at the heart of modern operations, means that information security and cybersecurity have become crucial. These two intertwined disciplines are designed to ensure the availability, integrity and confidentiality of digital information and protect individuals, organizations and societies from the expanding world of cyber threats (Jereb, 2019). The following presents the general importance of cybersecurity in the light of planning and implementing business digitization.

Information security encompasses the strategies, practices, and technologies implemented to protect information from unauthorized access, use, disclosure, interference, alteration, or destruction. It involves a holistic approach that encompasses people, processes, and technology. The most important key aspects of information security include:

- **availability:** ensuring that information and services are accessible and usable when needed,
- **integrity:** maintaining the accuracy and trustworthiness of data by preventing unauthorized changes,
- **confidentiality:** ensuring that information is accessible only to authorized individuals or entities,
- **authentication and authorization:** verifying the identity of users and assigning the appropriate level of access,
- **data encryption:** converting data into an unreadable format to prevent unauthorized access,
- **risk/vulnerability management:** identifying and addressing vulnerabilities that attackers could exploit,
- **employee training:** educating employees about security best practices and potential risks.

Cybersecurity focuses on protecting digital systems, networks, and devices from cyber threats. These threats encompass a wide range of malicious activities, including hacking, malware, ransomware, fraud, and more. Key elements of cybersecurity include:

- **Network Security:** Protecting computer networks from unauthorized access, data breaches, and other cyberattacks,
- **Endpoint Security:** Securing individual devices (computers, smartphones, IoT devices) from malware and other cyberthreats,
- **Incident Response:** Developing strategies to effectively respond to cyber incidents and reduce their impact,
- **Threat Intelligence:** Collecting and analyzing information about emerging threats to anticipate and mitigate attacks,
- **Security Audit and Monitoring:** Regularly assessing and monitoring systems for signs of intrusions or suspicious activity,
- **Cybersecurity Policies and Procedures:** Creating guidelines and protocols to ensure consistent and effective security measures.

In today's world, with interconnected organizations of all types and sizes, the importance of information security and cybersecurity cannot be overstated.

Cyberattacks have the potential to disrupt critical infrastructure, compromise personal data, and harm national security. The challenges in these areas are constantly evolving due to the increasing sophistication of cybercriminals, rapid advances in technology, and the ever-increasing number of attack vectors.

In addressing information and cybersecurity, we face challenges that we try to overcome with some generally accepted strategies to ensure a secure digital environment. The most important of these strategies are proactive and comprehensive approaches that organizations and individuals must adopt, including:

- **Education and training:** Continuous training and awareness programs are essential to empower individuals to identify and respond to cyber threats,
- **Advanced technologies: Strategies** such as artificial intelligence and machine learning are used to detect/prevent cyber threats in real time,
- **Collaboration:** Sharing information and communicating threats and best practices between organizations (including governments) to strengthen shared cybersecurity,
- **Rules and compliance:** Adhering to cybersecurity regulations and standards to improve data protection and privacy,
- **Resilience planning:** Developing incident response and disaster recovery plans to reduce the impact of cyber incidents.

A more detailed description of ensuring security against IT threats and attacks is presented in the chapter on information and computer security.

4 IT risk and investment management

When establishing a security management system, organizations must ensure systematic risk management, which must be consistent with the needs, policies and environment in which the organization operates. Ultimately, the management of individual (operational, IT, exchange rate, etc.) risks must be consistent with the management of all risks that the organization faces. Security policies relate to the timely and effective management of risks in areas where and when necessary. It is a process that must be established and, once established, continuously implemented and supplemented.

IT risk management is a key component of overall risk management in an organization. It involves identifying, assessing and mitigating risks associated with information technology to ensure the availability, confidentiality and integrity of information and systems. The key aspects of IT risk management are presented in Figure 1.2. They are summarized in ISO/IEC 27005:2022 (*ISO/IEC 27005*, 2022), which is a standard that describes the risk management process and its activities to ensure information security.

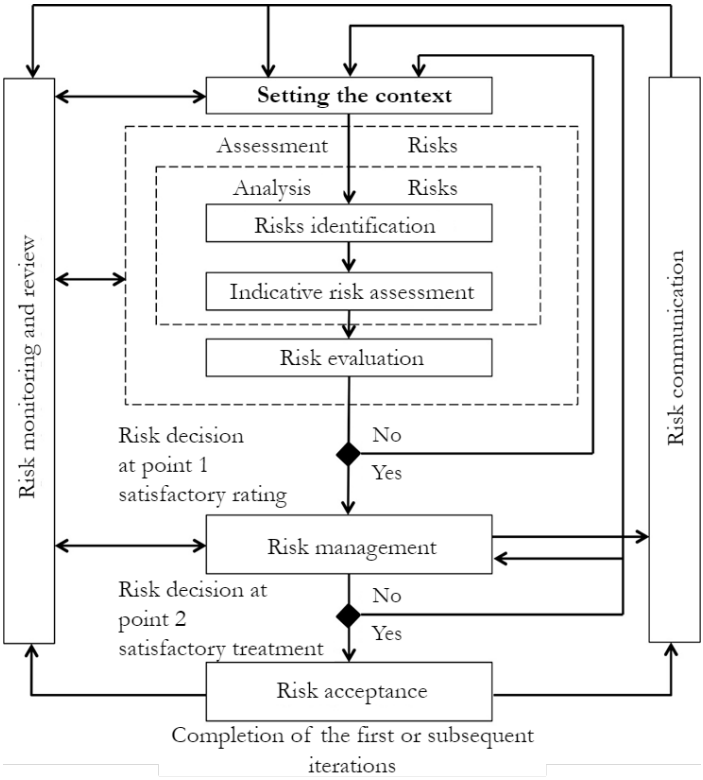

Figure 1.2: Information risk management activities
Source: (Jereb, 2019).

