PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020
108

DATA, INFORMATION AND IT SECURITY - SOFTWARE SUPPORT FOR SECURITY ACTIVITIES

Pál Michelberger, Ágnes Kemendi
Óbuda University, Hungary
E-mail: michelberger.pal@bgk.uni-obuda.hu,
kemendi.agnes@phd.uni-obuda.hu

Abstract

Data protection, information and IT security became number one priorities in these fast- paced days that top management needs to focus on. A number of IT solutions have been developed on the market to address the security challenges that require prompt actions. These solutions contribute to a control environment that is robust and stand the potential threats. This research describes the framework of governance, risk and compliance and provides an integrated, holistic approach which helps to increase process performance and to ensure that the organization follows its own rules, risk appetite, and complies with external regulations. These systems fulfil a core role in the enterprise's defense system. This research reviews the features of security packages relevant to IT GRC and provides an overview of the security elements and describes their main characteristics. This review covers the configuration database related to the enterprise business model; the business impact analysis; the risk management-, governance and compliance functions; the data security; the data protection and GDPR; the business continuity management; the network -, IoT - and industrial control system safety, the access - and log management. Embedding these solutions to the business and operations processes strengthens the response of an organization to the various risks and requirements that it faces and reduces the likelihood of major non-compliance or security gaps.
Keywords: *data protection, GRC software solutions, information security*

Introduction

The Corporate leaders often face information security challenges. The IT system of an enterprise is made up of a number of basic software (operating systems), applications, database managers, hardware and network components. Significant parts of these components have information and data protection function. However, users, key users, and administrators (and external business partners using the IT of the enterprise) are reluctant or unable to take advantage of the myriad - but sometimes insufficient - opportunities that are "readily available" on the shelf.

Corporate executives, on the other hand, want to keep their own and their business partners' data secure; they force company stakeholders to use security-conscious information technology and to implement complex solutions that support an information security management system which controls information security threats (Kuyoro et al., 2011). In recent years, a number of companies have offered complex IT security solutions that oversee, analyze, and support the role of the IT security manager in all 'areas of protection' (Vunk et al., 2017).

Key concern is to understand the need behind proper risk management processes on enterprise level with respect to data, information and IT security and to identify hands-on solutions available for corporate stakeholders to manage the security risks. In this research, the

https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

theoretical framework and the possible features of security software packages are studied to provide both theoretical and practical reference material to address this problem.

Purpose: The purpose of the research was to provide an understanding behind the framework of governance, risk and compliance model with focus on data, information and IT security and to provide a structured approach on related security solutions.

Design/methodology/approach – The research purpose has been accomplished through describing the role of the governance, risk and compliance model and through reviewing the features of security packages relevant to IT GRC and through providing an overview of the security elements and specifying their main characteristics.

Findings – The research has identified a set of IT solutions that can be used to manage the data, information and IT security risks. Furthermore, the research has provided an overview of the identified software solutions.

Originality/value – The research – that covers data, information and IT security with respect to software solutions for security activities in enterprises – provides a unique approach because it brings under one umbrella the literature background behind governance, risk and compliance model, the proper enterprise defense system and the software solutions that meant to mitigate the risks in this area. The research identifies the practical solutions and demonstrates their features. The research can be leveraged as a best practice in corporate environment, can help to increase process performance and to ensure that the organization follows its own rules, risk appetite, and complies with external regulations. The research can be used as a tutorial in this respective area.

Information security management system in practice (areas concerned):

- Classification of information (public, internal, confidential, strictly confidential – 'confidential handling')
- Threats and risks
- Encryption (process and stakeholders)
- User access, authorization
- Electronic mail rules
- Internet usage
- Virus Protection
- Password usage (training rules, change management)
- Printing
- Mobile devices and data storage
- Manage archives
- Verbal communication rules
- Control on Information management (clean desk - clean screen, protection of IT assets and data carriers, prevention of data leakage)
- Backups
- Human resources (recruitment, training, monitoring, dismissal)
- Information and Communication Technology (ICT) vulnerabilities (reliability - network, firewall, servers, core and application software)
- Logging (logins, transactions, errors, incidents, prints, copies, logs analysis)
- Incident management (lessons learned)
- Responsibilities, procedures
- Information Security Management Systems (ISMS) monitoring and development by Plan-Do-Check-Act (PDCA) model).

Possible features of security software solutions:

- 'Inventory' (configuration database; hardware, network, peripherals, operating system, database manager, applications (including protection solutions, etc.), clouds, users, processes (workflow), data assets – i.e. resource properties and their relationship in a structured way)

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

- Vulnerability testing and risk management (monitoring of threats and protection measures developed to address them; risk management plan and risk report (indicating the degree of vulnerability))
- Log management (broken down by actions), log analysis, database recovery
- User behavior analysis, user authentication, identity management
- Secure data storage
- Compliance assessments, preparation for audit (internal regulations, recommendations (e.g. COBIT), standards, ISMS (e.g. ISO/IEC 27001))
- Maintenance and testing of Business Continuity Plans (BCP) providing alternative solutions, incident simulation
- Data protection; compliance with data management rules, the European General Data Protection Regulation (GDPR) audit
- Network security (gateway, firewall, virus protection, authorization and access management, Application Programming Interface (API) management).

