American Research Journal of Humanities & Social Science (ARJHSS)
E-ISSN: 2378-702X
Volume-03, Issue-06, pp 169-184
June-2020
www.arjhss.com

Research Paper **Open Access**

Informatıon Technology Management And It Rısks

Asst. Prof. Dr. Bulent Gunceler
İstanbul Okan University, Turkey Faculty of Business and Administrative Sciences
Orcid Nr. 0000-0002-3332-0751
**Corresponding author: Asst. Prof. Dr. Bulent Gunceler*

ABSTRACT: *This article sets out the basic concepts that describe international practices in information technology management and information security rules. It highlights what has to be followed in order to manage them successfully. These concepts can be mentioned as : reliable management of information systems; secure data storage and protection; IT risk management assessments and mitigation of theserisks. It describes universal rules on securing data, protecting them against external threats, disaster recovery and business continuity plans.*

Key words: *IT Management, Information Security, IT Risks, Disaster Recovery, Business Continuity*

I. INTRODUCTİON

Information Technology (IT) has become the most rapidly spreading miracle solution for institutions during late 1900s. It has entered to personal lives by revolution of digital developments during commencement of Millennium. When you compare the big change from stone-age level of technical infrastructure of those days with today's high-tech features; you can easily see that difference is unmeasurable.

IT is a concept, that refers to digital technology, i.e. hard- and software for creating, collecting, processing, storing, transmitting, presenting and duplicating information. The information may be in the shape of e.g. sound, text, image or video, and IT mean hence a merging of the traditional areas of computers, telecom [1] and media.

This means, everything in human's activities are embadded to daily life and unevitable. We can name digital technology as a stairway to a voyage from past to future. Just try to compare the distance; from gramophones to i-pod, from kites to remote control toy or drones, from 4 engine airplanes to space shuttles, from analoge telephones connectable by help of operators to smart phones, from typewriters, heavy duty calculators at the office to very advances softwares, from physical controls and inspection to remote, digital controls and thousands ofchanges in daily and business life has changed the world into a new era.

Technology is in our lives at everywhere. Business life, production and commerce has taken a great slice from this changing crowd and continuing its development in an uncontrollable speed. It is definite that IT has brought uncountable features to our lives by bringing in high speed, rich data collection and storage, easy access to transactions, fast delivery of works, increased efficiency in production, quick integration to any place in the world and so on. But, among all of these good facilities, how about looking at IT from a different angle?

What happens if someone uses these facilities of technology with malicious intent? Is it possible? Sure it is. A qualified programmer can increase or decrease the interest of a product in a company, by changing one dot in the computer program. Or the quantity of the stocks in the warehouse list can be changed by deleting one line in the accounting program. Or, the cost analysis may be manipulated to a different route by playing with the formula of the calculation. This reveals the fact that, very fast growing digital technology is containing fantastic features in itself however may become a nightmare if it is used with a different approach. This leads us to the concept to be named as: effective and adequate IT Management to have smoothly running information systems and to avoid any risks that may arise from the institution's IT infrastructure.

II. WHAT İS IT MANAGEMENT ?

IT Management refers to the monitoring and administration of an organization's information technology systems: hardware, software and networks. IT management focuses on how to make information systems operate efficiently. Just as important, it's about helping people work better. Increasing numbers of organizations are putting IT at the center of their strategies. In the digital world, IT departments are tasked to do more than ever and are becoming a fulcrum for reinvention. "The digital workplace merges work and life – a virtual space with applications, services and information on demand," says Forbes Insights. "For users, this means access to the technology they need, when they need it, on whichever device they prefer to use [2] "

IT management is the process of overseeing all matters related to information technology operations and resources within an IT organization. IT management ensures that all technology resources and associated employees are utilized properly and in a manner that provides value for the organization. Effective IT management enables an organization to optimize resources and staffing, improve business processes and communication and enforce best practices. Individuals working in IT management must also demonstrate abilities in such general management areas as leadership, strategic planning and resource allocation.

2.1 Enterprize Risk Management and Managing IT Risks

After identifying and evaluating possible risks, assesment contains 4 important segments of which management has to decide how to treat:

- Avoid,
- Mitigate,
- Share or
- Accept.

The methods of these treatments are called Enterprize Risk Management (ERM). By definition; (ERM) is a plan-based business strategy that aims to identify, assess, and prepare for any dangers, hazards, and other potentials for disaster—both physical and figurative—that may interfere with an organization's operations and objectives. [3]

The risk management in companies make assesment to plan for estimation of the impact of various disasters and evaluate the possible damages that the risks and disasters may materialize.

IT Risk Management is using the risk management tools on risks of information technology for managing and mitigation. While managements have to find a way for mitigation of these risks, they focus on the IT risks under following options:

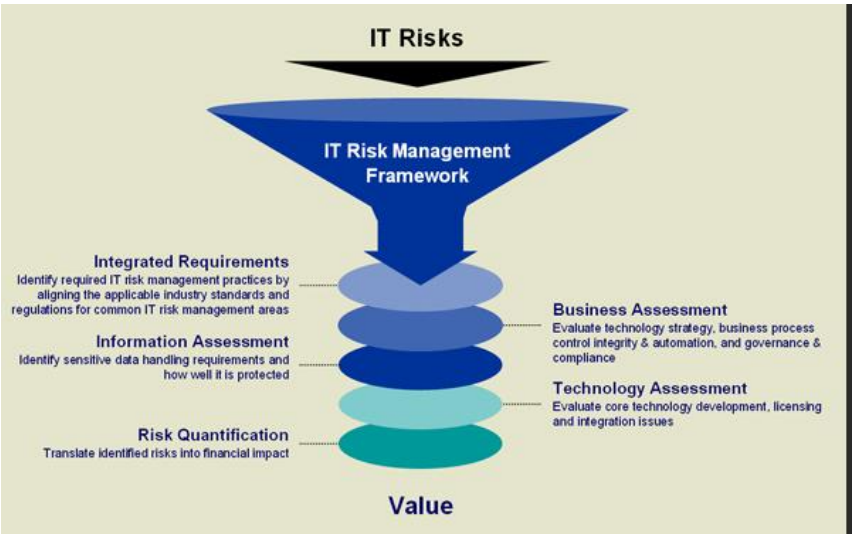
- **Risk mapping**: To asses the potential risks in order to continue the operations of IT system and decide on how to implement controls to reduce the possible risks to an acceptable level
- **Avoiding Risks**: To evaluate the risk and decide if the infrastructure is adequate to mitigate the risk at the time when it happens (e.g., stop working of the system when they observe a risky situation)
- **Limiting Risks**: Implementing some management or technical controls that will reduce or minimize the threat and its negative impacts. (e.g. periodic physical controls and technical checks)
- **Risk Planning**: To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Acceptance of Risk:** When they asses the risk as accepted risk, it means institution has chosen the option to live with the risk. It means; accurance probability is low and try to mitigate might be more costly than its damage if it happens. So they choose the option to live with it but carry on with controls.
- **Transferring the Risk**: This is the easiest way to to handle the risk. By taking some cost, risk can be transferred to third parties such as buying insurance policies or outsourcing the operation to a service supplier.

