Cesare Gallotti

with the contribution of
Massimo Cottafavi and Stefano Ramacciotti

INFORMATION SECURITY

RISK ASSESSMENT
MANAGEMENT SYSTEMS
THE ISO/IEC 27001 STANDARD

January 2019

Dedicated to, in order of appearance:
Roberto and Mariangela Gallotti;
Clara;
Chiara and Giulia;
Paola Aurora, Alessio and Riccardo;
Juan Andrés and Yeferson, came from afar
directly in our hearts.

Contents

Introduction and acknowledgements

> *My twenty-five readers may imagine what impression such an encounter as has been related above would make on the mind of this pitiable being.*
>
> Alessandro Manzoni, *The Betrothed*

The first version of this book was in Italian and dated 2002. I've since had the pleasure of meeting more than 25 people who had read and enjoyed it. Unfortunately, they'd often borrowed it from a library, and sales were low.

In 2014 I wrote a second edition, in Italian, with all the ideas developed during the training courses, presentations, discussions with colleagues and friends, and meetings for the writing of ISO/IEC 27001:2013. In some cases, beliefs from 2002 had changed, thanks to numerous audit and consulting projects.

The third version was a minor update, with few new examples and ideas emerged during the process of writing ISO/IEC 27003:2017.

This fourth version is the first one in Italian and English. I've updated some example and corrected some text.

The first part explains the basics of information security and information security management systems.

The second part describes risk assessment with broad theoretical ideas balanced by many examples; the calculations are not needed to fully understand the concepts.

The third part describes the security threats and controls, based on ISO/IEC 27002.

The fourth part discusses the requirements of ISO/IEC 27001:2013 according to my interpretation of the meetings I attended to write the standard, training courses, and discussions with clients.

The first three appendices contain some brief presentations made during some training courses.

The Common Criteria and FIPS 140 Appendix is by Stefano Ramacciotti.

Subsequent appendices are taken from some of my checklists.

This text relies heavily on ISO/IEC 27001 but is not an official guide for the latter's interpretation: for that, see ISO/IEC 27003:2017.

This book was written for those who want to learn about and deepen their knowledge of information security. To help with that, I've tried to answer all the questions I have been asked over the years.

I also believe that some ideas may be of interest to those who already know the material and could be the starting point for new discussions. Each has their own views, some different from mine, and we can only benefit from comparing and contrasting them.

This book does not cite the standards for copyright reasons, and because, in some cases, I wanted to make the text more meaningful.

Definitions are taken mainly from the 2018 edition of international standard ISO/IEC 27000. Some definitions have been slightly modified to make them, in my opinion, more understandable. Any additions are placed in brackets. Deleted segments are indicated by ellipses.

I would like to thank the following people for helping me write this book, in alphabetical order:

- Max Cottafavi: a governance, risk and compliance expert with whom I have talked for many years and who read the drafts and gave me helpful ideas and a bit of text to copy;
- Roberto Gallotti: my inflexible proof-reader and idea man; although he may not claim to be an expert in information security, he is a professional from which I would like to learn more;
- Stefano Ramacciotti, with whom I discussed information security around the world during some meetings of the SC 27 and who also helped for parts of text (in particular, the Common Criteria Appendix, the Fort Knox example, and the third and fourth PS).

These people are among the most competent and friendly professionals I know, and I am very proud that they dedicated some of their time and energy to me.

I also would like to thank Franco Ruggieri, Pierfrancesco Maistrello and Francesca Lazzaroni with whom I have had the opportunity to discuss many things over the years and provided valuable feedback.

Finally, I would like to thank all of the clients, colleagues, competitors, participants, etc. with whom I was confronted in recent years and who were not afraid to share ideas and mutual incompetence even through my blog.cesaregallotti.it and my monthly newsletter. We are all competent but also acknowledge that our field is extremely changeable, and there's nobody better at it than others.

Contacts

To contact me, report mistakes, or suggest improvements, please check www.cesaregallotti.it.

I invite all who are interested in subscribing to my (Italian) newsletter to follow the instructions on my website. I'm also (in English) on LinkedIn and Twitter.