The Role of GRC Systems

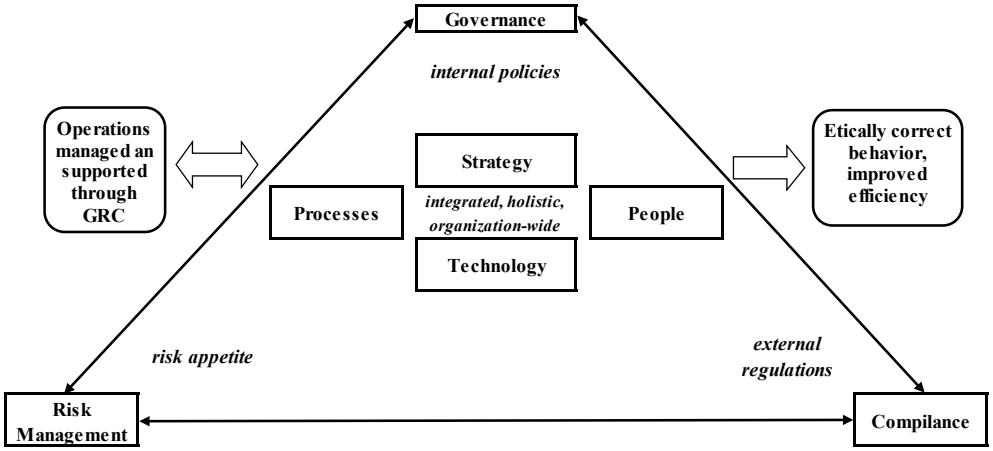
The Governance, Risk & Compliance (GRC) systems cover the organization's safety network pillars in terms of governance, risk management, and compliance.

Racz et al. pointed out in 2010 that the concept behind the GRC acronym has not yet been sufficiently explored and its interpretation varies amongst professionals in the so-called Frame of Reference for Research of Integrated Governance, Risk & Compliance conference paper.

The research team laid down the definition of GRC (see Figure 1.): 'GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.'

Technology is key, but the concept is much more than that; the integrated GRC is designed to increase process performance and to ensure that the organization follows its own rules, risk appetite, and complies with external regulations through its strategy, processes, technology, and consistency of the human factor to enhance synergies and driving performance.

Figure 1
Frame of Reference for Integrated Governance, Risk & Compliance (Racz et al., 2011, p.9.)



https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

The elements of the GRC model (Racz et.al, 2010) are as follows:

- Governance - corporate objectives, processes and the organization which operates the processes, with special emphasis on information technology that also supports the achievement of underlying objectives (ISO / IEC 38500),
- Risk Management – the identification of expected events and their risks and the formulation of the expected level of security for all company processes, resp. information technology tools (Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management, COSO ERM),
- Compliance - the company must comply with internal regulations, policies, laws, standards and contractual requirements.

The application of the model also means a comprehensive list of requirements that is constantly evolving in response to the changing circumstances. The management of the company is aware of the risks and the expectations it meets at a given moment.

The self-sustaining regulatory circle can lead to risk-based management decisions. The model manages the corporate strategy, the material and the administrative processes, the technology and the employees (Michelberger & Lábodi, 2012).

Management tools in support of the company's decision-making process have a key role in successful company management (Francsovics et al., 2019). The design and the operation of the risk management framework have a fundamental role in the company's risk response and ultimately reduce the likelihood of major gaps. A well-functioning system has a number of benefits that generate value for an organization: contributes to transparency, enables continual improvements, and strengthens the quality management system which increases customer satisfaction and market position consequently.

GRC systems are linked to the various levels of the organization's defense system; these lines are the primary, secondary, and tertiary lines of defense. The three lines of defense model in effective risk management and control have been defined in the January 2013 resolution of the IIA (Institute of Internal Auditors, Position Paper, 2013). (See Table 1.)

Table 1

Roles in the Risk Management Process according to the Three Lines of Defense Model

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk owners / managers	Risk controls & compliance	Risk assurance
-operating management	-limited independence -riports primarly to management	-internal audit -greater independence -riports to governing body

Source: IIA Position Paper, 2013, p.6.

The primary line of defense is the risk management embedded in the business processes itself. The responsibility of business process managers includes the identification and proper management of the risks in the corporate processes within their competence, and they have to ensure the operation of controls.

The primary line of defense provides active protection at the level of operational processes.

The secondary line of defense is the risk management and compliance function, which is also part of the so-called protection network of the organization; this line monitors and controls the operation of primary processes.

The third line of defense tests and verifies already as an independent function, in the form of an internal or external audit.

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

The above model also reflects the need for an integrated system for managing, effectively documenting and operating corporate processes (Norman, 2007).

All the three lines of defense play a prominent role in the organization's broader governance framework. Governing bodies and members of senior management are the primary stakeholders (IIA Position Paper, 2013).

The advantages of GRC systems in practice:

- Effective risk management
- Transparent, efficient internal processes, stronger control environment and increased process security
- Support the decision-making process
- Effective audit support
- Easier identification of continuous improvement opportunities.

The GRC market has been present for about more than 15 years and is characterized by dominant user demands. The GRC software market is mainly dominated by key players like IBM, Thomson Reuters or SAP.

Initially, it was characterized by its own developments; nowadays, there is a growing demand for comprehensive software solutions that large developers can meet. The market is price sensitive; typical business scenario is that the business need for software needs to be seriously substantiated in order to win the consent and approval of the company's internal decision makers and in case of acceptance usually only a limited budget is available.

The functionalities of the software are becoming more and more extensive as a result of market demands (Cau, 2014; Recor & Xu, 2017a).