Illustration 1. Components of Risk Management

Source:https://yandex.com.tr/search/?clid=2186617&text=IT%20Risk%20management&lr=11508&redircnt=1588081598.1

If you magnify the Risk Management issues to be specialized for IT Risk Management issues, you come across with below points for managing IT risks

Illustration 2. IT Risks



Source :
https://yandex.com.tr/search/?clid=2186617&text=IT%20Risk%20management&lr=11508&redircnt=1588081598.1

All risks are mainly based on multi assesments of risks that business is facing at various levels during their operations. Everything must be linked to business assesments vs. technology.

These assesments mentioned at Illustration 1 & 2 can be categorized under following segments:

a. Business Assesment

Evaluate technology strategy, business process control, integrity & automation and governance and compliance.

b. Technology Assesment

Evaluate core technology development licencing and integration issues.

c. Integrated Requirements

Identifyrequired IT Risk Management practices by aligning the applicable industry standardsand regulations for common IT Risk Management areas.

d. Information Assessment

Identify sensitive data handling requirementsand how well it is protected.

e. Risk Quantification

Translate identified risks into financial impact.

In the past, information technology activites were fullfilled by a small department or a person who has some limited knowledge on hardwares and/or some information on the softwares. They had little impact on day-to-day operations.

2.1 The Difficulties of IT Management

IT has entered to our private and business life which exists in all parts of the day-to-day activities. These challanges are so much integrated to everthing we do. Due to its fast growing impacts, the risks in IT and its management has become very important in running a business.

Any IT infrastructure faces solution partners, vendors and suppliers that they must deal with. From each party management expectations canges and there is a lot of communication while during day-to-day process. The relationship among all these parties makes things more complicated as each of them have different motivation. It's a hard to manage job and totally should be handled by IT manager.

Another IT challenge is that any change at IT infrastructure may impact security and data management therefore careful steps have to be taken during the process. If there happens a failure, IT management accused for the burden of responsibility.

In this respect, IT management must design stress scenarios, evaluating impacts of any failures, analizing monitoring these risks before running or closing the process.

This approach can be handled by following questions:

- Can the exiting structure in hardware, integrated software, applications to this software and any integrated programs support the changes in technology?

- Any problem at the structure may create newer risks, unexpected errors or threatful incidences in IT which may impact every cycle of the technology set-up in the business. Is the system ready for them?
- In order to eliminate the undesired negative results, it has to be monitored closely which will provide management to mitigate the risks in IT. Are we ready for this?

The next step must be to recruit qualified staff and establishing strict rules for managing IT operations. The operation should run in compliance with standards established by local regulators and international practices. But this creates another dilema to comply with regulations, which usually are very frequently changing.

2.3. Steps of Running an Effective IT Risk Management

In order to perform effective IT risk management, application of general international rules and practices as well as applying risk management methods of IT to manage the inherent risks in that place. To achieve this: below steps should be taken for assessment of all business risks associated with using IT, ownership, operational activities and controls in IT. [4]

2.3.1. Identifying Risks (Risk Mapping)

Risk management in IT can not be performed without identifying possible risks in the environment. Therefore, all senior managers and whole staff must be aware of these risks and the rules related to these risks. Steps for identifying risk can be explained as follows:

2.3.2. Analyzing the Risks

When Risk Mapping is structured the management must decide the category of the risks as high, medium or low risk if they happen. Evaluation of the severity of the impact has to be deterimied. Each identified risk has to be evaluated sererately. All these evaluations and estimated impacts must be exist in the Risk Assesment document.

2.3.3. Risk Rating and Evaluation

Once the risks are assesed they must be prioritized. At this stage the management must develop monitoring and following strategies in order to control them. This is can be done by finding out how the risk can harm the IT structure. The following step is to determine the possibility of occurance and possible size of the damage. When all information is created, then management has to decide what to do with those risks. All these information must exist in the risk mapping document, too.

2.3.4. Risk Acceptance

If identified risks appear to be a significant issue for the future of the institution, then all the evaluations will be a target for the institution. Next steps will be the plans for action. This will be called risk management planning. In the plan, high risks will receive top priority by management for elimination or control them as much as possible. Other levels will also be evaluated how to treat them or reduce them. The whole process will be treated according to these evaluations. The whole structure must also be supported by preventive measures and contingency plan for business continuation.

2.3.5. Monitoring and Tracking the Risks

When the plans and relevant attachments are in place, Management has to monitor and review for the developments. This should be conducted by a seperate independent department and/or function who is not involved in day to day operations. This unit, who is called Risk Management department should be responsible to track what is going on in the organization in the perspective of managing risks. This function should not be confused with auditing, which is totally different from risk managent. Audit functions are after-the-fact function where risk management must be a live organism running parallel with day to day operations. Their responsibility is tracking and reviewing the progress on mitigating the risks in the organization. This will be an action to understand how the staff is dealing with the risks as well as ensuring if nothing is left over, forgotten or uncovered with preventive measures.

