SICUREZZA INFORMAZIONI

The First 100 Days

of the Information Security Manager

Oracle Community For Security

Dealing with the issue of Information Security in stages

Cover page: diagram of Antikythera mechanism - processed from Wikipedia image

CONTENTS

Contents 3
1. Management Summary 4
2. Motivation, Objectives and Scope of Document 6
3. Rules for using the document 8
4. Context analysis 9
4.1 Macro-economic and social context 9
4.2 Technological context 11
4.3 Security context 13
5. Security in "Made in Italy" enterprisees 17
5.1 The role of the Information Security Manager in business environments 17
5.2 Legal aspects - reference framework 20
5.3 Factors contributing to Information Security 24
6. The first 100 days of the Information Security Manager 29
6.1 Methodological approach 29
6.2 Establishing the conditions of entering the company and knowledge of the business 34
6.3 Analysing the current situation and drafting a plan of action 35
6.4 What to do: the current and essential issues 46
6.4.1 Security policies: what's in place and what needs doing 48
6.4.2 Conformity management 49
6.4.3 Data classification 50
6.4.4 Inventory of Assets 51
6.4.5 Adopting and/or configuring perimeter protections 54
6.4.6 Wireless network security 56
6.4.7 Patch Management 58
6.4.8 Hardening 60
6.4.9 System Vulnerability Checks 62
6.4.10 Protection against malware and minimum safety measures 63
6.4.11 Digital Identity Management 64
6.4.12 Managing access to data and IT resources 66
6.4.13 Incident management 68
6.5 Long-term strategy 70
6.6 Training and awareness- raising 73
6.7 Reporting on the 100 day results 74
7. Annexes 78
7.1 Brief overview of international security standards 78
8. Authors and contributors 79
8.1 Team leaders and editors 80
8.2 Authors and contributors 80

1. MANAGEMENT SUMMARY

The role of ICT systems and the relative management processes in small and medium businesses, has over recent years seen constant evolution both in terms of the consolidation of some phenomena not deemed especially innovative (e.g. the digitalisation of business processes, the gain in popularity of multi-channel services for access to applications and services, etc.), and the appearance of new paradigms, such as the adoption of Cloud Computing services, the use of Social Networks, Mobile Computing or Big Data.

The technologies related to these approaches and solutions enable enterprises to introduce new models and instruments useful to achieve their current business priorities within the organisation, but at the same time expose data and corporate information to new security risks.

It is therefore evident that these technologies lead to new challenges that require an innovative approach in managing IT systems and the related security aspects, especially as those used until now have shown limits that are inadequate for dealing with these new challenges and changes.

In this scenario, one of the elements to ensure continuity in the business environment is undoubtedly the attribution of responsibility for protecting data and information to a single specific representative within the company, who in this document will be referred to as "Information Security Manager"

Whether this is a dedicated role or not, whether created within the context of a business environment or acquired on the market, the Information Security Manager finds her/himself facing a range of challenges and will certainly be required to fulfil a variety of tasks, ranging from simple to more complex procedures, either requested by the company management or required as compulsory by law. Some tasks will be particularly visible, others decidedly more "transparent" to the various company positions, but equally relevant [1].

Of these tasks, some must be implemented as promptly as possible while others may lead to results only in the medium and long term.

For this reason, it is reasonable to assume that on his/her definition / employment the Information Security Manager may well ask him/herself:

- can the security issues be dealt with in a structured manner?;
- which elements and activities need to be considered priority, and which not?
- do different possible solutions share common aspects?

With this document, the Oracle Community for Security has set the objective of supporting the Information Security Manager in addressing all these aspects, at least in the initial period in this role, in order to define concrete objectives, propose actions that can lead to visible results, as well as offering an approach that enables constant performance and improvements over time.

With this objective, even considering the vast amount of problems to be dealt with, the Community maintains that in the first 100 days, the Information Security Manager needs to address at least the following aspects:

- to first of all establish a systematic approach to the protection of company information, based on an iterative model (PDCA), which envisages ongoing improvements to assigned tasks;

[1] In the end, a good security manager is often seen as the person able to guarantee that business can go on without any significant security event, within the agreed financial constraints…

- to become aware of the initial setting of the company where s/he is to work, using structured approaches and suitable tools (presented below as Quick Assessment), without neglecting to seek the resources and necessary support from within the company, before looking at external security suppliers, products and services;
- to fully understand the assigned role and relevant responsibilities, also to establish strong working ties with those colleagues in company roles where interaction is most likely,
- to plan, on the basis of effective models, activities for the development of the Information Security Management System (ISMS), guaranteeing both the need to cover all the above-mentioned issues, and the need to highlight the achievement of immediate improvements, working on multiple levels of intervention. This basically means that this planning phase should involve the creation of parallel PDCA cycles for improvement;
- to guarantee, in any event, to constantly have under control all aspects related to legislation and standards as relevant to the industrial sector in which the company operates, both in terms of aspects related to the new role taken on (for example, the Italian Workers' Statute, the so-called Administrative Liability of the companies, etc.) and for more broad-reaching legislation which may impact on company information (protection of personal data, intellectual property, etc.)

2. MOTIVATION, OBJECTIVES AND SCOPE OF DOCUMENT

The main objective of this document is to provide a series of suggestions, not only with regard to methodology, but also practical hints for all those who, for various reasons, have been assigned specific responsibilities for the protection of data and information.

Indeed the Oracle Community for Security believes that there is an evident need to create awareness and competence in concrete issues related to information security, such as those faced by a newly assigned Manager in a small or medium Made in Italy enterprise.