A number of software development companies and consulting firms conduct studies on GRC, but these can be scientifically biased due to their underlying business interests (Racz et al., 2011).

To review the status quo, we present however the results of Forrester Consulting in 2019, in which, commissioned by SAP, it assessed the importance of GRC tools in today's modern business environment.

As a result, the importance of GRC is widely recognized, however, many companies do not take advantage of its inherent business values.

Integrating the GRC function into the business processes can be an effective, value-adding part of the decision-making and planning processes; this requires that GRC-related corporate practices are more directly integrated into the business workflows.

For investment decisions related to intelligent GRC solutions, the most determining factors are the increased profitability through the reduced effects of error and better process efficiency. According to the survey, these solutions are mostly related to risk management and mitigation, resp. they provide value to companies through continuous monitoring.

By automating the related routine tasks, a more efficient operation of the system can be achieved (Forrester Opportunity Snapshot, 2019).

Ensuring effective and reliable compliance with Sarbanes-Oxley's segregation of duties and conflict prevention rules is an example of a labor-intensive, administrative area, where the implementation of process in-built controls and automation save significant time of human resources and provide an audit trail as well.

A robust GRC system can also contribute to financial success. The complex regulatory environment itself and the monitoring of the changes are regular tasks that can be relieved as a result of automation: minimizing the risk of human error and making routine compliance tasks more efficient. In addition to the general business risks, such as the macroeconomic situation, competitors, rising costs / wages, cyber security emerges as a major business risk that needs to be addressed (Oxford Economics, 2019).

https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

In simple terms, GRC systems actually serve to protect strategic business goals. The benefit of examining the relationship between strategy and risk is that it helps to identify which of the different degrees of severity and impact of risks can be described as the most critical ones for the company (Anderson & Frigo, 2020).

Reliable data quality at all times is efficient, free from error operation calls for the operation of the GRC modules as an integrated system where a piece of data is recorded only once and is updated in the related modules.

Overview of GRC Software Functions

The primary function of GRC software is to automate most of the documentation related to risk management and regulatory compliance that are closely related to corporate governance and business objectives. Primary end users include internal auditors, compliance officers, and management. The main functions of the GRC software cover Risk management, Business Continuity Management, Policy- and Knowledge management, Compliance, Legal and Audit management. (See Table 2 for the specifications of these functions.)

Through GRC solutions, companies can improve their internal processes and automate risk management processes, which increases process security and can also result in significant reduction of manual work.

Table 2
Main Functions of GRC Software

1. Risk- & Business Continuity Management
- IT Risk Management, IT Vendor Risk Management, Operational Risk Management, Business Continuity Management - Supports risk management professionals in risk-related documentation, workflow, assessment, analysis, reporting, visualization & remedation. This function focuses primarly on risks and incident monitoring, but may also collect data from risk analysis tools e.g. credit risk, market risks, etc. to provide a comprehensive status of risks.
2. Policy- & Knowledge Management
- Supports the document management process, from policy creation to review and approval, manages changes and the archiving process, assigns policies to mandates and business objectives on the one hand, and to risks and controls on the other. It handles also the related information flow.
3. Compliance, Legal
- Corporate Compliance and Oversight Enterprise Legal Management - Supports the relevant professionals in documentation; workflow; reporting and visualization of control objectives, controls and related risks; questionnaires and self-assesments; testing and remediation. It covers all areas of compliance, including with internal processes.
4. Audit Management
- Supports the internal audit team in managing working papers, planning audit tasks, scheduling and reporting.

Source: Cau, 2014; Recor & Xu, 2017a

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

IT GRC

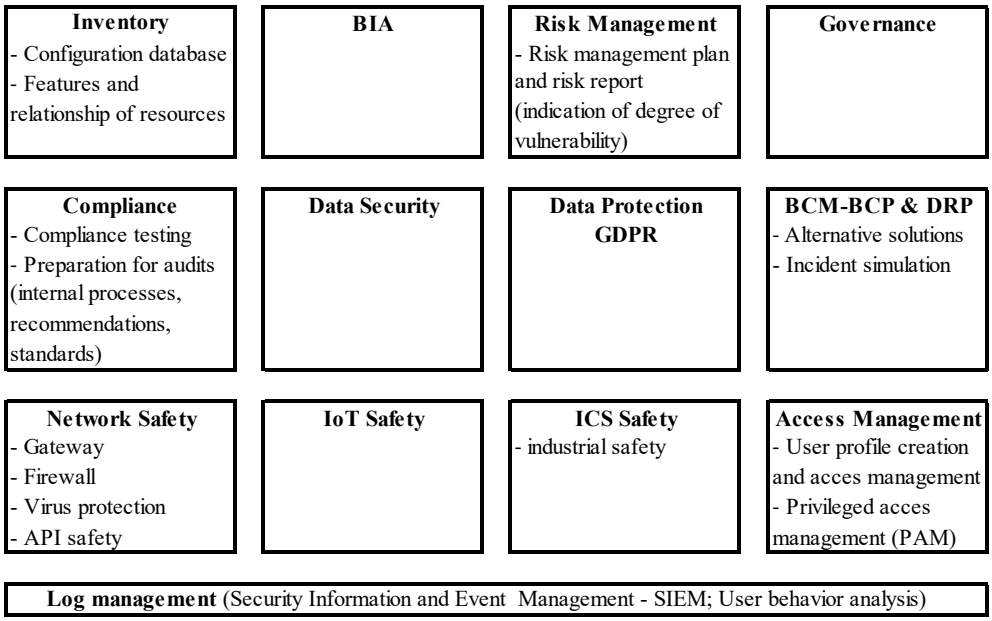
The management of information and communication technologies in the company is supported by the ISO / IEC 38500 international standard from Australian origin, which can also be interpreted as a management framework. On the basis of the standard a policy can be developed which monitors, evaluates and manages how business processes are served from IT perspective. This addresses the responsibilities of managers, the information technology aspects of corporate strategy, the procurement and performance of information technology tools and compliance with business objectives, and human behavior (Michelberger & Lábodi, 2012).