1.3.6. EGIT & COBIT 2019

In recent years in Turkey, especially in the financial sector all industries have been influenced by a wind called CobiT. Over the past few years, this wind has not been limited to the financial sector, but has started to appear in many different areas, from production to entertainment, from large holding companies to SMEs. So, it worths to investigate what is this CobiT?

Enterprise Governance of Information Technology (EGIT)

In order to understand CobiT well, firstly we must explore the term , "*Enterprise Governance of Information and Technology* **(EGIT)** against the changes happening at Information Technology digital transormation. This has become very important for the 3 common steps: a.support, b.sustainability and c.growth of the institution. Previously, governing boards (boards of directors) and senior management could delegate, ignore or avoid I&T-related decisions [5].

Due to this; digitalized enterprises have become increasingly dependent on I&T for survival and growth. In this respect, the concept of, governance of information and technology (EGIT) has arisen over the last three decades. EGIT is an integral part of corporate governance. It is managed by the board that oversees the whole institution [6].

Control Objectives for Information and Related Technology (CobiT)

This leads us to the definition, **CobiT** which is an abbreviation of "*Control Objectives for Information and Related Technology*". This definition is important in terms of expressing the purpose of CobiT. It sets out the goals to be achieved in Information Technology management.

The biggest feature that distinguishes CobiT from other similar standards such as ITIL, CMMI and ISO standards is that; it provides a framework which covers all IT structure in the establishment. To put it differently, if you evaluate all processes defined in CobiT, you are covering every area of IT management. Therefore, it is fair to say that, unlike other standards, CobiT focuses on managing IT not on IT processes. Generally, in most institutions, IT infrastructure is maintained by senior level decisions usually by Executive Committee who is leaded by Chief Executive Officer (CEO).

CobiT by nature defines almost all managerial components in the company in order to create and sustain an effective corporate governance modal. This covers: business processes, organization chart, business policies and procedures, corporate culture values, corporate image, data flows and storage, evaluation of skills and performance behaviours.

In order to understand the concept better, it must be analized what is Cobit and what is not by a comparison table as illustrated below :

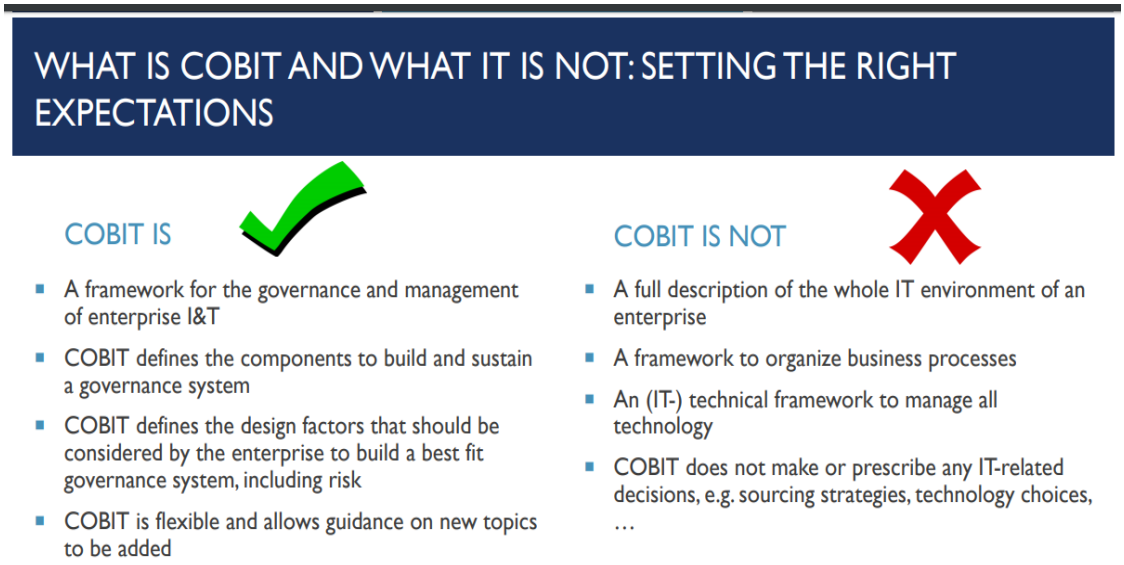


Illustration. 3

Source: ISACA RISK EVENT 2019: 19

1.4. IT Risk Management Strategies

IT risk management strategies are the pre-determined methods of IT Management for their data processing systems and operations in order to ensure that there will be no interruption and system is protected from all attacks, threats and abuses. It is a process where economic and operational costs are alsoconsideredduring all kinds of protective measures created for these purposes.

As a general rule, the determination of these strategies, the probability and impact of the risks and their consequences are evaluated. Accordingly, IT Managements try to assess the size of the threats, the damages they may cause and the possible results may create; constitute this strategy.

The following 3 criteria are focused in the strategy determination works:

1. Assesment (Risk Mapping): Risk is weighted by determining each risk according to its importance.
2. Mitigation of risks: Deciding on the measures for the identified risks.
3. Evaluation of possible results: At the end of the risk assessments, the efficiency of the taken measures (considering the cost) has to be evaluated. Based on the results obtained during ongoing reviews, new measures would be taken by reviewing the existing plans, and the issues that need change or improvement.

III. WHAT IS INFORMATION SECURITY?

3.1. Overview

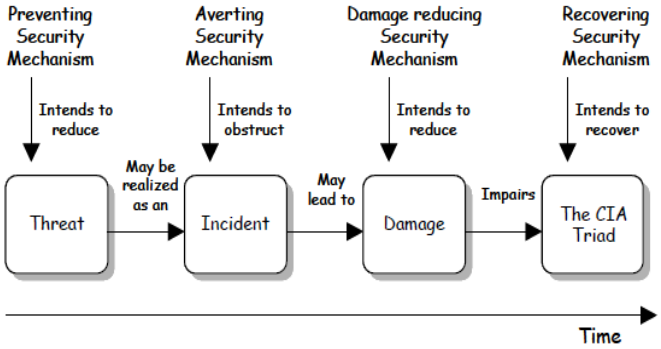
Information security or infosec is concerned with protecting information from unauthorized access. It's part of information risk management and involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspect, or recording [6].