This aspect becomes even more critical when we examine the evident gap frequently found between the level of security that would be needed in the company to guarantee a reasonable level of information protection, and that effectively in place in the various companies with whom the Community deals on a day to day basis.

Without taking individual cases into consideration, this discrepancy is obviously attributable to a series of elements shared on an Italian setting, with the main ones already easy to identify:

- the difficulty, in the current economic climate, and thus relative constraints on ICT and IT Security investments in Italy.
- the cultural approach to the issues of security, which has always been rather limited;
- the introduction of new technological paradigms that significantly extend the security risks;
- the introduction of new types of “attackers” (internal, such as dissatisfied employees or external, such as new types of computer hackers);
- the emergence of phenomena on a world scale, such as industrial espionage or cyber crimes, which are much more frequent than one would imagine.

Thus, while on the one side the opportunities of these new paradigms find omnipresent and highly effective echoes in the media, on the other the initiatives aimed at analysing these events and addressing the security challenges are still seriously limited or superficial. Articles in the media and numerous conferences highlight events that have occurred (for example the latest “defacement” of a famous website of this or that private organisation, or government authority), but nevertheless tend not to offer possible strategies to prevent such incidents.

This approach is in part attributable to one of the aspects mentioned above, i.e. the serious need to suitably raise awareness of security issues and thereby achieve company commitment in this area, and not only in financial terms. The ongoing difficulty lies in convincing the company to employ “known” economic and human resources to deal with an “unknown” danger.

At the same time, objective accident prevention is complex. It involves constantly pursuing a moving goal, which aims to see the enterprise evolve, and requires the IT department and the relative security component to evolve at the same pace, or even anticipate these developments, enabling new ways of interacting with clients, saving on costs and all other aspects deemed useful or necessary for company success. Therefore there remains little time and few resources to dedicate to security “by design”.

On the other side of the “barricade”, the attackers are continuously developing new mechanisms, methods and tools, and in some cases adopt approaches that could be described as “Crime as a Service”, with a division of roles and “tasks” on an international scale, achieving high earnings while drastically reducing the risks to those who they commit crimes against.

Meanwhile, the crisis and social discontent increase the tendency towards unlawful behaviour by company personnel themselves.

Obviously the best practices used to implement an Information Security Management System (ISMS, as defined by international standards) are comprehensive and have been developed with great expertise. The regulators of all types (the Italian State, European Union, trade organisations, the Data Protection Authority, and all bodies that have issued and promoted sector standards, such as PCI-DSS, Basilea II and III, etc.) set down codes of conduct and safety measures that in general make sense, but where do we start?

The efforts of the Community aim to help the newly appointed Information Security Manager make the best initial choices, or at least to identify which elements should be considered to develop and plan prospective objectives and actions, supporting the assigned priorities of the tasks both in the immediate and long term, to enable a clear understanding of the importance in protecting company assets.

Within a limited time frame of 100 days, as implicit in the title, the Community will attempt to select and propose the most significant actions to ensure effectiveness, efficiency and conformity of standards, but above all the possibility of attaining visible results in the short term, and to offer an ongoing approach that will continuously maintain and improve conditions.

More specifically, this document has been drawn up with a view to support the Information Security Manager of a medium Italian enterprise - the classic enterprise set-up that represents our nation worldwide - with all related products and services.

As regards larger enterprises, where the knowledge of some concepts outlined below is presumably greater, this document aims at offering a pragmatic and structured view of the suggested approach, with a view to consolidating the actions of this role in the company.

We hope to make this contribution to the Italian debate without the presumption that it is valid in the absolute sense, but that it draws from a broad-reaching set of skills, expertise and values shared by the participants of this Community.

3. RULES FOR USING THE DOCUMENT

The licence used, entitled Creative Common – Attribution – Share in the same way enables anyone to use our production, even to add a development, provided that the original authors are cited and that the same type of licence is still used in turn. We authorise the full or partial publication of text and images not already protected by other copyright, stating our URL http://c4s.clusit.it.

The authors freely provide their considerations in the full spirit of collaboration, which for years has united them within the Oracle Community for Security, and for whom they have made numerous other contributions for public debate, such as the documents:

- "Privacy in the Cloud: The challenges of technology and the protection of personal data for an Italian business"
- "Mobiles and Privacy: Formal requirements and safety measures for compliance in the handling of personal data within a business"
- "ROSI Return on Security Investments: a practical approach"
- "Electronic Health Records: the role of technology in the protection of privacy and security"
- "Security in Social Media. A guide to safe use of Social Media for Made in Italy companies"

For information on all the above, visit the websites of the Community and Clusit (our reference association) or the relevant pages at http://c4s.clusit.it.

4. CONTEXT ANALYSIS

4.1 Macro-economic and social context

The economic and competitive context in which enterprises work can have a significant impact on the evaluation of some risks to which each company is exposed, and thus also on the areas of attention for the newly appointed Information Security Manager.

Continuous research to attain optimum efficiency, combined with rapid changes to the business model, organisational development, various degrees of outsourcing to external partners and technologies that enable external applications of relevant IT components (such as the Cloud), in fact have a great impact on the company organisation and production, as well as commercial and technological processes. All this naturally leads to significant consequences in terms of control and security.

This section does not aim at analysing these consequences, but rather to highlight their overall relevance in countering the interpretation of the Information Security Manager as a technical and sector-specific role, focussed on the technological infrastructure and relative malware, firewalls etc.

4.1.1 Outsourcing company processes

One example is the case of outsourcing company processes. The decision alone of evaluating the opportunity of outsourcing a task or company process inevitably impacts on internal relations, generating tensions within the departments concerned. Once aware of this fact, the relation of trust between company and employees, together with some consolidated work practices, ceases to become taken for granted. Those who feel their position is questioned for reasons beyond their professional capacity and the efficiency of their department or position itself inevitably then start to question, wholly or partially, their loyalty to the company itself.

