Managing information security in healthcare

Velibor BOŽIĆ
General Hospital Koprivnica, Croatia
E-mail address: velibor.bozic@gmail.com

Abstract
Smart city consists of: waste management, smart energy, education, smart communications, smart transportation, traffic management, smart parking, smart streetlights and smart healthcare. All of these areas require management of information safety. Here, the topic is management of information safety in healthcare. The objective is to show the new approach to management of information safety, which involves all employees in this process. Whether manufacturing or service, public or private, organizations increasingly depend on information and communication technology (ICT). ICT presents in such extent that its users are not even aware of its influence. It is a usual part of any organization. However, the dependence on ICT holds a potential hazard for organization's performance. Some issues about the ICT safety should be addressed in every organization. First, does the management of an organization is aware of the potential risks and problems in the ICT area, such as potential ICT unavailability (risk culture) or accidental damage? Is there a systematic approach to threat identification, vulnerability exploration, and evaluation of the impact of realized threats on the business? Is an organization aware of the value of ICT, which should be treated in the organization as any other asset influencing business efficiency and effectiveness? Preventive and corrective actions (system of controls) are warranted for mitigating the risk of destruction or abuse of ICT. In this paper, we discuss these questions and suggest possible solutions. There are many works about the topic but these are stressed only one segment in management of information safety. We used case study, observation and structure analysis in our exploration. The results will be presented here. The results will be useful for everybody who is worried about information security in organizations. Value of this paper is showing the need of multidisciplinary approach in management of information safety.

Keywords: healthcare sector, information systems, risk, risk management, COBIT, ISO 27799.

1. Introduction
We live in the 21st century, in which organizations in the broadest sense of the word (production, non-production, service…) are completely dependent on communication co-information technology (I K T), whether they want to admit it or not. Their survival entirely dependent on the effect that the effective and K here. Complete dependency also carries with it the risks of doing business. The risks, viewed as a combination of the likelihood of an event occurring and the impact of that event on the business, can be both positive and negative. There are countless examples of such a claim through history. Let's just stay in the area of IK T. Would Bill Gate s has failed to take the risk? Probably with a certain amount of security, he went into the risk of founding Microsoft, and the rest is slowly becoming a legend ... On the other hand, security lapses related to Sony's gaming consoles have caused major financial losses to the company, but what's worse is the loss of reputation among users. These are just two isolated examples that confirm the fact that risk can have both positive and negative consequences.

Risk can be both a driver and an impediment to business at the same time. It is an inseparable part of an organization's business and has to be put under control in order to achieve its business goals.Whether it is production or non-production (service) activities, the application of communication information technology becomes a critical factor on which the fulfillment of the business strategy, efficiency and effectiveness as well as the

viability of the organization depends. The dependence of the organization on the good functioning of information technology is a risk in itself at the highest level of business. How to deal with that risk?Do you accept him, fight him or ignore him? What is the relationship between management and IT risks?Are owners and managers aware of IT risks or not? Can we teach management how to deal with IT risks?[1], [2]

The question is, can we manage risks in general and then in the field of information technology? The answer to this question will attempt to crystallize in this paper. In order for an organization to be able to make the most of positive risks and to deal with negative risks with quality, it is necessary to have knowledge of risk management. Good risk management in the field of information technology is possible and will be the subject of this paper. Information technology risk management contributes to the efficiency and effectiveness of the business and the achievement of the organization's vision.[1]

2. Context of smart healthcare

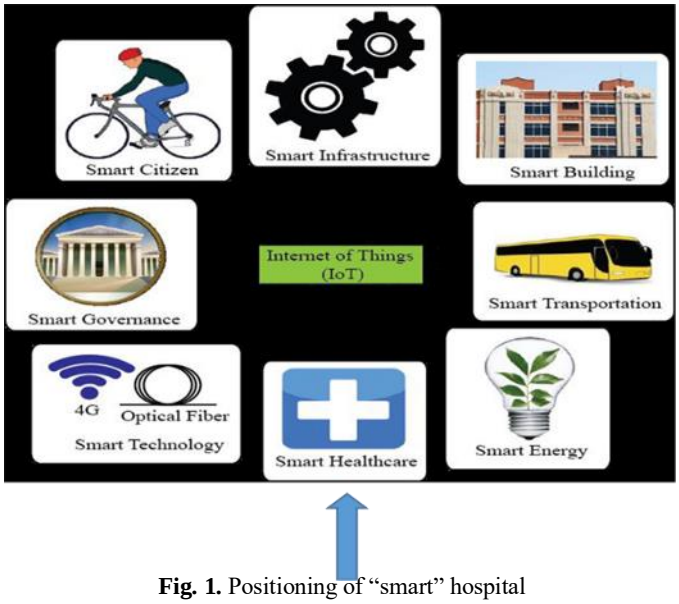

Fig. 1. Positioning of "smart" hospital

The goal of hospital information and communication technologies is to create so-called a smart hospital, that is, a hospital that continually learns and thus improves its business processes, refines the knowledge of its employees, monitors the latest technology, and thus influences patient satisfaction and, indirectly, financial results.