Warning

The web links in this book were verified on August 8, 2018.

Chapter 1

Introduction

> *What [...] there was to be interpreted in "Play nice"?*
>
> John Niven, *The second coming*

Mankind has always felt the need to secure information. We want our personal information, such as health reports or bank balances, to be accessible to no one other than a few trusted people. We want it to be accurate and correct. We don't want it to be improperly used, e.g. to call us at home for marketing purposes or slander us on social networks. We want it to be available quickly, especially on the Internet.

Organizations (e.g. companies or institutions) desire the same security. For example, they want to keep innovative projects and customers' details secret, they want accurate economic data, product design and performance, availability of computer systems.

The first part of this book defines and explains the basics of information security.

The term *security*, however, is in itself a contradiction. It brings to mind something absolute and incontrovertible, which is impossible in reality.

It is often said that Fort Knox, which safeguards the monetary reserves of the United States, is one of the most secure places in the world, with top-of-the-line sensors, perimeter defenses, and alarms. It is also home to numerous military units standing by for any problem, and the name itself is now an idiom for an infallibly secure location. But, what would the response be should a meteorite with a 1km+ diameter fall on it?

As you can see from this simple example, security is never absolute. Fort Knox is not resistant to a large meteorite. For this reason, never trust anyone offering products or solutions that guarantee 100% security.

Risk assessment helps us establish *appropriate* levels of security that can then be achieved through corresponding *treatment* actions. If the desired level cannot be reached, we can then analyze the deficiencies and, if necessary, accept them.

Over time, the assessment should be repeated to see if the desired and actual security levels are still valid. These activities (risk assessment, action or acceptance, and repetition) constitute *risk management* and are better explained in the second part of the book.

The third part of this book lists *information security controls* that help ensure the security of the information. They are mainly organizational, not technical. In fact, good processes lead to choosing good and appropriate technologies and to managing them properly. The opposite is not true: good technology does not lead to good processes.

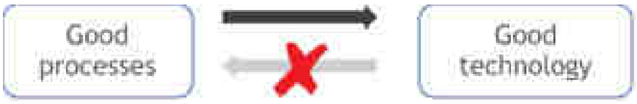


Figure 1.0.1: Processes and products

The fourth part of this book deals with the requirements of ISO/IEC 27001 for information security management systems.

A bit of history

Information security has been an issue since the dawn of humanity. Just think of the *mysteries* connected to different religions. Caesar even discussed methods to safeguard messages in war (in Chapter 48 of book V of the *De bello Gallico*). The use of double entry to ensure the integrity of accounting, described in 1494 by Luca Pacioli, is undoubtedly older than the 15th century.

In organizations, until the diffusion of information technology, information security referred to paper documents and oral communications: today it also includes IT security.

Before the 1990s, technicians ran IT security without any connection to *corporate security*, although the risk of information theft and espionage was nevertheless taken into account.

In those years important events helped develop the economic and social context of IT:

1. the spread of information technology, thanks to personal computers and increasingly intuitive interfaces: Microsoft Windows (1985) and Mosaic, the first graphical browser for surfing the web (1993);

2. the increase in people and connecting devices over the Internet (itself not designed for security [120]);

3. the increase of threats known to the general public: the first virus, Morris worm (1988);

4. the publication of regulations with respect to IT security: in Italy the first laws related to IT security date back to 1993;

5. increasing social unrest due to renovations of many companies;

6. the use of more and more suppliers and increasing relations with external actors as represented in Figure 1.0.2.