As technology is placed itself to the heart of our lives by rapidly developing speed, any security related incident which occurs, requires more attention of information security managers who are assigned to reduce or eliminate the negative impacts to the organization. These measures will be in various forms like electronic controls or physical checks; by software programs or user checks.

The focus of any information security program is protecting the confidentiality, integrity and availability of information [7], which will be targeting for keeping up the organizational productivity. Therefore, information security should be considered as the protector of ongoing operations by preventing any malicious threats. This has leads us to apply policies, user rules, protection softwares like encryption, firewalls, antivirus programs and some standards for passwords, user limitations etc.

Every organization puts some standards to their operations consolidated in a Information Security Procedure which underlines all preventive guidelines for running a smooth and safe IT Operations.

Illustration 4. Phases of Information Security



Source: Oscarson, P. [8]

Information security can be achieved through a series of guidelines which should contain the acceptable rules for information security.

3.2. How to structure Information Security Program

Institutions who want to place efficient information security program should start with defining following:

1. Defining threats to İnformation Security System,
2. Placing Information Security Policies throughout in the organization,
3. Acceptable Usage Rules (Access Control),
4. Physical Security measures,
5. Software Limitations and Controls.

3.2.1. Threats to Information Security System

Running IT functions contain a lot of threats. An Information Security Program must first identify possible threats to IT Systems during the course of their daily operations.

Some of these threats can be listed as:

- Errors, wrong entries, missing records by employees
- Internal and external fraud attempts
- Hackers, viruses, worms
- Lack of protection against syber attacks
- Cheating efforts of staff and/or sabotage
- Malicious coding in programs
- System bugs
- Program Crashes
- Failure of duplicate records and back-up systems
- Lack of physical protection

3.2.2. Information Security Policies

All above threats must be covered under a policy book of the organization which provides information and debate on principles, strategies, application models, running techniques, usage rules & methodologies and applications of organizational management responsibilities in the company.

Cornerstone of effective information security architecture is a well written policy statement. This is the wellspring of all other directives, standards, procedures, guidelines, and other supporting documents. As with any foundation, it is important to establish a strong footing. As will be discussed, a policy performs two roles: one internal and one external. The internal portion tells employees what is expected of them and how their actions will be judged. The external portion tells the world how the enterprise is run, that there are policies that

support sound business practices, and that the organization understands that protection of assets is vital to the successful execution [9] of its mission.

3.2.3. Acceptable Usage Rules

In order to create a well established Information Security structure, the company must prepare a standard to be complied with by all staff. The objective of this standard should be targeting to ensure all employees and third party personnel and IT resources will understand and apply to fulfill their job responsibilities. This standard should cover for all and every resource who will be using any portion of the IT structure of the company. Following can be the guidelines for this purpose:

a. Access Control

- Users should be aware that allthe previliges assigned to the are given to them only for a need basis and by an authorization given to them to fulfill their duties.
- Unauthorized access to system files should be considered as misconduct and may be treated as diciplinary action.
- Personal computers and similar electronic media devices must not be connected to IT system.

b. Password Confidentiality

- Passwords must be kept confidential. Easy to remember but impossible to be guessed by a third person. Never to be used first name, family name spouse's, kid's, mother, father, other family members name, birthday, telephone, consecutive numbers etc which are very easy to guess
- Never lent to other collegue even to the supervisor. Must be kept strictly confidential.
- Passwords should be changed immediately if it is suspected that the password has been compromised.
- Passwords should be forced by the system to be changed periodically. This will increase the protection of the password to be comprimised by third parties.

c. Internet Access

- Access to the internet shall be allowed to only those users who are specifically authorized for this purpose. Authorization should be based on business needs and appropriate to the person's position level in the organization.
- Management must monitor the users internet traffic in order to identify any questionable visitto inappropriate web sites, gambling sites or other unacceptable places. During employement contract, management must reserve the right to terminate internet sessions that adverely. may effect operational performance of the company's information systems.
- Great care must be taken when downloading files, documents from external sources (some companies fully restrict this activity). If downloading is allowed, users should not download executable files (e.g.. exe, .dil, .com, .bet files) from internet.
- Employees and third party users must be held responsible for their unauthorized internet activities.
- There must be a policy for downloading, copying or pirating softwares and electronic files in order to protect from copyright prohibitions.
- Information obtained from internet sourcesshould be verified before being used for business purposes.
- Computer files received from unknown senders should be deleted without being opened.
- It is recommendable to restrict all public e-mail services (e.g. hotmail, yahoo, gmail etc) . If there is a need for it, there must be a formal exception process.
- Accessing to certain internet contents (e.g. terrorism, pornography, offensive data, political issues) should strictly be prohibited.

d. Social Networking

Social media content generally includes (but is not limited to) personal opinion, views and opinions, researches, personal announcements, commentory, memory sharing, event sharing, videos, pictures, commercial or non-commercial ads, business information.

Examples of these social media include facebook, twitter, youtube and linked-in. However, blogs, special interest forums, user communities are also considered social media. Considering that government bodies, ministers regulators, related government and civil organizations are heavily using some of these media avenues; below general rules at a minimum should apply:

- Any expression that may harm the companies reputation in public is prohibited,
- Except the authorized persons, no staff can comment on any thing on behalf of the company,
- Staff may not disclose any sensitive, private or confidential information about the company without obtaining approval from management,
- Staff should not upload, forward or post any links, unkown files or any other material which may harm the company or anyone in the company,

- Staff should not disclose, post or forward any confidential or sensitive content belonging to a third party.
- They must respect to intellectual rights,
- No arguments or conflicts which may give the impression that may be felt as it is the company's view.
- Respect to others privacy,
- Avoid publishing contact details of others. Also, be careful with publishing personal details as it will stay in internet environment forever.
- Never join to discussions or arguments about collegues, supervisors or sabordinates in social media,
- All employees should ensure ethical & moral responsibility and act accordingly as a representative of their company. They must remember that public will see him as the company.

e. E-mail Usage

- It is recommended to assign e-mail storage quotas for effective usage of computer disk space,
- Limitations can be assigned to e-mail attachments (like 2MB, 5MB, 10MB etc.),
- The recepients may be restricted to a certain number unless otherwised approved,
- All business related communications must be done by individual's official business e-mail address,
- The safety precautions must be taken if the mail is going out of the organization's network.