The IT GRC dimension of GRC systems can be interpreted at two levels: 1) the usage of IT tools to manage GRC processes according to the structure presented in the previous part of the article, and 2) ensuring that all IT systems and processes that support business processes is also appropriate from a GRC point of view. In the following part of the article, we review the main groups of security functions according to this latter definition (Rasmussen, 2009).

GRC Software Review – an Overview of the Security Elements Relevant to IT GRC

The software available on the market aims to serve a wider range of customer needs. In the followings (see Figure 2), we provide an overview of what the customer requirements are and how IT GRC developers respond to the software needs in the digital world (Balasys, n.d.; Secube, n.d.).

Figure 2
Security Elements Relevant to IT GRC



https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

Inventory Module

Inventory module describes the corporate operating model; a configuration database where the structure, the operation of the company together with the essential resources necessary for the operation can be recorded and managed. Configuration elements can represent hierarchical relationships and dependencies/linkages. The basic goal is to correctly map the underlying corporate structure, therefore being customizable is a prerequisite

The Inventory module is actually the null module, as the workflows of the other modules are built on this module. It can be interpreted as an inventory of the so-called information security management system asset.

The configuration elements of the enterprise business model explore and provide a good overview of the organizational structure including the human resources, the site - and the inventory structure, the data property, the services and systems, the business and production processes and the safeguarding measures.

Business Impact Analysis (BIA)

On the basis of business impact analysis, we can determine the value of our resources, the value of the assets based on their impact by assessing their potential damages that would occur during possible damage/loss to business activities, systems or data assets. Under damage we mean breach of availability, confidentiality and / or integrity. Material and intangible valuation aspects can be also identified, a typical example of this latter case is loss of reputation. BIA provides input also for the identification and risk analysis of critical resources.

Risk Management

Governance & Compliance functions are covered only briefly since their details have been already introduced in the earlier sections.

Risk management covers the analysis and management of corporate risks according to the steps laid down in the risk management methodology. Risk analysis creates a relationship between the vulnerabilities of our resources and the threats they pose; analyses business impacts and the safeguards used as a risk management tool. The result of the risk analysis is the list of risks, which is managed by the company through the risk management plan and related reports. In the followings the Risk management – Governance & Compliance functions briefly since their details have been already covered in the earlier sections that contain indication of the degree of vulnerability. The ISO/IEC 27001 Information Security Management System and ISO/IEC 27005 Information Security Risk Management Standards are the ISO quality assurance aspects behind the applied methodology.

Governance

Governance is related to the operation of the information security management system. With the help of Governance, security tasks and documents related to the maintenance of the system can be managed; security incidents and security exceptions - that are allowed in special cases - can be recorded. Incident simulation and related analyses are also part of the system.

Compliance

Compliance refers to compliance with various requirements - such as ISO/IEC 27001 (ISMS), Sarbanes Oxley 404 management assessment of internal controls, internal regulations

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

e.g. parent company requirements, information security objectives, recommendations (e.g. COBIT) - compliance review & testing, audit, analysis of deviations and development of action plans, preparation for audits and their documentation.

Data Security

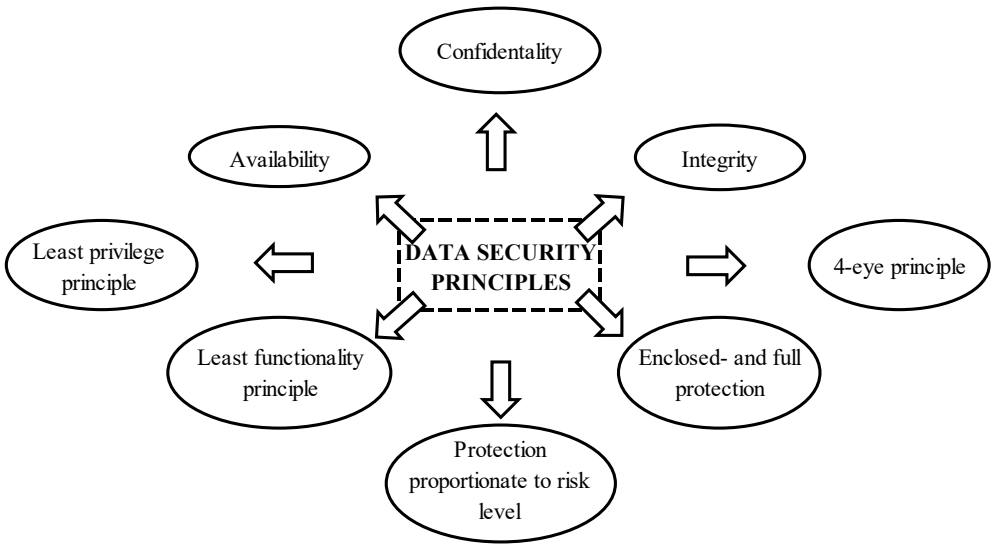
Data security is a key pillar of IT systems that interweaves the security elements discussed.