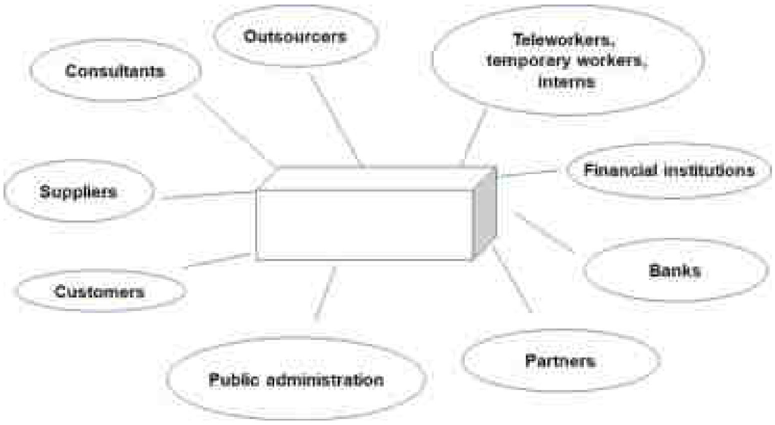


Figure 1.0.2: Open Enterprise

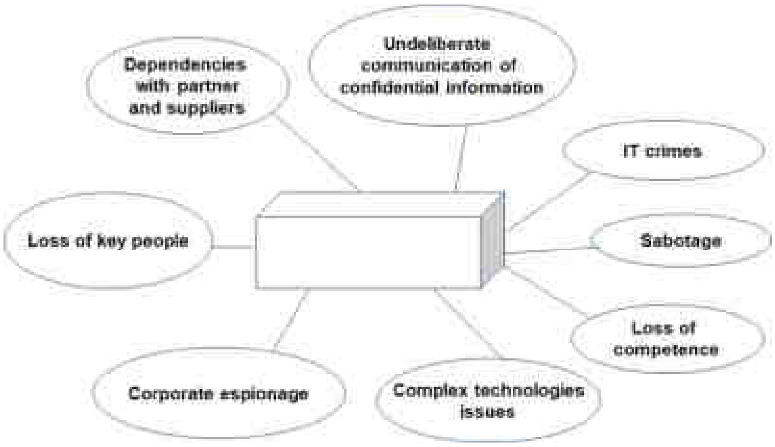

Dependencies with partner and suppliers
Undeliberate communication of confidential information
IT crimes
Loss of key people
Sabotage
Loss of competence
Corporate espionage
Complex technologies issues

Figure 1.0.3: New threats

All these events increased awareness of information and computer security, as shown in Figure 1.0.3.

In the 1990s, the approach to security also changed due a need for specialization (e.g. in IT, physical sites, personnel) and for priorities and budgets based on risk assessments.

Over the years, security requirements have increased due to more recent events (September 11, industrial espionage, etc.), new regulations on information security, and the ever-growing globalization of companies.

Methodologies and practices for information security were introduced to help companies. Among the most important initiatives are those related to IT products and systems security (TCSEC of 1983, ITSEC of 1991, Common Criteria of 1994 and the NIST Special Publications[1] issued since the early 1990s), information security (BS 7799 of 1995, whom history will be the subject of section

[1] http://csrc.nist.gov

13.4) and information security risk assessment methodologies (CRAMM of 1987, Marion of 1990 and Mehari of 1995) [23].

Part I

The basics

Chapter 2

Information security and organization

Where is the life we have lost in living?
Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information?

Thomas Stearns Eliot, *The rock*

This chapter provides a basic definition of *information security*. The next chapter specifies what an *information security management system* is.

The following activity may be useful: list the news or events related to information security which you have been witness to or victims of. For example:

- in 48 B.C.E., the library of Alexandria was burnt down and destroyed[1];
- in 1998, the Italian Finance Ministry sent millions of tax assessments to the wrong taxpayers[2];
- in 2003, due to a tree falling on high-voltage transmission lines in Switzerland, Italy experienced an energy shortage that in some areas lasted more than 24 hours[3];
- in February 2006, the computer systems of the city of Milan were unusable for a week because of a virus[4];
- in 2007, some drawings of the Ferrari F2007 fell into the hands of its competitor McLaren[5];
- in 2010, the head of counter-terrorism at Scotland Yard had to resign after being photographed in plain sight with a document classified "secret" under his arm[6];

[1] https://en.wikipedia.org/wiki/Library_of_Alexandria.

[2] www.contribuenti.it/cartellepazze/cartellepazze1.asp.

[3] http://edition.cnn.com/2003/WORLD/europe/09/28/italy.blackout/index.html.