Inappropriate e-mail usage should include the following:

- Creating or distributing any disruptive or offensive messages and comments about religous beliefs, political beliefs, nationality, race, gender, disabilities, age, sexual contents or pornography. This restriction must be applicable for those people at inter-company network.
- Passing junk mails like jokes, chain letters, banners etc.,
- Sending or receiving e-mail attachments that are executable (e.g. exe, .dil; .bat)

f. PC Sharing

- All information and communication systems must be property of of the company. Therefore all received and transmitted data will be stored in the company which must be audited at periodic basis.
- Users must be discouraged sharing their personal PC. If there is a need for this, necessary arrangement must be done on the PC to use a departmental shared folder.
- Personal files, documents, mails, company statements etc can be stored in company PCs but should be kept in personal files clearly marked personal or private.

g. Security of IT Assets

- Usage of personal USB data storage and communication devices should be prohibited. Exepctions must be by a formal process,
- Access to system tools that have the capability to override the system and application controls must be forbidden for all users. IT staff given previlage must be assigned by management and preferably under dual controlled passwords,
- Installation of unlicensed products should not be allowed,
- Users must ensure proper shutdown when leaving their places,
- Employees with access to confidential information need strict procedures.

3.3. Security Measures at Data Center Area

A Data Center is basically a building or a dedicated space which hosts all critical systems or Information Technology infrastructure of an organization. The number of security attacks, including those affecting Data Centers are increasing day by day. Data Centers contain all the critical information of organizations; therefore, information security is a matter of concern. A Data Center must maintain high standards for assuring the confidentiality, integrity and availability of its hosted IT (Information Technology) [10].

The physical security of a IT environment is a series of guidelines that will stop any damages to information systems which stores the institution's vital and sensitive records. The identified measures must cover every item which can be classified natural catastrophic events to internal frauds or to terrorist violance.

3.3.1 ISO 27001 Directives on Data Center Physical Security

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature [11].

Security concerning IT and information is normally defined by three aspects, or goals; confidentiality, integrity and availability (see e.g. Gollman, 1999; Harris, 2002; Jonsson, 1995). The concepts can be seen as the *objectives* with security regarding IT and information and are often referred to as the 'CIA triad' [12].

The focus should be on following basics:

- User desktops
- Manager Laptops
- Servers
- LAN, WAN
- Server Room and AC System
- Routers
- Fire Extinguishers and Fire Detectors
- Generators, Emergency Light System, Back-up Batteries
- Software Licences

On the other hand, ISO 27001 directives recommend following physical security controls [13]:

- Secure Site selection by considering location factors like networking services, proximity to power grids, telecommunications infrastructure, transportation lines and emergency services, geological risks and climate, etc.
- Natural disaster risk-free locations or Disaster Recovery site
- Physical Access Control with anti-tailgating/anti-pass-back turnstile gate which permits only one person to pass through after authentication
- Single entry point into the facility
- Additional physical access restriction to private racks
- CCTV camera surveillance with video retention as per organization policy
- 24×7 on-site security guards, Network Operations Center (NOC) Services and technical team
- Regular maintenance of hardware in use
- Monitoring access control/activities
- Air conditioning and indirect cooling to control the temperature and humidity
- Monitoring of temperature and humidity
- Uninterruptible Power Supply (UPS)
- Smoke detectors to provide early warning of a fire at its incipient stage
- Fire protection systems, including fire extinguishers. Preferably the fire prevention shall be with zoned dry-pipe sprinkler
- Cabling Security including raised floor cabling, for security reasons.

3.3.2 Software Using Limitations and Controls

Security is always the first priority in IT Management. Therefore it's constantly improved by ensuring that up-to-date technologies are used and that security policies are enforced for both staff and end-users. IT Management should utilize industry standard encryption, attacks protection systems, security policies, and multi-factor authentication mechanisms to ensure security compliance [14].

In this respect software and communication limitations and controls are vital applications for the organizations. Following can be mentioned for a sound controlled environment:

- Apply end-to-end encryption during transport of data
- All messages to be encrypted
- Establish protection for trial-and-error attacks for guessing account passwords
- Use code signing certificate to guarantee that binaries are not altered or compromised by a third party
- Establishdatacenter and Network security which is compliant to ISO Certification and COBIT directives
- Maintain logs of device access control lists and have them controlled
- Establish two-factor authentication (maker-checker function) as an additional security layer
- Make security testings by penetration tests on regular basis
- Establish auditing rules and apply them periodically
- Any modification, deletion, addition to data programs must be documented in detail under multiple controls
- No one ever should have single acces power to the program garden of the company software and applications. If there is a necessity due to lack of competent staff, all activities must be documented for audit trail.

3.3.3. How to Prevent Data Breaches

Data breaches are the events when there is a leakage from outside to the sensitive information that are under protection measures of information security. This incident ends up with stolen, viewed, manupilated or changed critical records of the company by unauthorized people.

Cyber attacks, social engineering and phishing, ransomware and other types of malware, physical theft of hard drives, slow vulnerability assessment and patching cadence, bad information security policies, poor security

awareness training and a lack of general cyber security measures can all result in data loss and data breaches [15].

The aim of cyber criminals target mainly to below sensitive information:

- Credit card detais of the client,
- Personal information of staff and clients such as tax number, social security number, telephone numbers, addresses to be used in internet world,
- Private information like social media addresses, national ID, information of family members, friends, private photos, documents available in the social media place,
- Some general information which is confidential for the company,
- Any sensitive information which may be importantant and may harm the company if learned by competitors like vendors, service suppliers and general business activities.