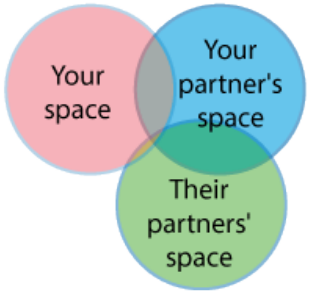
This type of context is undoubtedly more vulnerable to internal sabotage or fraud, and at the very least is more exposed to a risk of social engineering. In the case where the people involved belong to technical structures working in an IT environment, this can also represent a risk for the infrastructure. In these cases, customary practices, even if formally prohibited, such as the knowledge/sharing of credentials among a small group (director-assistant; director-direct subordinates, between colleagues and between system administrators) are transformed from minor sins into acutely dangerous vulnerabilities. Additionally, any increasing discontent increases the probability of unauthorised release of critical and reserved information, even as a means to find new employment.

It is also worth noting that this problem arises not only when an area is re-organised, but also starts to emerge when a plan simply to evaluate a different organisational option enters the public domain.

A highly topical example in this regard, which has significant impact on the enterprise organisation, and affects the security of a company ICT, is certainly the emergency option of using the external services of Cloud computing. The Information Security Manager is not usually a stakeholder in this category of business decisions but evidently has to be part of the management process of the decision itself. The critical nature of his/her role naturally depends on the type of company business and increases in proportion to the critical nature and attractiveness of company information which is made accessible outside the organisation.

4.1.2 Relations with External Partners

Another type of situation in which the role of the Information Security Manager is highly relevant consists in the involvement of external partners in the area of marketing. Examples would be production or other relevant activities such as customer care or telemarketing/teleselling, as well as the practice of outsourcing to external suppliers as backup to in-house resources in order to complete work tasks, a frequent option in the IT departments of Italian companies.



In all these cases, the company perimeter is modified in order to include all or some of the supplier companies, business partners or external consultants, meaning that each security strategy based on perimeter defence needs to be reviewed.

However, it does not end there. The most critical aspect is that company security thus depends on the degree of security of the partner organisations involved and, in turn, their network suppliers.

Figure 1 Breakdown of the organisation and process confines with partners

In this way it would be reasonable to expect that aspects of security and compliance in relations with partners are and must be dealt with contractually, envisaging specific forms of control and obligation. On the other hand, it is far more difficult to intervene in the relations that the partners themselves have with their sub-suppliers or partners.

Naturally, each assessment needs to be approached in relation to the degree of critical information concerned and the assets managed by the company. However, it is definitely recommended that this assessment is based on considerations made within the broader scope of business decisions. In fact post-decision interventions frequently lead to additional burdens for the company with regard to new imposed obligations. Indeed even in the least problematic cases, such as a detailed contract of a non-critical business, an adequate security model for cooperation with external parties cannot be the same one used in a traditional company with a well-defined physical perimeter and IT system, if any already exist.

In the two elements described, business demands, originating from company departments other than IT generate phenomena that deeply affect the setting, and therefore also the probability of harmful events. The same risk assessment cannot give the same results if conducted at a time of business growth or at a juncture of painful re-organisation, or when outsourcing activities that concern a large number of employees. The results and security strategies that arise from these assessments may therefore no longer apply.

The success of intervening not only in terms of the choices, but also cost analysis and impact evaluation of these decisions implies acknowledgement by the company of the role of the Information Security Manager. This is not always obvious and certainly not easy to fulfil.

The essential premise to achieve these results is the awareness of the Information Security Manager him/herself of the assigned role, which needs to be consolidated immediately.

The first one hundred days are therefore essential, not only to achieve concrete results, but also to avoid any delay in affirming the relevance of these aspects in the contexts of the relevant enterprises.

4.2 Technological context

The technological context that has characterised the ICT sector in recent years has seen the consolidation of certain long-term trends, such as an ever increasing digitalisation of business processes within both public and private organisations, and the increasing popularity and importance of internet and mobile multi-channel strategies to access applications and services. At the same time, we can see new phenomena emerging with potentially disruptive effects: Social Networks, consumerization, BYOD (bring your own device), cloud computing and big data. Technologies related to these latest trends promise to provide now tools useful for achieving the current priority business objectives of organisations, resulting in significant impact on ICT expenditure over the next few years.

4.2.1 Digitalisation of business processes

In recent years we have witnessed a broadening of the scope of the original dematerialization of hard-copy projects, as companies have realised that digitalisation in the broad sense of enterprise processes can lead to much greater savings, and the increase in personnel productivity made possible by the more efficient processes can be extremely significant. And in fact, digitalising means first of all redesigning company and inter-company processes in the light of technological opportunities, trying to exploit the exchange of information in a structured and processable format. The drive towards digitalisation resulting from the definition of the regulatory framework at a national level was fundamental, in particular with the introduction in 2005 of the Italian Digital Administration Code (DAC) (*Codice dell'Amministrazione Digitale - CAD*) and the new DAC at the end of 2010. These laws in Italy have generated considerable impetus to the digitalisation of relations between public administration, citizens and enterprises, with a potentially significant impact on all sectors, such as Italian Health Services, the Taxation Bodies and Social Security. Some of the specific areas of intervention of the Code are dematerialization and document retention, the IT protocol and electronic health records, electronic payments and invoicing to the PA, together with enabling Italian services such as certified email (*Italian* PEC), electronic signatures and electronic identity card (eID) and National Services Card (*Italian* CNS).