The principles of data security (see Figure 3) are confidentiality (available only to the authorized individuals), integrity (can only be modified by the authorized persons) and availability of the information (can be used in the required time and for the duration). These are the key security goals.

Data security is ensured when the protection is enclosed: all relevant threats are assessed by the system and the protection is full: all system components are covered, including IT, physical, and personal security features.

The principle of minimum levels of access requires that jobs are performed with a bare minimum of accesses through a precise definition of competence in the particular job/role. Furthermore, the configuration of the IT system is limited also to the necessary services as the least functionality principle lays that down. The four eyes principle applies where two independent and competent persons knowledgeable about the process perform checks over the particular process step to ensure that the execution - and the financial transactions are properly controlled. This principle has twofold benefits: through the checks of different persons the segregation of duties is maintained as well as possible process errors, incidents can be prevented as a result of this control step. In addition as per the protection proportionate to risk level principle the cost of data security protection is proportionate to the value of the damage that may occur (Breithaupt & Merkow, 2014; Dayarathna, 2009; Vega et al., 2017).

Figure 3
Data Security Principles



https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

Many repositories and software are available in the so-called cloud through the Internet. The spread of cloud-based IT has lifted IT services to a new level, enabling economies of scale, making backups cheaper as data can be mirrored into multiple redundant locations in the cloud provider's network. To ensure appropriate protection against attacks effective operation of policies and technologies is essential (Marston et al., 2011).

Data Protection, GDPR

Protection of personal data whenever collected is the key objective of the related rules. Under EU data protection rules the protection of the personal data subject to data collection must be guaranteed both for digital and paper-based data (Your Europe European Union, n.d.).

In connection with the EU General Data Protection Regulation 2016/679, it is necessary to register the company's data management activities and to demonstrate compliance.

The European GDPR regulates the organizations' data management and processing based on non-information security considerations. The question is what we want, resp. what we have to protect from our own and our partners 'data. Basic principle is that only as much personal data (name, address, tax identification number, social security number, e-mail address and password, bank account number, IP address, portrait, etc.) can be processed and only for as long as and to the extent that is strictly necessary. Failure to comply with GDPR requirements (non-compliance) is privacy incident that can result in severe penalties and damage to the organization's reputation. In the event of loss of purpose or in case of request, the data must be deleted (including the paper-based data) and the deletion must be documented. The protection of personal data is not (only) the responsibility of IT professionals (data processors), but primarily the responsibility of data controllers (purchasers, marketers, HR professionals, etc.). If possible, the IT Security Officer, the Data Protection Officer (DPO) and the Information Security Officer should be three separate individuals who work closely together to resolve data protection incidents.

Data protection incidents must be reported to the designated authority within 72 hours, and for instance in Hungary to the National Authority for Data Protection and Freedom of Information (Politou, et al., 2018).

Business Continuity Management (BCM)

The purpose of business continuity management is to be prepared for possible business disruptions. From the point of view quality assurance, the ISO 22301 Business Continuity Management System Standard lays down the requirements for such systems.

The scope of BCM is applied for major impairment of operation in a factory unit or in the office space, failure in the systems. Among others hardware failure, fire, flood, or loss of human resources are events for which emergency preparedness through BCM activities with a list of actions developed by the company is required.

The elements of BCM are the BCP and the Disaster Recovery Planning (DRP).

BCP aims to ensure the continuity of business processes through carefully planning which alternative solutions can be applied in the event of a downtime in the support-processes and by doing so making the smooth run of the business possible.

DRP focuses on providing the resources needed for the processes involved in the business operation - to replace, restore - in the event of an emergency.

The system includes standby preparedness for emergency (resource management planning, IT resource recovery plan, etc.), testing, ongoing maintenance, simulation of incidents and emergencies, preparation of statements the measurement of impacts, and setting recovery time targets (Conrad et al., 2016; Recor & Xu, 2017b).

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

Network Safety

Network safety is a crucial part of safety in the IT field; security gateways, firewalls, virus protection, the so-called API security are key to a company's security system. API security is covered in detail as the volume of data traffic due to the rapid development of API became very significant, and recently there have been a number of related security incidents that calls for attention to this area.

The APIs connect to the Web and cloud services, mobile and IoT devices through machine-to-machine communication. (An API is a programming interface and its documentation which allows the system to connect to another program. This solution makes it possible to use the services of the other program system without the need to know the internal details of the other program and is independent of the program language.)

The second EU payment services directive, the EU Revised Directive on Payment Services (PSD2) provides the opportunity for the so-called third party service providers to access the banks' current account management system and to the data stored in that. API communication is playing an increasingly important role, so appropriate protection measures are key.

Sensitive data, such as personal identifiers, financial data, and confidential information, is handled through the API, so addressing security threats, such as analyzing and controlling API traffic, is core requirement to focus on to protect systems that store internal data.

The EU General Data Protection Regulation also imposes significant data protection requirements, which must be complied with. The secure handling of credit card data is subject to the Payment Card Industry Data Security Standard (PCI DSS) global data security standard and is intended to protect credit card data and sensitive identification data wherever such data is processed, stored or transmitted. PCI DSS requires security controls, processes with appropriate controls over them, information security policies, secure networks and systems, protection of stored card data and encryption when transmitting data over public networks. By strengthening the control environment related to data protection, the number of bank card frauds and other collusions can be reduced (PCI DSS Quick Reference Guide, 2018).