2. 2. A smart hospital viewed through the application of information and communication technology

In smart hospitals [2], various mechanisms are used for their operation, which include ICT, cloud computing, smartphone applications and advanced data analysis techniques. Patient information can be accessed in real time at various smart hospital offices or even at various smart hospitals in different cities or in the same city. Doctors, nurses, and medical

technicians can access test data without losing time when physically transferring the same data from one office to another. Similarly, different doctors may see information to judge a patient's condition. Therefore, real-time decisions about the patient's health can be made.

Telemedicine can be considered as a specific example of smart healthcare. Telemedicine can also be considered as a subset of smart healthcare. Telemedicine uses information and communication technologies (ICT) to provide long-distance or remote healthcare. This approach is especially useful for places where health services are not easily accessible; telemedicine removes obstacles remotely and improves access to medical services in remote locations

3. Purpose of protection management and information systems in hospital

Protect the **confidentiality , availability and integrity** of patient information [8], [9]

Elements that must be satisfied when protecting information:

- Patients, public, employees, laws and regulations, management, supervision (Governing Council?)
- All of them must be satisfied in some way in the context of protecting the integrity, protection and availability of information. Risk must be taken into account when protecting data.
- risks
- The confidentiality, availability and integrity of information are affected by many threats that attempt to exploit system vulnerabilities. As a function of the likelihood of a threat taking advantage of the vulnerability of the system, the magnitude of the consequence that threat can cause is a risk. [7]
- By protecting information systems, the risk must be reduced to an acceptable extent.
- The essence of managing information security systems (what is this about?)
- Confidentiality, availability and integrity of information are at **risk.** Increasing risk is directly affected by **threats to the** system. Threats exploit the **vulnerability of the** system. System vulnerability also increases risk. System vulnerability allows exposure **of** system **assets** (information in this context). System assets have some **value** that affects the overall **organization.**
- Risk directly affects the value of an asset by reducing it. The organization (the hospital in our case) has certain **security requirements.** These security requirements are met through certain **controls.** Controls are key to reducing risk (meeting the requirements for confidentiality, availability and integrity of information). The controls help to protect against **threats** against the system. This closes the system protection circuit.

Risk factors in health care facilities include medical factors (e.g. Medical errors, nosocomial infections ...), financial factors (uncontrolled borrowing /payment, no common cost management, poor financial management ...), regulatory factors on re (disrespect of laws, regulations, directive…). In medical institutions there is a high risk of unavailability of data, unauthorized access to data, and unauthorized alteration of data. In order to reduce all these risks to an acceptable level, the risks should be managed. There are three basic risk management mechanisms:

- BSC (Balanced Scorecard) - strategic level (BSC / 4A matrix) [15], [16]

- COBIT 4.1 + IT Risk (COBIT 5.0) - tactical level (control targets should be grouped into one of A (access, availability, accuracy, agility) in the so-called 4A approach)
- ISO 27799: 2008 - Operational level - Specific activities. [13], [14]

The three mechanisms listed below will be explained in more detail. But before that, something about the roles in risk management.

4. Roles in risk management

Roles of management (hospital management) in risk management: [3], [11], [12]

- assessing the nature of the risk and defining the level to which it must be reduced in order to be acceptable to the business
- risk likelihood estimation
- determining how to manage unacceptable risks
- defining the ability of an enterprise to minimize the likelihood of threats occurring and their impact on the business
- identifying the costs and benefits of risk and determining control activities
- defining criteria for measuring the effectiveness of risk management
- Consideration of the impact of risk on the decisions of the Management Board.
- The roles of CEOs (members of the Hospital Expert Council) are:
- have responsibility for conducting risk management daily
- need to spread risk awareness within the areas they manage
- need to familiarize employees with the goals of risk management
- They must ensure that risk management becomes an equal topic with all other topics at management meetings.
- They must ensure that risk management is integrated into the project as one of the project phases without which the project itself cannot be successfully completed.
- In addition to the roles mentioned above, the Board and CEOs have a common role to play in ensuring effective and efficient risk management, which means that:
- adopt risk management policies and strategies
- define risk management at the strategic and operational levels
- create a culture of risk awareness in the company
- provide risk monitoring processes
- coordinate activities within the company that are related to risk management
- develop risk responses (what to do if risk is achieved - business continuity programs)
- Prepare risk reports to owners and anyone else interested in the business.
- For effective risk management, the company also needs internal control. The roles of internal control are:
- controlling critical risk management (identified by management)
- pointing out possible failures in the management process
- assistance in identifying risk to
- coordinating risk reports with management and owners