4.2.2 Multichannel Internet and mobile devices

Despite Italy's domestic Internet access still being far from satisfactory compared to the European average in the 27 countries with an even more significant gap in the area of broadband connections, Internet usage has still more than doubled in the past decade, highlighting the increasing use of this channel as a means of communication even here.

The strategic importance of the availability of broadband and ultra wideband connections for the development of the Italian economy, is shown by the processing of the corresponding National Plans for Broadband and Ultra Wideband and the great debate on the creation of a Next Generation Access Network (NGANs).

On the mobile device front, Italy's position as reference market for mobile phones has been consolidated over the years and with the sales of smartphones overtaking those of traditional phones in 2011, we are now witnessing the explosion of the tablet and touch screen interfaces.

At the same time, penetration of mobile data services is growing, in anticipation of the launch of the new 4G networks (LTE) in 2013. The changes in the way business is done by companies and organisations is even more significant, thanks to the spread of the Internet and mobile devices.

4.2.3 Social Network

The widespread use of social networks in Italy (approximately 22 million Facebook users, 2.8 million LinkedIn users and about the same number of Twitter users) is testament to the emergence of new forms of interaction and socialisation, made possible by the new media. It is therefore natural that, even within the workplace, companies are assessing

the possibility of applying similar models in order to develop more effective forms of collaboration which are in line with the times.

4.2.4 Consumerization

Unlike the past, thanks to the increasing penetration of Internet connectivity and mobile terminals, many of today's trends started in the consumer world (Social Network, applications for mobile devices) but ended up finding their way into the workplace. As first generation digital users make their way into the world of work, this trend is accelerated even more, requiring new ways of communication both within and outside companies. In concrete terms, today (and ever more frequently) employees want to have more say in the devices, services and applications used and which they can access to obtain the best functionality, user experience and flexibility.

4.2.5 Bring Your Own Device

Related to the previous phenomenon is the trend indicated by the acronym BYOD (Bring Your Own Device). This refers to the increasing use of company policies that allow, or even encourage, the use of personal mobile devices in the workplace, allowing them to be used to access information and business applications. The potential benefits we commonly find include the ability of employees to better combine work and personal commitments, resulting in higher productivity and satisfaction, more rapid introduction of technological innovations related to new devices and reduced costs.

However, BYOD introduces new risks, particularly the loss of direct control by the company of the devices themselves and the location from where (physical and virtual) the information is processed and once again, the proliferation of the boundaries mentioned above.

4.2.5 Big Data

The amount of data managed by the ICT systems has exploded in recent years thanks to the increasing number of channels and communication formats used (voice, video, email, texts, tweets), the spread of social networks and the first examples of the use of the so-called “Internet of things” (RFID, QR Codes, NFC, etc.). The ability to efficiently analyse this massive amount of data to gather information on the tastes and behaviours of customers and prospects will be an important factor in terms of competition for organisations.

4.2.6 Cloud Computing

Cloud computing in its various forms (public, private, hybrid or community clouds) and services (IaaS, PaaS or SaaS), is radically transforming the ability of companies to offer new services by reducing the time-to-market, improving efficiency in the use of ICT resources (elasticity / self-service) and making costs variable (pay per use). These benefits are not just within the reach of large companies but also SMEs and Public Administrations, who have the opportunity to innovate and significantly improve their efficiency and effectiveness. The renewed effort towards the establishment of a national Digital Agenda and new themes, such as that of Smart City, extend the potentially beneficial impact of the spread of cloud computing even further.

All these elements of technological innovation, which appear and are combined in different ways within each company, and where security is often not planned in the initial phase, involve a series of challenges that the new Information Security Manager has to deal with: he/she must comply with these elements for the business, understand their limitations in terms of security, and control them while paying close attention to the risk profile.

4.3 Security context

Thanks to the evolution of mobile devices, the advent of Cloud Computing, the spread of social media and collaboration systems, society is changing the way it communicates, progressing towards a new global dimension. But the security risks of this paradigm have not yet been fully understood and neither is there is a full awareness of the rapid evolution of methods and tools that hackers use.

As illustrated by the recently published 2013 Clusit Report on the ICT Security situation in Italy, the amount and types of attacks by hackers are changing considerably, with a significant increase in incidents caused by hackers, cyber criminals and cyber warfare between 2011 and 2012, and a trend that is decreasing but nevertheless high in terms of IT violations by unidentified people.