IoT Safety

Internet-connected devices also require enhanced data protection and security measures; large amount of data is transferred through these devices, data is collected and shared, thus being in the crossfire of cybercriminals. This is an area requiring special attention in the context of Industry 4.0. It is essential to control network data traffic, e.g. using security router, as the necessary protection functions in IoT devices are missing or not sufficiently developed in most cases. Large volume of sensitive information is shared, such as in case of mobile-managed and paid online shopping.

The use of IoT poses additional security challenges; increased caution is required due to the communication of devices connected to the Internet.

The safety requirements of the IoT are described by Babar et al. (2011) co-authors and are grouped as follows:

1. User Identification: The approval process, which validates the users before using the system.
2. Tamper resistance: compliance with security requirements, even in the event of intrusion by malicious parties.
3. Secure Execution Environment: refers to a secure, managed-code, runtime environment designed to protect against deviant applications.
4. Secure Content: protects the rights of digital content used in the system.

https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

5. Secure Network Access: network connection or service access is only possible with an authorized device.
6. Secure data communication: authentication of the communication partners, ensuring the confidentiality and the integrity of data, prevention of the denial of the communication transactions and protection of the 'identity' of communicating entities.
7. Identity Management: this broad administrative area deals with the identification of individuals / things in a system and controls their access to resources in the system by associating user rights and restrictions with the user ID.
8. Secure Storage: confidentiality and integrity of sensitive information stored in the system.

Industrial Control System (ICS) Safety

The safety of industrial control systems is of paramount importance for large market companies and for strategically important companies (critical infrastructure). In an industrial environment, a network attack can lead to malfunction, complete operation failure, personal injury and / or environmental damage.

Attacks can be the so called Advanced Persistent Threat (APT) attacks as well, which are built-in for the purpose of obtaining hidden information, taking advantage of zero-day vulnerabilities, temporary unpreparedness of defense devices, in which case the goal is not a specific damage, but the constant unnoticed presence and espionage (Grooby et al., 2019)

In the era of industrial digital transformation, various attacks, extortion viruses, malicious codes require a system of protection that provides an adequate level of border protection.

Access Management

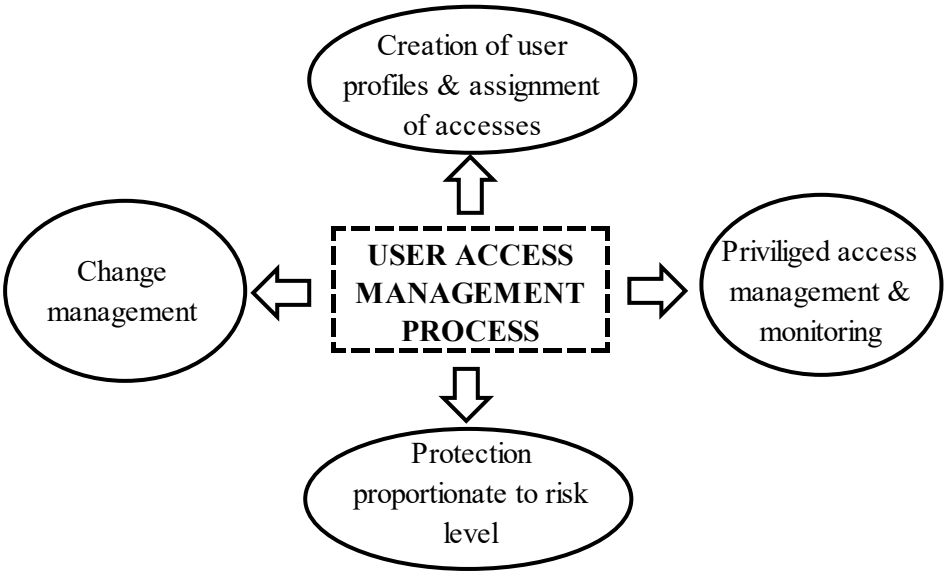
Access management – basic principle is to allocate only the accesses that are required as a bare minimum to perform the job; the roles of the users do not contain access rights that can cause segregation of duties conflicts; in the event of potential conflicts, appropriate risk mitigation controls must be introduced. A properly designed and operated access management process contributes to data security.

The internal control process of user access management is a key IT security process (see Figure 4): creation of user profiles and assignment of accesses incl. privileged accesses, managing and monitoring accesses incl. privileged accesses, operation of controls related to segregation of duties conflicts, and sensitive accesses.

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

Figure 4
User Access Management Process



The design and operation of the authorization and access management - from the creation of user accounts to the granting, monitoring, and, if necessary, termination of access - requires a robust process.

The so-called Identity and Access Management (IAM) systems are able to manage the critical security process at the enterprise level that covers who has and which accesses to networks, data and various applications. Authorization and access management can be used to efficiently and accurately assign access to users in systems; it is transparent who has access in the entire IT infrastructure and the associated security and non-compliance risks can be identified. This simplifies the change management process, including user creation, position change and exit of the employees. The implementation, operation and maintenance of such system is costly; it requires a targeted strategic decision to select the right product tailored to the needs of the company (Muse, 2017).

Privileged Access Management (PAM) covers the management and monitoring of users with privileged accesses. Due to the assigned privileges these are high-risk user accounts, which are popular targets for external cyber-attacks. Security risks can be reduced by recording user activity, logging and analyzing each keystroke in real time.