5. Balanced Scorecard

Kaplan and Norton introduced the idea of the Balanced Scorecard (BSC) in January - February 1992. The need for such a tool meant recognizing that measuring financial results alone was not enough to manage a modern organization. Most of the work that is done in

organizations today should not only relate to the processing of financial results - much more attention than so far should focus on achieving process improvement, employee training, inventing new ways of connecting with customers. It could be said that these activities are the cornerstone of a successful organization. They allow for more efficient management by helping to achieve a business strategy. Without a metering system that reflects a balanced view of organizational goals, managers behave as if they were driving a car looking in the rear mirror or operating a plane by looking only at a height measuring device [17].

In the basic version, the BSC includes four types of views on the organization: Finance, Buyers, Internal Business Processes, and Learning and Development. Some organizations also add a fifth area or replace all perspectives with one that is a unique reflection of their mission and strategy. For example, some organizations add an environment dimension to their scorecard. Nevertheless, the four perspectives described by Kaplan and Norton are generally applicable across organizations. An example for a hospital might look like this:

- *Patients*
  - Increasing patient satisfaction - faster response, shortening of treatment, choice of medical treatment methods, existence of informed consent, better protection of information
- *Finance*
  - Growth - timeliness of financing (inflow of funds needed for the functioning of health institutions
  - Profitability - Effective and cost-effective activities
  - Liquidity - analysis of the factors that determine the flow of money, better control of equipment and services that affect fixed assets
  - Stability - Better control of t labor costs
- *Internal processes*
  - Improving the quality of medical services - creating standardized medical procedures, research and problem analysis
  - Medical risk management - monitoring of medical practice, existence of traceability (from procurement of materials and medicines through to administration), minimizing medical error
  - Business Process Improvement - Simplifying and accelerating processes and separating professional and standardized processes.
  - Use of Information - Sharing information according to the "necessary piece of information, the one who really needs it"
- *Learning and growth*

What do we need to learn to really grow?

- 80

The BSC provides a fairly comprehensive overview of what happens to the business system when not just traditional financial measures are taken into account. That's just part of the BSC approach. The real benefit of the BSC approach is to create a scoreboard that reveals the assumptions for good business. The strategy will show that actions in the area of learning and growth affect the improvement of internal business processes that will meet specific customer goals and thus affect the financial result. BSC affirms a balanced

approach to business analysis, which means that critical success factors in the cause-and-effect relationship are sought.

Management defines the mission (why we exist) and the vision (where we want to go). Based on the mission and vision, a strategy is defined (the way to achieve the vision). Strategic goals should be defined in order to implement the strategy. They can be reached by different techniques (e.g. SWOT analysis). Strategic goals for medical institutions could be:

- Achieving and maintaining a high level of security and protection of patients' personal information
- Establishing and maintaining a high level of medical services
- Minimizing medical errors
- An immediate response to the medical needs of the community we are in
- Improving the exchange of information between medical facilities and the community
- Increasing staff skills and knowledge
- Identifying and addressing new challenges
- Implementation of collaboration between health system elements
- Setting up a system for full support for the health system
- Establishing a better environment for physician research work and advancing medical care

When defining strategic goals, care must be taken that they are in line with the mission and vision and that they are achievable, measurable, realistic and timely. For each strategic goal it is necessary to determine a series of activities, i.e. the process by which that strategic goal can be achieved

Failure to fulfill, i.e. poor implementation of each of the above strategic goals represents a strategic risk. Below I present the so-called. A "BSC / 4A" matrix that provides an overview of the technique by which the Management Board defines the relationship between business objectives, risk and business impact.

Table 1. List of strategic risks: [3], [10], [14], [15], [16]

BUSINESS OBJECTIVES	**IMPACT ON THE JOB (risks)**	**4A business impact**			
		agility	**accuracy**	**access**	**availability**
FINANCES					
Ensure return on investment in IT	Inadequate financial and return on IT investments	P			
Manage IT risks	IT risks are not managed, the company is insecure	P	P	P	P
Improve corporate governance and transparency	Insufficient transparency towards stakeholders, non-compliance with legislation	P			