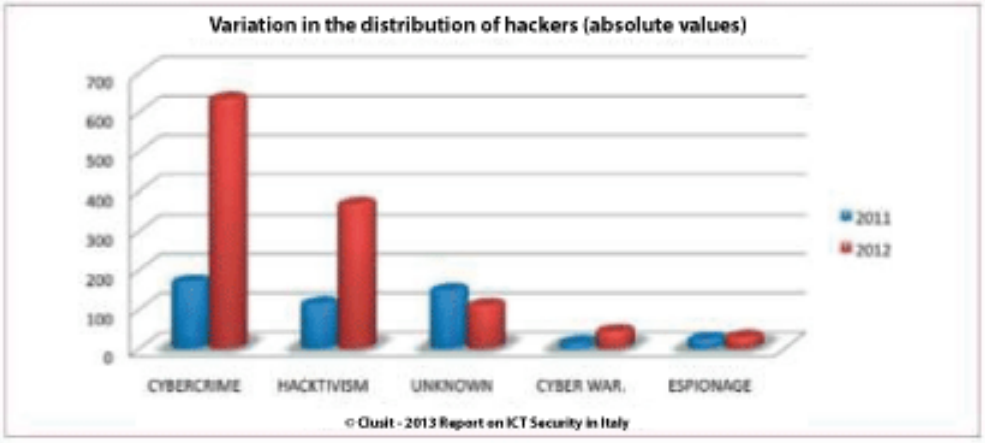


Figure 2 Change in the distribution of hackers from 2011 to 2012

The very face of hacking has changed. The hacker portrayed in films of the 90s was the brilliant yet misunderstood boy, hidden away in a basement, familiar with every nook and cranny of the protocols, exploiting the loopholes to prove or improve his technical ability and the quality of the protocol itself. Today however, the protagonists in the media are so-called “hactivists”. These are groups of people who, even without great technical skills, use ready-made tools in the name of protecting civil rights and civil disobedience to make their grievances known to government organisations, enterprises, celebrities and institutional bodies. Their typical attacks exploit (or extort) the strength of the community to carry out DDoS attacks designed to interrupt services or deface corporate websites, most of the time without obtaining any direct economic profit.

But in the shadow of all this, and the more recently significant media presence enjoyed by the hacktivists, organised crime, which several years ago started a process of global affiliation to exploit the imperfections resulting from the evolutionary developments, has begun to move undisturbed in the underground.

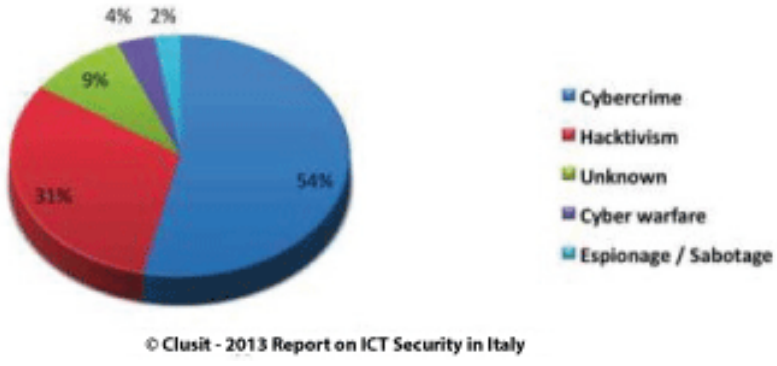


Figure 3 Type and distribution of hackers in 2013, related to the analysis of 1,183 known attacks

This phenomenon is confirmed by the Clusit Report, showing that overall incidents caused by cyber-criminals exceed those caused by hacktivists, despite the impression given by the media.

It is important to note that these individuals seek to remain in the shadows and take advantage of flaws in security in order to steal valuable information and trade secrets (credit cards, customer lists, credentials, health data, etc..), thus making it even more difficult to determine the actual extent of the attack and how it was carried out.

With a "turnover" of approximately 10-12 billion dollars a year and causing economic damage reaching several hundred billion, Cyber Crime obtains financial benefits by using unconventional computerized means which are easily available on the black market, carrying out attacks that take advantage of the large exposed areas resulting from the spread of malware and phishing.

No official statistics are available but in Italy alone, some companies in the sector estimated that approximately 2.45 billion Euro disappeared from the pockets of Italian citizens from January to September 2012 with 8.9 million individuals over the 12 month period being victims of a crime, which is one-third of active Internet users in Italy in 2012. According to the same report, Italian companies spend 78 Euro for each compromising situation on investigation, notifications, legal fees and costs associated with the interruption of their business. Rome is the second largest city in the world when it comes to Bots (60,000 machines compromised in May 2012) and Milan is the seventh in Europe for digital crimes.

Figure 4 Italian cities making the headlines for questionable ICT "insecurity"

Another significant element in the overall context of IT risks is represented by industrial espionage and sabotage, which as noted may even be sponsored by nation states to collect information from industry, and foreign government institutions or to attack critical infrastructure.

Usually industrial espionage is carried out through APT attacks (Advanced Persistent Threat) which is usually completely invisible and capable of collecting data and information.

Finally, Italy is unfortunately also in line with all the negative indicators of a global nature which refer to the hactivist matrix attacks against government agencies, universities, political associations, police forces and companies of various kinds.

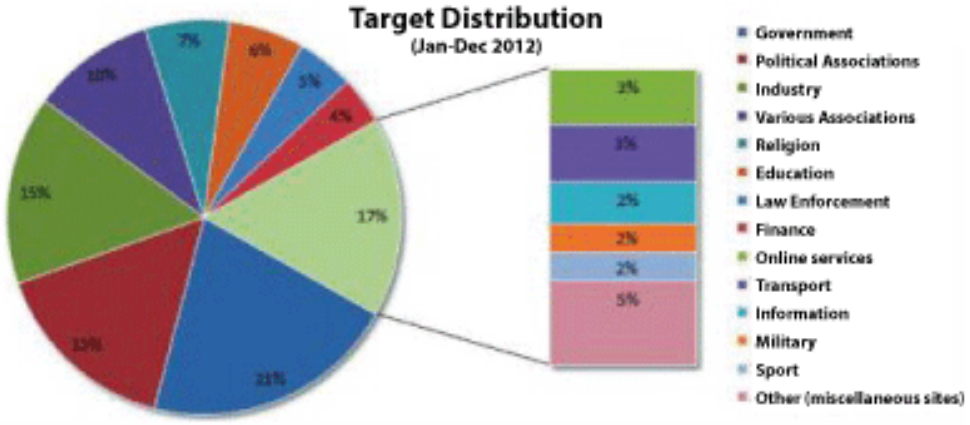


Figure 5 Distribution of the targets of attacks in Italy (sample of 196 known attacks) - Source: CLUSIT Report 2013

In this scenario, two different but extremely significant phenomena emerge in Italian companies:

- the imbalance between investments made in security and the perception of the results obtained;
- a rather broad scope of organisations where security issues are only marginally addressed; despite the high (and undeniable) dependence of the business on services provided by ICT, companies assume a passive role, or at most, a responsive approach to security issues.