[4] attivissimo.blogspot.it/2006/02/milano-ancora-ko-da-ks.html.

[5] news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm.

[6] https://www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak.

- in April 2011, some of Aruba's (Italian hosting company) computer services were unavailable due to a fire in the UPS system[7];
- in October 2011, the Blackberry network was unavailable for 3 days due to an incorrect system update[8];
- in 2011, the PSN Sony computer service was attacked by criminals who stole user data, including passwords; Sony stopped the service for months[9];
- in September 2013, the Alpitour (Italian tour operator) network was breached, and some links were made to redirect to malicious websites[10];
- at the beginning of 2013, Spamhaus' anti-spam services were blocked by an attack[11].

These examples illustrate how information security could deal with many potential threats: fire, natural disasters, equipment failures, human error, malicious attacks, etc.

2.1 Data and information

Before discussing data and information, we'll provide the definition present in previous versions of ISO/IEC 27000. In the latest versions, this definition is no longer reported because you can find them in ordinary dictionaries[96].

> *Information data*: knowledge or collection of data that has value to an individual or an organization.

Information is stored and transmitted on *supports*. They may be *analog* or *non-digital*, like paper, photos or movies on film, or *digital*, like computers and removable memories (e.g. USB sticks, CDs and DVDs). A special case of non-digital media is the human being, which uses its brain to retain information. Information can be transmitted via postal mail, telephone (which is now based on mixed technology), computer networks, and, since we always have to keep humans in mind, conversations between people.

Information security is not limited to *computer* or *ICT security*, i.e. related only to information in digital form and processed by information and communication technology (ICT) systems, but encompasses all systems used to collect, modify, store, transmit and destroy information.

This is one reason why we prefer to talk about "information" rather than "data: the term intuitively has a more generic value.

More rigorously, information security includes data security, as evidenced by the four types of knowledge representation [70, 85]:

- *data*: this indicates the set of individual facts, figures, sensory impressions, etc.;

[7] www.datacenterdynamics.com/content-tracks/power-cooling/ups-fire-brings-down-aruba-data-center/33362.fullarticle.

[8] www.bbc.co.uk/news/technology-15287072.

[9] attrition.org/security/rant/sony_aka_sownage.html.

[10] www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate.

[11] www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.

- *information*: organized and meaningful data;
- *knowledge*: information received and understood by a single individual;
- *wisdom*: the ability to make connections between pieces of knowledge to enhance decision making.

2.2 Information security

ISO/IEC 27000 provides the following definition.

> *Information security*: preservation of the confidentiality, integrity, and availability of information.

It is therefore necessary to define the three aforementioned properties (additions not in ISO/IEC 27000 are in brackets).

> *Confidentiality*: property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
>
> *Integrity*: property of accuracy and completeness;
>
> *Availability*: property of being accessible and usable [according to agreed timeframes] upon demand by an authorized entity.

These are often referred to as *CIA parameters*.

We use the terms *computer*, *digital*, *IT*, or *ICT security* when information security is limited to information stored on or transmitted between computer systems. Some ICT systems (for example, industrial ones) may not be considered relevant to information security because they don't handle relevant information.

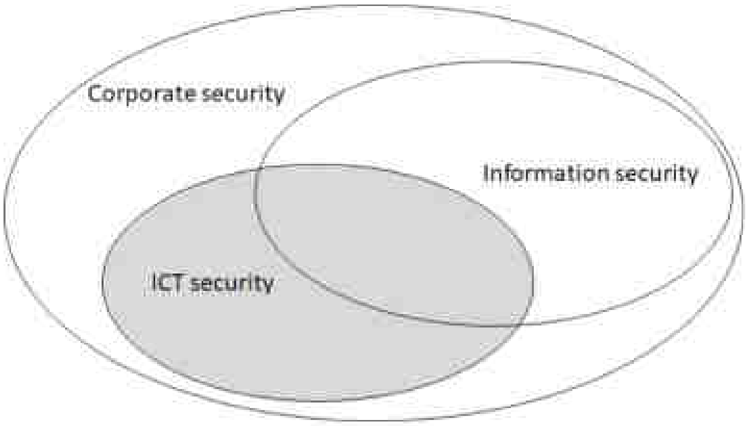


Figure 2.2.1: Information security and ICT security

Example 2.2.1. In 2016 Finland apartments were left without hot water for a week because the heating system had been subject to ICT attack[12].