BUYERS (users)						
Improve customer and service focus	Poor or insufficient customer service, loss of customers			S	P	P
Offer competitive products and services	Inadequate products and services; fail to meet customer needs; loss of income	P	S	P	S	
Setting up continuity and availability of services	Insufficient service levels result in customer dissatisfaction and loss of income			S	P	P
Create agility in line with new business requirements	Failure to respond to market changes or customer demands in a timely manner is a loss	P	S			
Cost optimize service delivery	Products or services that are too expensive cause uncompetitiveness and loss of customers	P				
Real and effective reporting is essential for decision making	Poor decisions at the strategic level result in the loss of clients; losses and decline in the value of the organization	P				
INTERNAL PROCESSES						
Improving and maintaining the functionality of internal processes	Inefficient and under-optimized processes in the organization			P	P	
Lower process costs	Lower profitability	P				
Compliance with laws, regulations and contracts outside the organization	Violation of the same results in criminal responsibility of the administration and those responsible			P	P	
Compliance with internal policies	Inefficient and inadequate processes			P	S	S
Business change management	Insufficient processes lead to non-	P				

	competitive arrowheads	
Improve and maintain staff productivity	Failure to do so reduces productivity and efficiency	P P
LEARNING AND GROWTH		
Product and business promotion management	Loss of chances, small growth, loss of market share	P
Attracting and retaining skilled and motivated people	Impossibility of progress (organization growth and current operations growth)	P S

P - PRIMARY IMPACT
S - SECONDARY IMPACT

6. COBIT - tactical level

It is at the tactical (CEO level) level that the benefits of COBIT are great because it ensures the quality implementation of the hospital information system and the management of operational risks. [1], [3], [19]

6.1. About COBIT

COBIT is an acronym for Control Objective for Information and Related Technolgy. It was created in 1992 under the auspices of two organizations: the Information Systems Audit and Control Association (ISACA) and the IT Government Institute (IGI). COBIT enables managers, supervisors, IT users to have a set of measures, indicators, processes and examples (best practice) that help them to maximize the benefits of information technology and develop appropriate management and control of business processes in their organizations.

COBIT offers a chance for IT not only to be an IT service provider but a strategic business partner. Its key role is to enable the control of all IT processes, to direct them towards constant verification and security of performance. The goal of COBIT is to manage business services and should address the so-called IT surplus, i.e. underutilized IT, on the other hand, should ensure that IT can support the requirements of the business system (IT deficit should be disabled) .

COBIT supports corporate IT, i.e. IT governance, by providing a framework within which to present domains, processes, activities in a useful and logical way. It consists of four basic domains and 34 processes within domains. Domains are:
Planning and organizing. This domain is about strategy and tactics; it defines the best way in which IT can contribute to the achievement of business goals.

Acquisitions and implementation. The subject of interest here is the realization of the strategy. IT solutions are defined, developed and enriched, implemented and integrated into the business process.

Delivery and support. This domain refers to the delivery of the services required, which includes the delivery itself, security management (RISK!) and continuity, customer service support, data management and operational services.

Supervision and evaluation. Over time, every IT process needs to be monitored to see if it works according to customer requirements. Within this domain, performance is managed, internal controls are monitored and processes are regulated.

Through these four domains and 34 processes within these domains, COBIT is achieving its purpose, which is to support the delivery of business services. But in addition to being process-oriented, COBIT is job-focused, control-focused and measurement driven. Focusing COBIT on business means that it is not only a tool for IT service providers, users and controllers, but it is a clear guide to managers and business process owners. This is because quality information is crucial to decision making, and information management and control are at the heart of COBIT. COBIT ensures that information is effective, efficient, confidential, if necessary, accessible, lawful, secure and verified. COBIT is focused on control through control objectives that ensure the quality of each of the 34 processes. In addition to process-specific goals, there are global goals that apply simultaneously to all processes in all domains. COBIT is a moving measurement ma. This means that within the COBIT -apply performance measurement to achieve the objectives and processes. In particular, the CMM model for determining the maturity level of a particular IT process is applied to determine the current state of the process and the need for improvement. There is an initial level and five further stages of maturity. These are: initial / ad hoc phase, repetitive but intuitive, defined process, manageable and measured, and optimized phase.

The basic COBIT principle is as follows: on the basis of business requirements, investments in IT resources are initiated. IT resources are used in IT processes. IT processes deliver business information. This business information responds to customer requests. Through this principle, it supports the core areas of business management: *strategic alignment* (linking business and IT plans; defining, maintaining and evaluating IT values, aligning IT and business operations), *delivering value* (ensuring that IT delivers business-relevant information, in line with strategy), *resource management* (optimal investment in resources[1]), *RISK MANAGEMENT* (requires awareness of the existence of risk by management, understanding the need for risk to be without progress, agreeing on significant risks, defining risks for the organization), *measuring performance* (monitoring implementation of strategies, execution projects, use of resources, process execution and delivery of IT services; BSC is used for monitoring).