Log Management

Log management activity logging provides the footprint of events in the IT environment; fulfils a security function, used as a troubleshooting tool but the logged data serves also as input for business analysis - such as performance measurement, network traffic analysis.

Security Information and Event Management (SIEM) solutions - covering security information and event management - play an outstanding role in the IT security strategy; management of security events and logs form one of their key areas. Successful log management centrally manages relevant events, defines and documents the covered set categories, is regularly monitored, and is properly documented (Swift, 2010)

https://doi.org/10.33225/pmc/20.15.108 ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

The so-called syslog-ng is a log management solution that optimizes the performance of the SIEM solution, filters and normalizes log data, thereby reduces the data size and complexity, allowing fast searching of logged data in almost second. The solution is compliant with legal requirements. Its safety storage device is the so-called syslog-ng Store Box, which archives automatically, is a non-manipulable storage device that is encrypted with SSL / TLS protocol, compressed, and timestamped and is supported by properly defined access controls to protect stored data. Data collection is central, ensuring transparency (Nawyn, 2003).

User Behavior Analysis

User behavior analysis – through user behavior analysis IT tools can identify abuses, and as a result of the early detection data theft attempts can be prevented. Digital behavior of the users in fact provides the digital footprint of the users: typical time of accessing the systems, typing speed, screen resolution, servers and services used. Behavioral analysis algorithms can be used to reveal unusual commands executed by database operators and administrators; this behavior is an automatic risk-increasing factor. User behavior analysis is able to identify security events that would remain otherwise uncovered: login with stolen credential is collected though in SngStore Box and is transmitted to SIEM, however, as it is a successful login, it does not generate an alarm in the SIEM system (Hamornik & Krasznay, 2017).

The high-risk system administrator activity became controllable by the so-called Shell Control Box (SCB) / Privileged Session Management (PSM) software that is able to monitor privileged user accounts (One Identity, 2017). The SCB is an activity monitoring device, client and server independent, so it can be integrated. It controls access to remote servers, virtual desktops, and networks and records the workflows of users connected to the systems in movie-like, repayable audit trail domains. Audit logs can be retrieved. The SCB is capable of real-time alerting and intervention in response to identifying suspicious user activity, such as a dangerous command.

Conclusions

Data, information and IT security are key objectives for the company management that are essential in the defense system of an enterprise. Adequate Governance Risk and Compliance system can contribute to the effectiveness and efficiency of an organization and support the enterprise management in its strategic objectives. Software support for security activities is inevitable in managing the risks in the highly digitalized world where the operation is closely connected to various applications which are exposed to security threats.

A number of security solutions are available to address the needs of an enterprise, thereof integrated solutions embedded into the day-to-day business and operational processes provide the best fit to utilize synergies. The features of the software solutions address the various needs of the customers that arise as part of their operations. These solutions generate value for an organization in a number of interconnected forms and contribute to an effective risk management, to transparent, and efficient internal processes, to a stronger control environment and increased process security. This system strengthens the organization in its decision-making process.

In this analysis it was provided an overview of the main attributes of a well-designed IT GRC system that covers the business processes end-to-end. Each of the explained functions - starting from the inventory module; the business impact analysis; the risk management-, governance and compliance functions; data security; data protection and GDPR; business continuity management; network -, IoT - and industrial control system safety, to the access - and log management – contribute to a well-established control framework that is capable of managing the IT risks.

ISSN 2029-6932 (Print) ISSN 2538-712X (Online) https://doi.org/10.33225/pmc/20.15.108

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020

Limitations and Future Research

The literature review and the list of corresponding IT solutions introduced in the research cannot be treated as exhaustive and closed. The nature of data, information and IT security risks and the variety of issues in the affected area – which changes constantly in the dynamic and globalized era of digital economy - indicate the need for future research on this matter. Neither the problems and solutions nor the applied practices are static. Further future research could capture and compare the security issues and solutions and identify the changes in the field of applied software solutions.

References

Anderson, R. J., & Frigo, M. L. (2020). *Creating and protecting value, understanding and implementing enterprise risk management.* Committee of Sponsoring Organizations of the Treadway Commission (COSO). https://www.coso.org/Documents/COSO-ERM-Creating-and-Protecting-Value.pdf

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. (Wireless VITAE).* (1-5). https://doi.org/10.1109/WIRELESSVITAE.2011.5940923

Breithaupt, J., & Merkow, M. S. (2014). *Information security: Principles and practices* (2nd ed.). Pearson.

Cau, D. (2014). *Governance, risk and compliance (GRC) software. Business needs and market trends.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_ins_governance-risk-compliance-software_05022014.pdf

Conrad, E., Misenar, S., & Feldman, J. (2016). Chapter 8 - Domain 7: Security Operations (e.g., Foundational concepts, investigations, incident management, disaster recovery). In Simon, B., & Katsaropoulos, C. (Eds.), *CISSP study guide* (3rd ed., 347-428). Syngress.

Dayarathna, R. (2009). The principle of security safeguards: Unauthorized activities. *Computer Law & Security Review*, *25*(2), 165-172. https://doi.org/10.1016/j.clsr.2009.02.012

Francsovics, A., Kemendi, Á., & Piukovics, A. (2019): Controlling as a management function. In: Szikora, P., & Fehér-Polgár, P. (Eds.), *17th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2019).* (35-42). Óbuda University Keleti Károly Faculty of Business and Management.