Therefore, even if the company is an SME or a big multinational company, they implement common data breach prevention tools in order to eliminate the risks of these type security threats.

How to Protect Sensitive Data?

Sensitive data is any critical data which needs to be prevented from unauthorized third party access in the IT infrastructure. IT Management has to establish adequate data security to prevent data breaches and unapproved information disclosures.

The organization may has to protect sensitive data for ethical or legal requirements, personal privacy, regulatory reasons, trade secrets and other critical business information. Such data could pose increased social, reputational, legal, employability or insurance risk for you and/or your customers if exposed and is often the target of corporate spying [16].

Sensitive information includes all data, whether original or copied, which contains:

- Personal information.
- Protected Health Information (PHI)
- Education records
- Customer information
- Card holder data
- Confidential personnel information
- Personal data

In general, below listed information can be considered sensitive data, too:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation
- Financial information (bank account numbers and credit card numbers)
- Classified information [17]

IV. DISASTER RECOVERY (DRP) AND BUSINESS CONTINUITY PROGRAM (BCP)

A disaster recovery plan (DRP) is a documented process or set of procedures to execute an organization's disaster recovery processes and recover and protect a business IT infrastructure in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster". Nowadays, organizations use technology to achieve fast, reliable and proper processing. This created effective means of production. On the other side e-mail has become an inevitable tool for performing the business needs effectively. Together with electronic data processing, staff also uses the facilities of Voice Over Internet Protocol (VOIP) telefon communication, tele conferences and video conferences. Skype, zoom, microsoft teams type online meetings, on-line trainings, webinars and all other tools of technology which brings businesses to high level technology. To maintain the quality of high-tech environment, companies are making huge investments to technologic devices and allocating expensive budgets for keeping the advanced good quality. The devices connected to system are providing fast processing operations and this infrastructure is capable of huge volumes of record storage; by use of desktop PCs, laptop and tablets and wireless communication articles and so on. What happens if technology can not work or stop due to an unexpected reason?

Company must establish a technology disaster recovery plan (IT DRP) together with a business continuity plan. The impact of events which are stopping working of technology must be assessed during risk mapping analysis. IT issues should receive priority in risk assesment plans. The aim of this plan must be

focusing on to restore non-working hardware-if not possible switch to back-ups, make applications work either prime systems or secondary systems and recover the data timely to start the activity back.
Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential [18].

4.1 IT Recovery Strategies

Recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource [19].
"Information systems are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful data, typically in organizational settings [20]"
If any of them has a problem or doesn't work, the system may not work properly. Therefore, the company must establish recovery policies which must bring the system operation back to the point where it was interrupted.
This procedure must cover following points:

- The area where computer room is located (the procedures must be taking care of temprature and climate controls in the room, measures of back-up energy supplies, emergency lights, access controls to the server room, cleaning the area from unrelated stuff in the room),
- Hardware main boxes and connected devices,
- Connections to outside providers (like data lines, fiber connections, cable connections, wireless set-ups, encryption-decription devices etc.),
- All software storage and protection rules (electronic data interchange, electronic mail, enterprise resource management, source codes, etc.),
- Fire extinguishers and thier availabity in the area,
- Disaster Recovery Manual and restoring data base.

Some industries like banks and financial institutions cannot tolerate any downtime in their systems for any reason. For this purpose they set-up a second data center for backing up all their processing needs in case of a failure at their primary systems. The structure of the secondary system (back-up) which can have the capacity of parallel running as well as having easy to shift in case of something happens to primary system.
The Disaster Recovery and Business Continuity Plan of the companies create scanarios for these events mainly for: technical downtime, war, earthquake, fire, riots Pandemic Situations, civil actions or other kinds of disasters that may stop to run the operations at the place of primary system. They usually set up this location outside of the city of headquarters.

4.2. Developing an IT Disaster Recovery Plan (DRP)

Every organization needs a Disaster Recovery Plan for their IT structure. The plan must be addressing all needs for hardware (servers, computers, connecting devices, modems and duplicate data). The plan should also have a strategy guidelines definition to make sure that all necessary data (prime records) are properly backed up and restored whenever there is a crisis after a failure in the IT systems.
Definition of Crisis Events which will be subject to Disaster Recovery
"Crisis event" means the state of problems like following:
(1) Long-term system failures due to natural disasters, contingencies in public utilities (power, telecommunications, etc.), and other accidents.
(2) System normal failures longer than a specified time: Interruption of business due to system defects and system operations problems which doesn't last until a specified time.
(3) Occurrence of serious information security incidents due to cyber-attacks or internal misconduct that requires an urgent action for the possibility of such incident may have increasing damage impact.
(4) "Cyber-attack": Improper acts which has intention to damage to secrecy, completeness and availability of the information system by abusing IT/communications technology infrastructure such as improper access to the Company's information assets and/or transmitting computer viruses/sucking a high volume of data, etc., by an outside party.
(5) Internal Misconduct: Improper acts by Company insiders that damage the secrecy, completeness, and availability of information systems, similar to cyber-attacks. This include sabotage activities, too.
(6) Miscellaneous Incidents: Sometimes, there are events which are assumed that these multiple incidents can occur in broad areas, therefore, called as "Threat" to IT Systems

What to do in order to create a disaster recovery plan;

Select the critical venues in the IT Structure

- Software used for company operations
- Data Storage and producing back up data.
- Avaibility of a copy of the software ready for re-installation
- Place of Source Codes
- Staff arrangement in the company or outsource agreements for emergency conditions
- Reserve hardware devices which can be used in case there is a need to replicate and reimage the operation
- Manuals and instructions for use of back-up staff for hardware and software restoration.

IT disaster recovery plan must be an integral part of company's Disaster Recovery Plan as well as a part of the business continuity plan. Company's internal auditors must control periodically to ensure that planned measures are working.

4.3. Business Continuity Plan (BCP)

Contingency Planning in general is the process of identifying risks from disruption of operations and services, developing plans to enable systems and functions to be resumed in the predetermined shortest possible time and exercise those plans to familiarize the recovery staff with their content. The goal of the BCP is to secure the employees life safety and to minimize financial losses to the institution, serve customers and financial markets with minimal disruptions, and mitigate the negative effects of disruptions on business operations.