The concept of goal in COBIT is crucial. There is a hierarchy of goals here. At the highest level is the business objective. It is achieved through IT goals. Each IT goal is realized through the achievement of process goals. Each process objective consists of a series of

activity goals. The achievement indicator of each goal in COBIT is called a scorecard (in earlier versions it was the so-called key goal indicator). The scorecard indicates whether a goal has been achieved. It is always used after the event. Performance indicators (previously key process indicators) are linked to the goal and its achievement. Performance indicators indicate whether there is a chance of any goal being met. It actually shows the ability of a process to accomplish a goal, sometimes called a performance engine (in BSC for example).

Due to the hierarchy of goals, the same thing that at the higher level was the benchmark of results, at the lower level it becomes an indicator (driver) of performance.

In COBIT, every IT process has a specific view structure. There are four parts to the view:

- First part:
  - Information criteria are presented (what information must be)
  - What business requirement does the IT process satisfy
  - Through the achievement of its goals, the IT process meets the business requirement
  - What activities does the IT process take to achieve the goal
  - How goal achievement is measured
  - Which business area within the business management IT process primarily processes, and which secondarily supports
  - What IT resources process used to achieve the ci mound
- The second part:
  - Contains control objectives for the purpose of the IT process
- Part Three:
  - Contains inputs and outputs from the process (these are activities from different domains)
  - So called. RACI matrix showing what activities the IT process is comprised of, and who is responsible for each activity, who counts, who consults, and who informs; Responsible, Accountable, Consulted, Informed)
  - The RACI matrix also shows the functions required to fulfill the purpose of the IT process (management, IT chief, executive director, manager, employee, project manager)
  - Goals in a hierarchical relationship and metrics for measuring achievement
- Part Four:
  - Model of maturity of IT process according to CMM model.

COBIT is a good practice for managing IT in the organization and managing IT risks at the middle management level. COBIT processes used in risk management:

- Planning and organization
  - communicating management goals and directives through the organization
  - human resources management
  - assessment and management of IT risks
  - project management
- Procurement and implementation
  - identification of automated solutions

    - enabling operations and use
    - installation and accreditation of solutions and changes
- Development and support
    - defining and managing service levels
    - performance and capacity management
    - play continuous service
    - ensuring system security
    - user education and training
    - data management
    - managing the physical environment
- Supervision and evaluation
    - proper process measurement and evaluation

The description of each of these processes goes beyond the scope of this paper, so it will be avoided at this point. Only the role of the risk assessment and risk management process will be emphasized.

Process of risk assessment and management

The goal here is to set up an IT risk management framework. This means that acceptable levels of risk, risk reduction strategies and acceptable residual risk should be documented. It is essential that there is a consistency of business and IT risk-related goals. Any adverse event that may have an impact on the business should be able to identify, analyze and evaluate its significance. The task of mitigation strategies must be to reduce the risk to an acceptable level. The result of the risk assessment must be understandable to the owners and must be expressed in financial terms so that decision makers can reduce the risk to an acceptable level of tolerance.

7. Operational level - specific activities

ISO 27 799: 2008 is the standard for establishing information security in medical institutions. Information security involves protecting information from threats [13], [14]. The goal of information security is to ensure business continuity, minimize business RISK, and maximize return on investment and business opportunities.

Information security is achieved through the implementation of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. All of these controls should ensure, implement, monitor and enable reporting of business objectives. Information security is important in all organizations because it protects critical assets that have some value.

Information security is achieved through:

- The risk management process in the organization
- Compliance with laws, regulations, contracts, regulations
- Meeting business requirements that prescribe the way information is processed to support operations within the organization

A prerequisite for quality information security management is risk management. The results of risk management are the basis for managers to make decisions about increasing information security and implementing controls.

The set of controls that must be implemented in each organization are:
- Statutory controls
  - protection of personal data
  - protection of organizational records
  - protection of intellectual property
- Controls that represent "good practice" in achieving information security
  - information security policy
  - allocation of responsibilities for achieving information security
  - awareness of the need for information security, education and training
  - proper processing in applications
  - managing technical vulnerabilities
  - business continuity management
  - Managing and enhancing information security incidents.

Critical success factors for achieving information security:
- The existence of an information security policy, goals and activities that reflect business goals
- Defining approaches to creating, maintaining, monitoring and improving information

Security that is in line with the organizational culture:
- Visible support and commitment from all levels of management
- *Good understanding of information security requirements, risk assessment, risk management*
- Effective information security of all managers, employees and all other interested parties (shareholders, partners, etc.)
- Distributing information security guides (based on policy and standard) to everyone in the organization
- Creating and increasing the pool of information security activities
- Facilitating the creation of a “risk culture”, education and training
- Establishing effective information security incident management
- Implementation of a measurement system that assesses the performance of information security management (feedback for process improvements).