Grooby, S., Dargahi, T., & Dehghantanha, A. (2019). Protecting IoT and ICS platforms against advanced persistent threat actors: Analysis of APT1, Silent Chollima and Molerats. In: Dehghantanha A., Choo, K. K. (Eds.), *Handbook of Big Data and IoT Security*. Springer.

Hamornik, B., &Krasznay, Cs. (2017). Prerequisites of virtual teamwork in security operations centers: Knowledge, skills, abilities and other characteristics. *Academic and Applied Research in Military and Public Management Science, 16*(3), 73-92. https://www.uni-nke.hu/document/uni-nke-hu/AARMS_2017_03_05Hamornik_Krasznay.pdf

Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), 247-255.

Marston, S.; Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems, 51*(1), 176-189. https://doi.org/10.1016/j.dss.2010.12.006

Michelberger, P., & Lábodi, Cs. (2012). After information security – before a paradigm change: A complex Enterprise Security Model. *Acta Polytechnica Hungarica, 9*(4), 101-116.

Muse, D. (2017). *10 Top IAM Products*. https://www.esecurityplanet.com/products/top-iam-products.html

Nawyn, K. E. (2003). *A security analysis of System Event Logging with Syslog*. Sans Institute.

Norman, T. (2007). *Integrated security systems design - concepts, specifications, and implementation.* Butterworth-Heinemann.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1-20. https://doi.org/10.1093/cybsec/tyy001

Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). In De Decker B., & Schaumüller-Bichl, I. (Eds.), *Communications and multimedia security. CMS 2010. Lecture Notes in Computer Science, 6109*. Springer. https://doi.org/10.1007/978-3-642-13241-4_11

Racz, N., Weippl, E., & Bonazzi, R. (2011). IT Governance, Risk & Compliance (GRC) status quo and integration an explorative industry case study. In *2011 IEEE World Congress on Services* (pp. 429-436). https://doi.org/10.1109/SERVICES.2011.78

Rasmussen, M. (2009). An enterprise GRC framework: Defining a common governance, risk, and compliance architecture enables all parts of the organization to respond to these challenges together. *Internal Auditor*, *66*(5). https://go.gale.com/ps/anonymous?id=GALE%7CA210607347&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00205745&p=AONE&sw=w

Recor, J., & Xu, H. (2017a). GRC Technology Introduction. In: Tian, W. (Eds.), *Commercial banking risk management*. Palgrave Macmillan.

Recor, J., & Xu, H. (2017b). GRC technology fundamentals. In: Tian, W. (Eds.), *Commercial banking risk management*. Palgrave Macmillan.

Rosenberg, J. (2017). Chapter e6 - Embedded security. In Vega, A., Bose, P., & Buyuktosunoglu, A. (Eds.), *Rugged embedded systems: Computing in Harsh Environments*. (1st ed., e1-e74). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-802459-1.00011-7

Swift, D. (2010). *Successful SIEM log management strategies audit compliance.* SANS Institute. https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528

Vunk, M., Mayer, N., & Matulevičius, R. (2017). A Framework for assessing organisational IT governance, risk and compliance. In: Mas, A., Mesquida, A., O'Connor R., Rout, T., & Dorling, A. (Eds.), *Software process improvement and capability determination SPICE 2017. Communications in Computer and Information Science. 770.* Springer.

Forrester Opportunity Snapshot. (2019). *A Custom Study Commissioned By SAP February 2019 Leverage Intelligent GRC to Drive Business Value.*

IIA Position Paper. (2013). *The three lines of defense in effective risk management and control.* https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

One Identity. (2017). *Balabit Introduces Shell Control Box 5 for Improved Incident Management.* https://www.oneidentity.com/community/news/b/press-releases/posts/balabit-introduces-shell-control-box-5-for-improved-incident-management

Oxford Economics. (2019). *How Finance Leadership Pays Off.* https://www.oxfordeconomics.com/my-oxford/projects/494804

PCI Security Standards Council. (2018). *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1.* https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1586846570804

Secube IT GRC software. (n.d.). www.secube.com

Balasys Solutions. (n.d.). balasys.eu

Your Europe European Union. (2020). *Data protection and online privacy.* https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

ISO/IEC 27001:2013. (2019). *Information technology - Security techniques - Information security management systems – Requirements.*

ISO/IEC 27005:2018. (2018). *Information technology - Security techniques - Information security risk management.*

ISO 22301:2019. (2019). *Security and resilience - Business continuity management systems - Requirements.*

SOX Section 404. (2020). *Management Assessment of Internal Controls.* https://www.sarbanes-oxley-101.com/SOX-404.htm

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 15, No. 2, 2020
124

Received: *June 14, 2020* Accepted: *November 22, 2019*

Cite as: Michelberger, P., & Kemendi, A. (2020). Data, information and it security - software support for security activities. *Problems of Management in the 21st Century*, *15*(2), 108-124. https://doi.org/10.33225/pmc/20.15.108

Pál Michelberger *(Corresponding author)*	PhD, Professor, Institute of Mechanical Engineering and Security Sciences, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Népszínház utca 8., Budapest, Hungary, H-1081. E-mail: michelberger.pal@bgk.uni-obuda.hu ORCID: https://orcid.org/0000-0001-5752-0224
Ágnes Kemendi	PhD Student, Doctoral School of Safety and Security Science, Óbuda University, Népszínház utca 8., Budapest, Hungary, H-1081. E-mail: kemendi.agnes@phd.uni-obuda.hu ORCID: https://orcid.org/0000-0002-6452-8563