In the first case it is possible to easily recognise those companies in which an attempt has been made to address security issues in a more or less mature way. It is more than likely that in these contexts significant results have in fact been obtained, but it is extremely difficult to estimate a direct benefit from increased security.

The second case characterises in general the vast and extremely diverse world of Italian small and medium enterprises, and can be easily interpreted by the fact that there is still a market for “off the shelf” security products rather than a structured offer of skills and solutions based on real needs. These constitute a fertile “substrate” for the phenomena such as the spread of malware and the growth of botnets available to Cybercrime.

And what about large companies? Reading the descriptions of the attacks indicated in the Clusit Report, some large companies still clearly have difficulty in effectively managing the processes which are the basis of good IT management such as patching, or security process management, periodic monitoring etc. (e.g. Vulnerability Assessment - Penetration Test). According to the findings following the most publicised attacks, no particularly innovative techniques were used to violate the public sites and data centres of the numerous targets that leapt onto the front pages.

It is therefore undeniable that the new global and local challenges have tested the confidence that companies have placed in security management systems which they had relied upon for years. This is often because these were based on obsolete models, at times only adequate from the formal rather than a substantive perspective and they proved to be inappropriate to handle the new challenges and changes which have taken place.

In brief, the Information Security Manager can not ignore the emerging technological trends and phenomena that have the greatest impact on the ICT field (§ 4.2) and significant consequences on the way security is handled. One particular example is the dissolution of the company perimeter and the exponential growth in the volume of information processed together with the increasing pervasiveness and need to exchange this information.

Furthermore, within the overall equation which governs the workplace, we need to address the lack of awareness among users with regards to the security risks in the face of increasing threats and hackers, while at the same time ensuring the protection of trade secrets and compliance with laws and regulations.

Effectively addressing these issues certainly requires a change in approach compared to past traditional methods, often based primarily on prevention mechanisms to protect the perimeter.

The company that adopts a critical view towards its own security management system certainly demonstrates a “healthy” attitude towards this issue. The creation of the role of Information Security Manager, if non-existent, or the appointment of a new manager, is a first step towards implementing the changes required.

In any case, even if the number and the complexity of the issues involved is high, the Information Security Manager must not forget to look within his/her own company, before looking externally (suppliers, products, etc.) for the necessary resources and assistance. This will be a crucial element in the interaction with other organisational functions and by and large, achieving and maintaining concrete results from a security perspective will greatly depend on this. This will be discussed in the next chapter.

5. SECURITY IN "MADE IN ITALY" ENTERPRISES

5.1 The role of the Information Security Manager in business environments

5.1.1 The role

Considering the complexity of the current business climate as highlighted above, it is easy to understand how information represents a critical element in the pursuit of objectives and strategies.

The role of the Information Security Manager is therefore to ensure that information is correctly protected, but at the same time can be easily accessed.

This protection must be all-encompassing, as also indicated by the standard ISO-IEC 27001, ranging from purely logical aspects (related to IT systems) to organisational issues and regulatory compliance.

For this reason, it is easy to understand how the responsibilities and the role may present areas which overlap with other possible roles within the company in some cases introduced by explicit regulatory requirements.

For example, the rules on the processing of personal data require measures that have a direct impact on security management of information (e.g. known in the Italian regulation as "minimal measures"). This involves a very close relationship with the tasks of the Compliance Manager, if present. At the same time, in the case of personal data, there is a similar relationship with the role of the Data Protection Manager, and the probable introduction of the European regulation on privacy. Finally, there is an obvious relationship with the Security Manager, both in how often the Information Security Manager actually responds hierarchically to this role and because some tools for physical security have an important ICT component, such as IP cameras. It is worth noting that the difference between Safety and Security, "sicurezza" in Italian for both, may not be clear to those who interact with the Information Security Manager. These two roles must therefore, be fully aware of what lies within their competence, and make sure that these boundaries are also clear to the company and its stakeholders. At the same time, especially in smaller companies, it is possible that the same person could cover multiple roles, both at a management level (for example, he/she could also be the Data Protection Manager) and at a more operational level, for example, also holding the role of IT Security Administrator. There are generally no negative effects to this type of overlap, but this document is, however, focused on the specific role and responsibilities of the Information Security Manager.

It is useful to point out that the Information Security Manager is generally referred to at the international level by the term CISO (Chief Information Security Officer).

Finally, with regard to the role of Manager, the position within the company's organisation chart could be discussed.

Where there is a specific position of IT Security Manager, the corresponding functions are usually carried out, more or less implicitly, by the IT Manager. This is because they are functions that require specific technical expertise. It is common therefore, that when the role of Information Security Manager is established, this person will answer directly to the IT Manager. From an operational point of view this can be seen as an advantage, but if we consider the decision-making autonomy which the Information Security Manager may possess, it could be detrimental, especially when the job would require him/her to put constraints on the activities of the IT department. The alternative is that the Information Security Manager answers to the Safety Officer, formally a position which is more appropriate and provides greater autonomy, but often has two disadvantages. The first,

and one which should reduce over time, is that many Safety Officers have little sensitivity to the importance of IT systems, and therefore tend to give little space (and few resources) to the Information Security Manager. The second is that the IT system management requires the management of certain operational aspects of System security, which end up being dealt with internally, creating roles that duplicate some of the tasks for which the Information Security Manager is responsible. Although the Information Security Manager does not generally have too much control over this dynamic, it is desirable that this is taken into consideration in order for this position to be fulfilled in the most effective manner.