7.1. Specific health threats
Some of the threats to ICT in healthcare:
- Unauthorized access to data inside and out (stay in the program after termination of work - another person uses the program under someone else's password; compromised confidentiality and integrity
- Unauthorized use of the health information system - poor user identification and authentication, poor access control and privilege management
- Openness to malicious software (viruses, trojans, worms)
- Intruders into communication and destruction of messages

- Refusing to receive or send sensitive information due to lack of digital signature
- Errors when connecting to network services 8npr. Payment via CEZIH)
- Inadvertently sending sensitive information to wrong addresses
- Technical errors (servers, network, computers…)
- Lack of backup variants in case of power failure, fire, floods
- System malfunctions - inability to use the repair shop
- Errors in the application software functioning
- Operator errors (system administrators, network administrators)
- Maintenance errors
- User errors
- Staff shortages
- Data thefts inside / outside the organization
- Deliberate destruction of the equipment inside and out
- Terrorism

7.2 Management support (mastering IT as an essential prerequisite)

Management support is crucial to establishing an information security management system. Management must be fully committed and actively involved in the process of introducing an information security management system. Management support is reflected in written and oral statements that emphasize the importance of the security of medical information. Management must create a climate of readiness for change; it must be prepared to withstand resistance. On the other hand, management must define strategic threats, i.e. areas of information security that are essential to the business. Management must establish a body to implement the information security management system. This body should include a management representative, a lawyer, a finance manager, a quality manager and an IT manager, and a doctor who has complete knowledge of medical processes. This body should define:

- The goals of protecting information in healthcare
- What health information to protect
- Build an information security management system.

7.3. Health information which must be protect

There are several types of information whose availability, integrity and reliability need to be protected. Those are:

- Patient personal health information
- Pseudo patient information generated for some research purposes
- Information collected for statistical research purposes, including anonymous information derived from personal health information (in which no identifying information is available)
- Clinical / medical knowledge not related to the specific subject of medical care, including data used to make clinical decision-making (e.g., medication response data
- Information on health professionals, staff and volunteers
- Information relating to public health surveillance
- Trial-related information related to patient treatment
- Information produced by information systems; this also refers to controls that serve to access sensitive information (passwords, usernames, PINs, etc.).

The rigor of preserving the availability, integrity and reliability of information depends on the nature of the information being protected. For example, statistics need not be as confidential (everyone can see them, they are publicly available, but their integrity must be complete — not everyone can change them). For example, trial records related to the course of treatment need not require availability (in the sense that they must be available at the same second - response time may not be instantaneous), but their content must be completely reliable (this information may not be available to everyone).

What information will be retained depends on the risk assessment process. Risk assessment determines the level of effort, i.e. the need to preserve the availability, integrity and reliability of information.

Medical information to be protected (above all confidentiality):

- Personal information about patient health (electronic health record)
- Patient data within which patient identification is disabled by cryptography (for statistical purposes)
- other medical data for statistical purposes 8 data not necessarily related to patients)
- Non-patient related medical information (i. e. information on drug reactions, hospital infections, etc.)
- Information on medical staff, doctors
- Public health data
- control data, derived from the hospital information system
- Password, usernames, i.e. data essential to enforce confidentiality, integrity and availability controls.

7.4. Building an Information Security Management System - deming circle

Planning

Step 1: Define the scope of the information security management system
Step 2: Plan policies within the information security management system
Step 3: Plan a systematic approach to risk assessment
Step 4: Risk identification (assessment of risk factors and information assets)
Step 5: Perform a risk assessment
Step 6: Risk Relationship Planning
Step 7: Choosing a management goal and controls
Step 8: Preparing the Statement of Eligibility
Step 9: Recognizing the residual risk and letting the information security management system come to life

Documents generated here: description of system being monitored, security policy identified, diagram of management structure re management system inf. with promptness (who is responsible), and information asset identification procedures, inventory of information assets, risk list, risk assessment procedure, risk assessment report, risk treatment procedures, risk treatment report, risk treatment plan, information security measurement criteria, and statement of eligibility.

Do
Step 1: Perform the risk reduction process
Step 2: Allocation of business resources by management
Step 3: Using controls (planning required procedures)
Step 4: Perform training and training
Step 5: Operations Management
Step 6: Business Resource Management
Step 7: Define actions in the event of a security incident

Documents that result from this phase: risk management plan, information security plan, business information continuity plan, education and training plan, education and training procedures manual, procedures for managing information protection documents, training and education reports, on security operations conducted, plan for measuring the severity of security incidents, report on measurements of security incidents.