The highest management level of the organization must be responsible for implementing the information security policy and security system. In doing so, it implements the information risk management process in a way that considers the criterion of damage reduction. A very rough estimate is that when ensuring the availability, integrity and confidentiality of information, it takes into account the

business impact of a potential security incident on the business and the realistic probability of an information incident occurring (Jereb, 2019).

Since it is not practical to completely avoid risks, or eliminate them completely, we need to come to terms with them and learn to manage them. When managing risks, organizational leaders make decisions according to the following options:

- the risk needs to be reduced,
- the risk is accepted without additional action,
- the risk is avoided,
- the risk is transferred to contractual or third parties.

Information risk management according to ISO 27005 consists of the following activities, which are also shown in Figure 2.2 (*ISO/IEC 27005*, 2022):

- **Setting the** context in which we try to define the risk management framework.
- **Risk assessment:** where we try to evaluate the level of risk. This set contains two activities:
    - **risk analysis**, which is again divided into:
        - **risk identification,**
        - **risk assessment framework,**
    - **risk evaluation**,
- **Risk management:** where appropriate measures must be taken to avoid, reduce, transfer or accept risks as they are at a given moment.
- **Risk acceptance:** we decide to take measures related to risks and determine responsibility for identifying risks with justifications.
- **Risk communication:** where we ensure that there is a continuous high-quality exchange of information between all interested publics and risk managers about the existence, nature, form, probability, severity, acceptability and similar risk factors.
- **Monitoring and review:** where risks and their factors are monitored and reviewed to detect any changes within the organization and maintain a comprehensive view of the risk.

The practical application of ISO/IEC 27005 across industries is key to ensuring robust IT risk management. Some hypothetical case studies or examples of how ISO/IEC 27005 could be applied across industries are as follows:

- Financial sector:
  - Scenario: A financial institution or company implementing financial processes wants to improve its information security risk management processes.
  - Application: ISO/IEC 27005 can be implemented to systematically identify and assess risks associated with customer data, financial transactions, and regulatory compliance. The institution can then implement tailored risk management strategies to protect sensitive information and ensure compliance with financial regulations.
- Healthcare sector:
  - Scenario: A hospital is concerned about the security of medical records and medical data.
  - Application: ISO/IEC 27005 provides a framework for conducting a risk assessment of the confidentiality, integrity, and availability of health data. The hospital can use it to identify vulnerabilities, assess potential breaches, and implement measures to protect patient data.
- Manufacturing sector:
  - Scenario: A manufacturing company seeks to secure its intellectual property and production processes.
  - Application: ISO/IEC 27005 can help assess the risks associated with intellectual property theft, supply chain disruptions, and operational disruptions. The company can implement risk mitigation strategies to protect critical assets and ensure the continuity of production processes.
- Information Technology (IT) Services:
  - Scenario: An IT service provider wants to demonstrate to its customers its commitment to information security.
  - Application: ISO/IEC 27005 can be used to comprehensively assess the risks in its IT service portfolio. By identifying and managing the risks associated with data breaches, service disruptions and cyber

threats, the company can strengthen its credibility and demonstrate to its customers its commitment to information security.

- Government agencies:
  - Scenario: A government agency responsible for citizen data wants to strengthen its security measures.
  - Application: ISO/IEC 27005 can guide the agency in assessing the risks associated with the confidentiality of citizen data and the availability of critical services. The agency can develop and implement risk management plans to ensure the secure handling of cross-border information.
- Retail:
  - Scenario: A retailer is concerned about the security of customer payment data.
  - Application: ISO/IEC 27005 can help a retailer identify risks associated with payment processing, point-of-sale systems, and online transactions. By implementing security controls and regularly assessing risks, a company can build customer trust and protect financial transactions.

In any case, it is crucial to tailor the use of ISO/IEC 27005 to the specific IT risks and industry requirements. This includes understanding the unique assets, threats and vulnerabilities relevant to each sector and implementing effective strategies to manage IT risks and mitigate potential negative impacts.

References

ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection—Guidance on managing information security risks (Version 4). (2022). [International standard]. https://www.iso.org/standard/80585.html

Jereb, B. (2019). *Informatika in informacijska varnost: Repetitorij*. Univerza v Mariboru, Fakulteta za logistiko. https://doi.org/10.18690/978-961-286-251-0

Meier, A., & Stormer, H. (2009). *eBusiness and eCommerce: Managing the Digital Value Chain*. Springer. https://www.abebooks.com/9783540893271/eBusiness-eCommerce-Managing-Digital-Value-354089327X/plp