This brings us to the role of Manager within the company. It must be remembered that the task is not limited to ensuring that technological management of information is carried out in accordance with good practice or standards. The task is to help ensure that the company can achieve its business goals safely and effectively. To do so, the company business must remain the centre of attention: security needs to be a tool used to reduce the risks without unnecessarily reducing the operation.

The manager must therefore know the company, talk with the managers of the other areas in order to understand how to support them effectively in safely reaching their goals. Often, however, the Manager tends to stay within his technical role, isolated from the rest of the company. This generally leads to security management being difficult to understand and use, and ultimately less effective, given the fundamental role played by the human factor.

Finally, the Manager must know how to interact with other roles which are important to the business. This could include the Police Force, who they may need to involve when dealing with incidents and it may be helpful for them to be contacted in advance in order to be able to work quickly when an emergency arises. Another example would be suppliers, whose management is increasingly critical to company security.

5.1.2 The Responsibilities

Starting from the main objective of ensuring the proper protection of information, there are several specific responsibilities which can be attributed to this role.

In particular, the following in particular can be highlighted:

- defining a plan and strategies for company security, which is closely related to that enterprise;
- carrying out and updating security risk analysis;
- a supporting role in defining security architecture;
- defining and adopting appropriate measures of response and incident management;
- defining and adopting models and solutions to ensure the availability of systems;
- support for the design and implementation of development projects, supporting all aspects of security;
- addressing safe aspects to reinforce and configure systems;
- monitoring the performance of protective measures.

5.1.3 Skills and expertise

In order to properly implement all the responsibilities outlined above, it is clear that the Information Security Manager should be able to provide an ample portfolio of skills and competencies so as to cover organisational, technical and managerial elements.

While it is evident that these elements depend on the specific context in which he/she operates, the fundamental factors can be identified as follows:

- **business orientation:** the role of the Information Security Manager supports the activities of business. Therefore, an essential element is that of ensuring the ability to identify the needs and business strategies in order to properly orient appropriate choices for the protection of information;
- **technical skills:** obviously the foundation needed to ensure a correct approach to data protection is that of ensuring a base of technical skills. This aspect does not imply an in-depth knowledge of all the possible vertical issues (too many to be summarised in a single point), but it does imply being able to fully understand the issues and possible solutions;
- **strong relational skills:** in the vast majority of cases, the Information Security Manager should be able to rely on support for the activities promoted despite not having an organisational or hierarchical advantage. Therefore, in order to ensure that the set objectives are achieved, it is important that he/she proves able to communicate with all enterprise functions, effectively involving them in the protection of information. He/she should also demonstrate the ability to manage any conflicts (both between roles, and in relation to the contrasting requirements to ensure complex protection elements which make operation and solutions more complex rather than keeping them simple, in favour of a greater usability of the systems);
- **communication skills:** the Manager must be able to ensure messages are correctly and efficiently directed to the technical departments, and especially towards senior management, ensuring that they are brief and appropriate;
- **innovation:** the strong dynamism in the context of information security, as highlighted in the previous chapters, requires a strong adaptability and curiosity in new technological paradigms or new solutions;
- **legal understanding:** despite the exclusion of regulatory competence being shared, it is undeniable that the Manager must be able to ensure that the protective measures taken are in line with the regulatory requirements, but also that they may not be considered illegal. We need to simply consider that the correct implementation of security aspects could be related to the adoption of complex tracking measures, which if not properly established could prove counter-productive, and lead to specific sanctions. For this reason, the Manager must be able to understand the impact on their responsibilities introduced by a constantly changing regulatory environment;
- **knowledge of standards and models:** finally, the knowledge of the management frameworks (e.g. COBIT) and/or security standards (e.g. ISO-IEC 27001), is able to guarantee a systematic and structured approach to the protection of information.

5.2 Legal aspects - reference framework

The range of standards which the Information Security Manager is required to be fully aware of is partly objective and partly depends on how the role is defined at a functional level:

Figure 6 Key regulatory areas of reference

However, there are certain rules that can be considered a common factor.

The Information Security Manager knows from the outset that he/she is obliged to work within the context of issues that have (at least potential) impact:

1. labour laws, with regard to relations with his own team and within the company;
2. connected to the legal framework for the protection of personal data.

5.2.1 Impacts of Labour Law

The Security Manager must be fully aware of the regulations which govern relations with workers, whether they are employed by the company itself or are external consultants.

Amongst the most well-known regulations there is the Italian national Workers Statute (Italian Law 300 of 1970) in particular articles 1, 4, 8 and 13 (freedom of opinion, workers' control, tasks assigned).

It must not be forgotten that often in companies which make use of consultants, behaviours are adopted which may include the offence of fictitious intervention of manpower.

5.2.2 Impact relating to the protection of personal data

Often the activities of the Manager deal with the legal framework pertaining to privacy (currently regulated primarily by Italian Legislative Decree no.196 of 30 June 2003).

This aspect must be taken into account in a variety of situations which may have an impact on privacy:

- the installation of firewalls or other tools that filter browsing activities (for example recording, the attempt to access a black-listed site) and those that involve the collection of personal or sensitive data;
- re-using or removing storage media;
- verification of the activities of the Manager and those who have authority for "system administration";
- the provision of information to the Italian Legal Authorities (not everything requested is necessarily legitimate, there could be a request for information that infringes the existing legal framework submitted without the necessary formalities);
- the recovery of a computer following resignation, dismissal or change of duties of an employee;
- the installation of a video-surveillance system;
- the installation of GPS instruments for fleet management;
- the management of security incidents involving the personal data of clients;
- the introduction of new requirements or repeal of requirements for
- many other situations.