Check
Step 1: Monitor procedures and controls
Step 2: Oversight of the information security management system (monitoring the effects of the system, residual and acceptable risk).
Step 3: Report to Management

The documents that are generated in this step: Plan, procedures and checklists for internal audit; training and education reports relating to the information security management system, reports on information security enhancement operations, reports on benchmarks that determine the severity of information incidents, internal audit reports; minutes of meetings reporting to the management on actions taken, minutes of meetings of the task force to set up an information security management system.

Act - Correction (action)
Step 1: Define measures to improve the information security system (corrective and preventive actions)
Step 2: Discuss through the organization the actions that are being taken.

The documents that result from this step are the Risk Management Plan (accepting, avoiding, reducing or transferring risks), corrective and preventive procedures.

7.5. Information security areas (not just usernames and passwords)
When managing information security in healthcare, there are 11 main areas to be considered:

- **information security policy**
    - drafting an information security document
    - review of information security document (and changes if necessary)

- **information security organization**
    - internal organization

- Management commitment to information security
- Coordination of information security
- Sharing responsibilities for information security
- Authorization of the process of information processing by those responsible
- Confidentiality agreements
- Communication with experts
- Communication with stakeholders

- independent assessment of information security
- external organization
  - identification of risks associated with external partners
  - determining risk when we allow partners to access organizational assets
  - determining security measures in outsourcing contracts

Outsourcing

- **Asset Management**

Liability for the property

- property inventory
- ownership of the property
- acceptable use of property

Classification of information

- classification guide (how to classify information in categories of their value, sensitivity, importance to the organization
- managing and tagging information

- **Human resource reliability**

Pre-employment activities

- Roles and responsibilities
- Supervision (employee verification)
- Conditions of employment a

Activities during employment

- management's responsibility to familiarize the employee with information security policy
- developing awareness, training and education on information security
- disciplinary action for breach of security
- finishing or changing jobs
- responsibilities when completing work
- return of property
- extinguishing access rights

- **Physical and environmental safety**

Safe areas

- defining physical security barriers
- Physical input control
- Safe rooms, offices, etc. (system room)

- Protection against external and environmental threats
- Work in safe areas
- Public access, delivery areas

Equipment safety

- Installation and protection of equipment
- Support services (power, electricity, fire protection, air conditioning…)
- Cable security
- Equipment maintenance
- Maintenance of spare equipment
- Safe disposal and reuse of equipment

Equipment exclusion (equipment removal must be authorized).

- **Communications and Operations Management**

Operating procedures and responsibilities

- Documented operating procedures
- Change management
- Division of duties
- Separation of development, testing and operations functions

Managing outsourcing deliveries

- Service delivery (SLA contracts)
- outsourcing oversight and reporting
- Change management of outsourcing services

System planning and adoption (minimizing the risk of systematic errors)

- Capacity management (controlled use of resources)
- System acceptance (new IS, new versions, changes…)

Protection against malicious and mobile code

- Controls against malicious code
- Controls against mobile code

Backup

- Backups of information

Network security management

- Network controls
- Security of network services

Media management

- Management of transmission media
- Media disposal
- Information management procedures
- Security of system information

Information exchange

- Information sharing policies and procedures
- exchange contracts (referring to partners outside the organization)
- securing physical media in transit
- Defining electronic messages
- A way of developing business information systems

Electronic commerce services
- Protection of electronic commerce
- Online transactions
- Publicly available information

Supervision
- Control records
- Defining the use of surveillance information in the system
- Protection of surveillance records
- Existence of records of administrators and operators
- Error logs
- Time synchronization

- **Access control**

Business access control requirements
- Access control policy

Managing user access
- User registration
- Privilege management
- User password management
- User rights review

User responsibility
- Use of passwords
- User equipment properly protected
- Protection of sensitive information on desktop and computer

Network access control
- Policy for using network services
- Authentication of users with external access
- Identification of equipment online
- Remote diagnostics and configuration of network inputs (must be controlled)
- Divide the network into smaller segments for ease of management
- Control of network routing

Access control of the operating system
- secure login procedures
- User identification and authentication
- Password management system
- Use of system services
- Session timeout

Access control of applications and information
- Restricting access to information
- Isolation of sensitive systems

Mobile computing and remote work
- Defining the conditions of mobile computing and communications
- Defining remote working conditions

- **Procurement, development and maintenance of information systems**

Security requirements of information systems
  - Specification and analysis of security requirements

Proper processing in applications
  - Validation of input data
  - Control of internal processes
  - Message integrity
  - Validation of output data

Cryptographic controls
  - The policy of using cryptographic controls
  - Managing cryptographic security keys