The BCP should provide specific and detailed information regarding the responsibilities of all staff and departments during a disaster, and the overall business continuity recovery process that apply to all divisions and departments as outlined in the plan. The BCP plans are created based on a short and long term crisis scenario for a predetermined period.

Information technology (IT) contain many hardware and software instruments such as network system, hardware servers, desktop and laptop computers, tablets, connection materials, printing equipment and wireless devices. Business continuity of all of those devices are very important for the sustainability of the institution.

Therefore, the company must establish a strategy to recover any system failure so the IT activities can be restored quickly with no significant losses.

Development BCP should contain following steps:

- Business conducts an **impact analysis** to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement **to recover critical business functions** and processes.
- Organize a **business continuity team** and compile a business continuity plan to manage a business disruption.
- Conduct **training for the business continuity team** and testing and exercises to evaluate recovery strategies and the plan.

Illustration 4. Business Continuity Plan

Source: Ready USA, National public service campaign, https://www.ready.gov/business-continuity-plan 30.04.2020

Template for Data Recovery Plan and Business Continuity

1. **Basic Policy**	**The data needed in order to continue the priority operations should be stored. Backup copies of necessary programs and procedure documents should be available in addition to business-related data whenever an IT disaster happens.**
2. **Location of Backup Data**	**Backup data and programs are to be kept at a location that has a small risk of being affected by the same disaster that hits the main site. (A place adequately away from the main site) This locantion must be at a place where you can easily reach.**
3. **Preparation of a Method to Recover Data**	**A system (IT solution, etc.) to allow the use of necessary backup data quickly to restart the priority operations is to be put in place. If this needs some new set-ups company may go into a contract agreement with a provider**
4. **Appropriate Frequency of Checking Data Backup**	**There must be a program which ensures and verifies if backup data are taken frequently enough (daily, weekly, monthly….etc.) and adequately to allow restarting operations in case of emergency.**
5. **Appropriateness of Backup Data Transmission time**	**If backup data needs to be transmitted/transported to the DR site or to a place where restoration process is needed at the time of a disaster:check if the method of transmission is workable under disaster scenarios.**
6. **Duplication of Important documents**	**Important documents should be duplicated (copies should be kept) as well, if needed for business continuity. This has to be audited by auditors.**

Physical Conditions of DR Backup Site (Data Recovery Site)

7. **Backup Site**	**Backup site should be facilitated to resume emergency business operation, and must have capacity to continue predetermined critical operations (i.e. clearing and settlement, all operations for customer and command center function if available), and equipped with required IT infrastructure and other resources required to continue predetermined functions and critical processes as planned in the BCP**
8. **When Selecting Location of Backup Site**	**Following points are to be considered when selecting location of backup site:** **(1) Has little possibility to be suffering from the same incident (keep reasonable distance from the main office)** **(2) However, backup site must be located at a place where emergency staff can travel within the time predetermined in the BCP (this plan must consider all aspects in terms of distance, method of transportation and fast arrival as well)** **(3) Has to accommodate unit specific risks. Another alternative to switch must be available for unexpected restrictions. For instance for units located at an area where all of a sudden a high risk for infectious disease, pandemi situation coup etc happens and access to the backup site may not be possible if the backup site is located at an area at the restriction zone.** **These measures must be considered for the units located at an area which is prone to risks such as earthquake, flood, terrorism, riots, coups d'etat etc., and all types of disasters arising from government and military facilities, broadcasting station, foreign offices and such.**

9. **Additional Points to be Considered**	**If the selected backup site location is not a property of the company, an agreement on the following points shall be predetermined:** **(1) Conditions of agreement/contract – All restrictive clauses** **(2) Cost and period of agreement/contract** **(3) Size of the space, allocated configuration** **(4) Power supply and utilities** **(5) Communication lines** **(6) Maintenance clauses** **(7) Definitions for support conditions and penalties** **The back-up location may also be used as a management headquarters where the company senior management can take control and also perform operations other than those functions of backup site (i.e. decision making, status monitoring, command and control etc.) . For this purpose, setting up an office environment with minimum facilities is highly recommended**
10. **Data Backup**	**It must be similar to details explained in Disaster Recovery Plan**
11. **Items to be kept at the DR site**	**Besides backup data (business data), an ID to use the backup system and the system's manual should be kept. Keeping sufficient stationary should not be forgotten**
12. **Facility Standards**	**The site must satisfy certain facility standards required to continue predetermined critical business.**
13. **Power Supply**	**The site must have the equipment to provide enough power (without depending on the public facilities)in order to continue predetermined critical business.**
14. **Loading the program and restoration of Lost Data**	**The following points are important when you try to reflect lost data in the backup system at the DR site.**
14.1 Types of Lost Data	**There are two types of lost data as described below. A business continuity scenario involving lost data should be created for each of the critical operations.** **1. Data to be restored in the backup system: the data which will be entered to the backup system for updating the data base from the last restoration to the time of the disaster when it hit the main system.** **2. Data of manual transactions while system operation is suspended: the data of manual transactions that took place after the main system was hit by a disaster. These transactions are the ones which could not be stored in the main system or to the backup system.**
14.2 Identification of Lost Data	**The data of manual transactions that took place while a system is down can be identified easily, using related documents. However, as for the data yet to be reflected in the backup system, it is important to find out where the evidence of transactions can be obtained (in the company, or outside of the company, etc.) beforehand so that such transactions can be identified quickly. If it is difficult to identify such transactions, the company may need to make a public announcement about the extent of damage done by the disaster, and have customers submit applications to re-do the transactions.**

	Establishing a procedure is necessary to be followed in such cases.
14.3 Reflection of Lost Data and Resumption of Operations	**There are following two options depending on the timing of reflecting lost data and restarting customer transactions. Procedures to restart transactions and how to handle customer inquiries, etc. need to be considered in advance.** **Priority is : restarting customer transactions after reflecting all missed data (target is integrity of transaction data)**

5. LIST OF POINTS TO BE COVERED AT AN INFORMATION SECURITY PROGRAM (Common Examples)

IT Management guidelines, Disaster Recovery Plan and Business Continuity Plans has evolved into the enterprise wide IT management structures mainly with strict information security rules.