This is not exactly an attack with impact on information, but it's definitely an ICT incident.

In this book we don't use the term *cybersecurity* because this is identical to ICT security, only with a more impressive name. It is taken from the term *cyberspace*, invented by William Gibson in 1986 as part of cyberpunk literature, perhaps because the term "Internet"was not widespread enough. Gibson himself has admitted to having used the Greek word "cyber"(helm, from which also come the terms "government" and "cybernetics") without knowing its meaning but just because it was interesting.

Over the years, many have tried to justify the use of the words "cybersecurity"and "cyberspace"in science without finding a shared or rigorous solution, which has spread confusion and false expectations. For example, it can be used to mean something both broader (e.g. if ICT security is supposed to exclude *Internet of things* or *IoT* security or *Operational technology* or *OT* security, that includes *industrial control systems* or *ICS* security, that includes *supervisory control and data acquisition* or *SCADA* network security) or narrower than ICT security (e.g. excluding physical and environmental security for ICT systems) or to put a name to security on the Internet, including phenomena such as online bullying (*cyberbullying*).

2.2.1 Confidentiality

Some incorrectly equate information security and confidentiality.

Common sayings in ICT include "a secure computer is shut down or, better yet, broken"and "the only truly secure system is powered down, smothered in a concrete block, sealed in a room with walls shielded with lead, and protected by armed guards, and even then, you might have any questions about"[24]. Obviously, this approach doesn't take into account the availability of information.

Confidentiality is often tied to secrecy, but the need to maintain confidentiality doesn't imply disclosing information to no one, but rather determining who has the right to access it.

It is not easy to determine the characteristics of confidentiality of any information and who has access to it, as shown by the following example.

Example 2.2.2. In a company, employee information is always controlled, but some people have access to it such as the appointed physician, management, executives, certain public agencies, the accountant, and the legal department.

Each of these entities shouldn't have access to all the data, but only part of it: payroll for the administration, health data for the physician, etc.

The level of confidentiality of information may change over time. A perfect representation of this concept is the U.S. Freedom of Information Act which establishes *declassification* guidelines (i.e. the removal of secrecy constraints) for government information no more than 50 years after their inception.

[12] http://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/

Example 2.2.3. The characteristics of a new car model have to be kept confidential. At design time they must be available to designers, at production times to workers, but in the end, when cars need to be sold, information must, albeit partially, be made publicly available.

2.2.2 Integrity

If something is incorrect or altered in an unauthorized manner, then it is insecure.

Example 2.2.4. Richard Pryor, in 1983's Superman III, manages to steal money from his company after having altered the accounting system.

He was allowed to access the system and see the recorded information because he worked in the accounting department, but he definitely couldn't have altered it without authorization.

Deleting information is an extreme form of alteration that also affects integrity.

2.2.3 Availability

Most people, as mentioned above, focus on confidentiality. Many computer experts, on the other hand, think that security is the ability to deliver requested information as soon as possible. However, this can't be always the case, so the availability parameter can be reformulated as follows: "information must be available within the established delay to those who need them and have the authorization to obtain them".

Example 2.2.5. The "delay"depends on various factors: milliseconds in the context of equity stock exchange, seconds in the context of an e-commerce website, a few minutes in a bank branch.

Availability can have impacts on confidentiality or integrity. Top management must establish what is more and what is less important and communicate it in the information security policy (paragraph 12.2).

Example 2.2.6. Backups improve the availability of information, but increase confidentiality risks because data are duplicated and they can be stolen.

2.2.4 Other security properties

The three properties described above constitute the classical definition of *information security*. Some people add others, like *authenticity*, *completeness*, and *non-repudiability*.

Information is *authentic* when it attests to the truth. This property is a specific form of integrity: non-genuine information is information that was modified without authorization.