System file security
  - Control of operating software (software within the operating system)
  - Protection of test, system data
  - Control access to program source code

Security in process development and support
  - Change control procedures
  - Technical review of applications after changes
  - Restrictions on application changes
  - prevent information leakage
  - outsourcing control of application development

Managing technical vulnerability
  - Control of technical vulnerability

- **Information security incident management**

Reporting on events and weaknesses within information security
  - reporting on information security events
  - reporting on security weaknesses

Managing and enhancing information security incidents
  - defining procedures and responsibilities
  - Learning from incidents
  - gathering evidence

- **Aspects of information security in business continuity management**
  - incorporating information security information into the business continuity management process
  - Risk assessment and business continuity
  - setting up a business continuity planning framework
  - Testing, maintaining and re-evaluating business continuity plans

- **Compatibility**
  - Compliance with legal requirements
  - Identification of applicable legislation
  - Intellectual property rights

- Protection of organizational records
- Protection of data and especially personal data
- Prevention of misuse of information processing
- Regulation of cryptographic controls

Compliance with security policies and standards and technical compliance

- Compliance with security policies and standards
- Check technical compliance with safety standards

Considerations for controlling information systems

- Information systems monitoring controls
- Protection of information systems control tools (special software or data).

Information security risk assessment and treatment is the basis for setting up an information security framework. Through identification, quantification, determination of importance of risk and determination of risk response, *activities and priorities for information security management are determined.*

The basic security requirements are confidentiality, integrity and availability of information. In healthcare, special attention is paid to *confidentiality,* i.e. the possibility of access to information only to authorized persons. In the second place is the *lack of* data, i.e. the prohibition that anyone can change the patient's data, as this can be dangerous even for the life of the patient. Because healthcare needs to respond on time, system *availability* is imperative at all times.

8. Conclusion

In this paper, I have attempted to highlight the complexity of health risk management. Managerial risk management skills cannot be reduced to IT, usernames and passwords. The field is much broader and more complex, and the introduction of risk management into healthcare must be organized as a project with a multidisciplinary approach if the problem is to be resolved with quality.

References

[1]Ž. Panian, M. Spremić et all. (2007), "Corporate Governance and Auditing of Information Systems", Zgombić & Partners - Publishing and Informatics Ltd., Zagreb.
[2]M. Crouhy, D. Galai, and R. Mark (2006), "The Essentials of Risk Management," The McGraw-Hill Company, New York.
[3]R. R. Moeller: "COSO Enterprise Risk Management" (2007), John Willey & Sons Inc., New Jersey.
[4]C. Alberts, A.Dorofee: "Managing Information Security Risks (2009), The OCTAVE Approach," Addison-Wesley, New York.
[5]P. Gregory (2008), "IT Disaster Recovery Planning for Dummies", Wiley Publishing Inc. New York.
[6]S. Snedaker (2007),: "Business Continuity & Disaster Recovery for IT Professionals", Syngress Publishing Inc., Burlington, MA, USA.
[7]G. Westermann, R. Hunter (2007), "IT Risk: Turning Business Threats into Competitive Advantage", Howard Business School Publishing, Boston.
[8]CL Pritchard (2001),: "Risk Management: Concepts and Guidance," ESI International Press, Arlington-Virginia, USA.
[9]JP Chavas (2004), "Risk Analysis in Thery and Practice", Elseiver Academic Press, London, UK.
[10]G. Monahan (2008), "Enterprise Risk Management: A Methodology for Achieving Strategic Objectives" by John Wiley & Sons Inc. New Jersey.

[11]ISO / IEC 31000: 2008 Risk management - Principles and guidelines on implementation
[12]ISO / IEC 31010: 2009 Risk management - Risk assessment techniques
[13]HR EN ISO 27799 (2008), Medical informatics - Information security management in healthcare facilities using ISO / IEC 27002 (ISO 27799: 2008, EN ISO 27799: 2008)
[14]ISO / IEC 17799 (2005), Information technology - security techniques - Code of practice for information security management
[15]"The RISK IT Practice (2010)," ISACA Press.
[16]"The Risk IT Practitioner Guide (2010)," ISACA Press, "COBIT 4.1 (2007)" ISACA Press. ADDITIONALLY.
[17]Kaplan, Norton (2001), "The Strategy Focused Organization", Harvard Business School Press; Boston, USA.
[18]Olve, Roy, Wetter (1999), "Performance Drivers - A Practical Guide to Using the Balanced Scorecard"; John Wiley & Sons; Chichester, England.
[19]ISACA, ITGovernance Institute: "COBIT 4. 1", "COBIT 5.0 Framework", "COBIT Mapping ISO / IEC 17799: 2005 with COBIT 4.0"; ISACA Press, London; 2001-2006.