These documents should contain following guidelines at least but not last [21]

- Firewall control
- Risk analysis
- Business Impact Analysis (BIA)
- Virus control and virus response team
- Computer Emergency Response Team (CERT)
- Computer crime investigation
- Records management
- Encryption
- E-mail, voice-mail, Internet, video-mail policy
- Enterprisewide information protection program
- Industrial espionage controls
- Contract personnel nondisclosure agreements
- Legal issues
- Internet monitoring
- Disaster planning
- Business continuity planning
- Digital signature
- Secure single sign-on
- Information classification
- Local area networks
- Modem control
- Remote Access

VI. CONCLUSION

Information technology, which covers: ongoing software developments together with hardware structure that is designed at the most adequate capacity; as well as an integrated system that requires constant maintenance and structured at the highest security level. On the other hand; the use of this structure, related processes and operating methods is also concerned other issues to be focused on.

All those critical important issues in these systems, where all of the vital information of the institution is stored, are; establishing standards for processing and storing data, easy access to the database, friendly setup to transfer them to users and the sufficient details of data which can be analyzed and reviewed by related stakeholders.

In this case, we can define Technology as a series of technical infrastructure and operating processes that have been built through computers and supplementary attachments in the network to achieve a goal. Thus, when we talk about the concept of IT, we can say, it is everything and anything about computer systems operations.

Information security is a chain of measures that protect all data and sensitive information processed at the institution, in order to ensure accurately recorded transactions, no manipulation, stopping any deletion, corruption or alterations by unauthorized or malicious persons.

We can say that, security measures include prevention from all innocent mistakes and any kind of malicious fraud and abuse. For example, protection of accounting, prevention from ID thefts, alteration or deletion of data and safe internet environment.

If security measures are not taken against such incidents; workflows may be interrupted and company's reputation may be damaged, too. In the same time, there might be consequences that ends with loss to the company. Therefore, institutions allocate significant resources for information security. For this purpose, universal security measures has been achieved over the time for establishing a sound IT Risk Management for the company. Thanks to all of the parties who have introduced the information security standards which are applied all over the World.

REFERENCES

[1]. Ocarson P, Information Security Fundementals, *Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden,* IFIP World Conference on Information Security Education (2012) p.4

[2]. IBM. (2020). *What is IT Management.* https://www.ibm.com/topics/it-management para.1 (26.04.2020)

[3]. Investopedia Article. (2020). *Enterprize Risk Management (ERM).* https://www.investopedia.com/terms/e/enterprise-risk-management.asp (25.04.2020)

[4]. Bridges, J. (2019). *Project Management 2019*.para.7 https://www.projectmanager.com/training/it-risk-management-strategies

[5]. Lanter, D. (2019). *Cobit 2019 Framework, 2018 ISACA Document*.p.11 para.1,3

[6]. Tunggal, A. T. (2020). *Information Security Article in Upguard.* Para.1 https://www.upguard.com/blog/information-security (15.03.2020)

[7]. Tunngal, A. T. (2020). *Upguard.* Para.2 https://www.upguard.com/blog/prevent-data-breaches (29.04.2020)

[8]. Ocarson, P. Information Security Fundementals, *Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden,* IFIP World Conference on Information Security Education (2012) p.9

[9]. Peltier, T R., J. Peltier, J. Blarkley. (2005). *Information Security Fundamentals.* Auerbach Publication p.72

[10]. Yadav, N. (2020). *The Most Common Physical and Network Controls When Implementing ISO 27001 in a Data Center.* Para. 1 https://advisera.com/27001academy/blog/2019/02/26/the-most-common-physical-and-network-controls-when-implementing-iso-27001-in-a-data-center/ (28.02.2020)

[11]. Humpreys, E. (2020). *ISO/IEC 27001: 2013 ISMS Standard.* https://www.pdfdrive.com/implementing-the-isoiec-270012013-isms-standard-e58196796.html (20.11.2019)

[12]. Ocarson P, Information Security Fundementals, *Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden,* IFIP World Conference on Information Security Education (2012) p.4

[13]. Yadav, N. (2020). *The Most Common Physical and Network Controls When Implementing ISO 27001 in a Data Center.* https://advisera.com/27001academy/blog/2019/02/26/the-most-common-physical-and-network-controls-when-implementing-iso-27001-in-a-data-center/ (15.03.2020)

[14]. Pulsway. (2020). *IT Management Security.* https://www.pulseway.com/it-management-software (29.04.2020)

[15]. Tunngal, A. T. (2020). *Upguard.* https://www.upguard.com/blog/prevent-data-breaches (29.04.2020)

[16]. Upguard. (2020). *Sensitive Data.* https://www.upguard.com/blog/sensitive-data (30.04.2020)

[17]. Upguard. (2020). *Sensitive Data.* https://www.upguard.com/blog/sensitive-data (30.04.2020)

[18]. Ready (Official website of the Department of Homeland Security). (2020). *IT Disaster Recovery Plan.* https://www.ready.gov/business/implementation/IT (30.04.2020)

[19]. Ready USA. (2020). *National Public Service Campaign*. https://www.ready.gov/business-continuity-plan (30.04.2020)

[20]. Bourgeois, D. & D. T. Bourgeois. (2020). *Information Systems for Business and Beyond.* Press Books, Chapter 1, https://bus206.pressbooks.com/chapter/chapter-1/ (03.05.2020)

[21]. Peltier, T R., J. Peltier, J. Blarkley. (2005). *Information Security Fundamentals.* Auerbach Publication p.30

Corresponding author: Asst. Prof. Dr. Bulent Gunceler
İstanbul Okan University, Turkey Faculty of Business and Administrative Sciences
Orcid Nr. 0000-0002-3332-0751