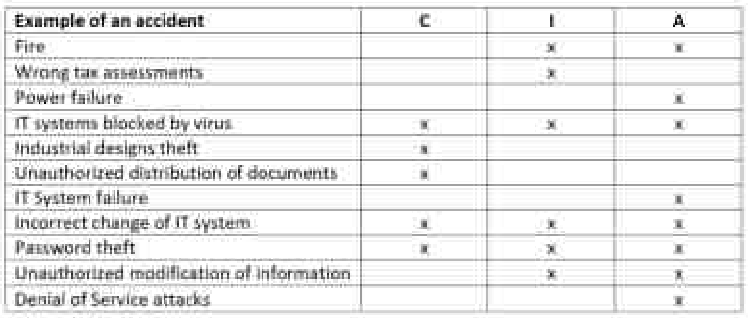
Information is *complete* if it has no deficiencies. A deficiency is equivalent to a total or partial cancellation of data, which is another special case of integrity.

Accurate information that is subsequently denied by its author is *repudiated*. It's easy to see how important it is to have information that cannot be repudiated: promises are kept and debts paid on time. A document signed by its author is an example of non-repudiable information. In other words, information is non-repudiable if it is complete with a signature or its equivalent; this parameter can also be viewed as a special case of the integrity.

Example 2.2.7. Each event can have an impact on one or more parameters. Table 2.2.2 links examples in the chapter opening with CIA parameters.

People may disagree on which parameters can apply to an example. The first thing to determine is whether a parameter is assigned according to the direct or indirect effect of the event: in case of the stolen Sony passwords, the direct effect only affects confidentiality, but it may later concern integrity (if those passwords are used to modify the data) and availability (Sony had to lock the site for several months).

Fire is associated with integrity and availability, but confidentiality could be affected if the evacuation of a building allows access to unauthorized persons or causes the scattering of sensitive paper documents.



Example of an accident	C	I	A
Fire		x	x
Wrong tax assessments		x	
Power failure			x
IT systems blocked by virus	x	x	x
Industrial designs theft	x		
Unauthorized distribution of documents	x		
IT System failure			x
Incorrect change of IT system	x	x	x
Password theft	x	x	x
Unauthorized modification of information		x	x
Denial of Service attacks			x

Figure 2.2.2: Events and CIA parameters

Another parameter of information (from the legislation on personal data protection) is the *right to be forgotten*, namely the need to delete information, whenever possible, to ensure the rights of data subjects[13].

2.3 Organization, processes, and functions

In accordance with ISO standards, we'll use the term *organization* to indicate any form of enterprise, company, institution, association, agency, etc.

Another definition is that of *business*: many standards distinguish between *business activities*, which are those that directly contribute to production or

[13] https://www.bbc.co.uk/news/world-europe-27388289.

service delivery, and *support activities*. In some texts. the term *business* refers to people who are not involved in the management of ICT systems.

This differentiation could make ICT seem extraneous to an organization's other activities, so we won't use the term in this book.

An organization consists of processes and functions, described below.

2.3.1 Processes

This definition comes from ISO/IEC 27000.

> *Process:* set of interrelated or interacting activities which transforms inputs into outputs.

This definition may seem trivial, but complexity lurks behind it.

Example 2.3.1. Consider the process of training staff. The inputs are the training needs and the output is the improvement of the employees' skills.

However, things aren't that simple. The inputs include the costs, budget, course dates, availability (if any) of a training venue, any offers and invoices from suppliers, the days when the teacher and staff are available. The outputs include the comparison of the costs and budget, the choice of training method, offer requests, orders and payments to vendors, invitations to the course, and test results.

There are many activities involved: collecting training requirements, tracking costs and comparing them with the budget, choosing the courses, dates, participants, and venues, summoning participants, confirming with and paying the vendor, collecting and submitting exam results and so on.

Each of these tasks can be performed with different tools (IT or non-IT).

A characteristic of processes, implicit in the definition, is that they must be kept *under control*, so that they provide the expected outputs and that deviations from the intended direction can be prevented or at least detected.

The control can be performed daily by individuals and their managers and periodically through checks or effectiveness and efficiency measurements. The ISO 9000 standard gives:

> *Effectiveness*: degree to which planned activities are realized and planned results achieved.
> *Efficiency*: relation between results achieved and resources used.

Example 2.3.2. Test results, costs, and manager and trainee satisfaction can all be used to measure the learning management process.

The following are characteristics of processes:

- each input is from internal functions or external entities, such as customers and suppliers;

- tools are used for each task in the process (e.g. forms and means of communication for administrative tasks; machines for manufacturing activities; software for computing systems);

- responsibilities are assigned for each task;
- there are established procedures to control the process;
- each process has outputs and each output has recipients, i.e. internal or external functions.

These expressions used when designing processes: they are *mapped* as they are and *modelled* as they are intended to be.

When mapping or modelling processes, there is no need to describe all details: real life is always more complicated than every possible description. The important thing is to have enough details to monitor the processes, explain them to interested parties (including those who have to implement it), and improve them.

2.3.2 Functions

An organization is structured into *functions*, i.e. groups of people usually gathered in offices or in boxes on an organizational chart.

Processes describe how functions interact with each other or within themselves, as shown in figure 2.3.1.

I *processi* descrivono come le funzioni interagiscono tra loro o al loro interno, come schematizzato in figura: 2.3.1.

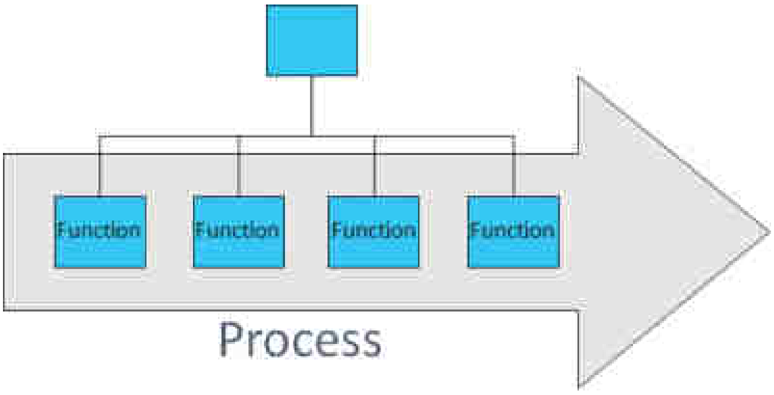


Figure 2.3.1: Process and functions

Communication within the same functions or between separate functions must use agreed-upon channels.

Example 2.3.3. For the training process, impacted functions may include the trainees' manager, the HR office, the finance department, and the purchasing department.

These functions can communicate via e-mail, computer applications, paper, or orally.

2.4 Processes, products, and people

Processes are important for the implementation of an information security management system, but they are certainly not sufficient. People and products are critical as well.

It is necessary to employ qualified individuals who understand and achieve information security by applying the right processes and using suitable products. These are the three Ps: processes (or procedures), people and products. In Appendix B, we introduce a fourth P for suppliers (partners).

Example 2.4.1. A race car in the hands of a newly-licensed driver wins no prizes and would presumably be dangerous because the driver has poor knowledge of procedures, lacks experience, and probably overestimates his or her abilities.

A less challenging car, in the hands of a skilled driver, would almost certainly get superior results thanks to better preparation and better knowledge, both theoretical and practical. However, only a correct combination of car, driver (with his team of mechanics), and procedures leads to the best result: victory.

Which of the three Ps is the most important? None of them: all must participate in a balanced way to achieve the goal.

Regarding information security, an antivirus is definitely an important product, but so are the procedures to keep it up to date and the people responsible for its installation and configuration.

When talking about people, we must address multiple issues, each involving a different task. Just like in Formula 1, where there are mechanics, engineers, and specialists, each trained for an apparently simple job such as changing a bolt on the wheel, information security is now a subject so complicated that you need not just one but many specialists that deal with specific processes and employ specific products.

For example, you'll need an information security management specialist, closely connected with the information systems manager, who depends on various specialists (e.g. on network equipment, servers, personal devices and software applications).