In these areas, a common mistake is related to the media interest that often surrounds these issues, creating an illusion that the Information Security Manager is able to update simply by referring to what is reported by the main channels of information; this mistake can lead to specific measures and other relevant events being neglected as well as different regulatory areas as those which are mentioned below.

5.2.3 Other regulatory areas of interest

In practice, the Information Security Manager, especially if the scope of his/her work is not precisely defined, must also be involved in other regulatory areas:

- In terms of administrative liability defined by Italian Legislative Decree no. 231 of 2001, for example in relation to different types of crimes, the role identifies:
    - "IT crimes", art. 24 bis of Italian Legislative Decree no.231 of 2001;
    - offences relating to breach of copyright, art. 25-novies, Italian Legislative Decree no. 231/2001.

  We must not however, discount the possibility that other types of offences can be integrated by the Security Manager, for example, corporate crimes.

  The knowledge of the single presumed offences (i.e., offences that are assumed because they can be integrated with this profile), together with ethical behaviour, are key elements in preventing the integration of the profile of Responsibilities of Italian Legislative Decree no. 231 of 2001.

- The protection of know-how is another aspect which must be taken into account; the Information Security Manager must avoid any behaviour which violates the rules for the protection of patents and copyrights.

  With regard to this specific aspect, a requirement emerges which should provide significant defence and should become widespread: this refers to the introduction of the classification of company information.

Through the classification of information, the interests of the company can be protected from numerous points of view. This includes the protection of personal data, which while representing the most noted, is not the only or the most important factor (the protection of know -how is much more relevant to the pursuit of core business).

The importance of classification of information is clear when certain company profiles are enabled to use social networks or the multiple means of communication which today must be “governed”. This also applies to cases where all “social” channels are inhibited within the enterprise but are freely used in the private sector.

Furthermore, social networking management, as it has repercussions in terms of security, cannot be left solely to the marketing function but must be subject to a transversal approach by the various functions, including the Information Security Manager.

Similarly, setting an activity of software customisation or assigning a certain level of “sensitivity” to information has an impact on the activity of the Information Security Manager and his/her role in the company.

- Knowing how to protect and preserve a corporate asset and establishing the correct protection framework around it is another skill required by the Information Security Manager.

  For example, he/she should know that depending on its specific country of use, this product may be subject to a type of patent protection or copyright. He/she must also be aware that the protection framework must be designed so as to protect the company's interests within a panorama made up of countries with very different or mixed institutions, and with an organic approach consisting of a framework activity and coordination of the different elements.

  Another aspect that should not be treated marginally, concerns the analysis of markets and identifying those that promote or protect against counterfeiting. Many sectors, including the manufacturing sector are inclined to underestimate this type of problem, considering the return in terms of “expansion of the sales market” to be greater.

  In fact with the technique of reverse-engineering the “recreation” of a product is becoming more widespread by producing a new one with characteristics which are identical / similar to the original, thereby drastically reducing the possibility of identification as a counterfeit copy, so that the merit for this innovation be attributed to those who actually created it.

  Untangling the definition and assumptions of intellectual property is already complex for a specialist, and becomes even more challenging for a person who needs to monitor and take an interest in issues that are extremely diverse in genre and nature.

  Traditionally there has always been a distinction between Intangible Property, Industrial Property and Intellectual Property, however, this distinction has become obsolete, since the works protected by copyright are in fact no longer just the result of an artistic experience (works of literature, music, visual arts, etc.) but also include so-called “utilitarian” works, such as software or databases. Today, the trend is to converge on the Anglo-Saxon concept according to which the protection of copyright can not be distinguished conceptually from any other exclusive right of an intangible asset.

  Particular emphasis should be placed on this issue if the company works with companies residing in countries which in this regard, have positions that are sometimes quite different from our own.

- With regard to “IT security” there are numerous regulations which may be of interest: industry standards (for instance insurance, banking) and regulations relating to the relationship with the public administration (the impact of certain provisions included in the CAD).

  These regulations may impose backup and recovery procedures, appropriate minimum security measures, security obligations and other similar aspects.

  With regard to security measures, we must highlight the importance of always being up to date on the “suitability” level, which is constantly changing. In this sense, it is useful to observe the behaviour of other individuals belonging to the same sector, to identify which measures are systematically adopted (and, therefore, presumably, appropriate), which will be introduced on an experimental or innovative level, and which measures are suggested by the Provisions of the Italian Antitrust Authority (for example the provision of the Italian Antitrust Authority “Measures and precautions required by holders of treatment with electronic instruments in relation to the functions of system administrator” of 27 November 2008).

Finally, the attention of the Information Security Manager must include observance of regulatory developments which, while not yet mandatory, will be so in the near future.

The European Regulation on data protection, to be adopted in the near future, introduces or clarifies certain concepts that should be implemented in companies in the short term, the introduction of which should not surprise those who work in this area, including:

- privacy by design;
- privacy impact assessment;
- security obligations;
- economic sanctions.

In particular, with regard to the concept of privacy by design, from the moment systems are designed, they should:

- avoid handling information which is not relevant;
- protect information that is legitimately processed.

This concept of privacy by design will include not only the protection of personal data, but also the many needs of the company represented by reasons of security, the pursuit of business goals and staff management. The needs of the company have a natural propensity to indiscriminate control or a massive collection of information in the interests of the employer.

Lastly, it is fair to point out that “the observance of regulatory developments” should not extend to observing developments related to privacy regulations still pending approval.

Each of the mentioned areas should be monitored.

For example, in the field of the Italian Administrative Liability of entities (regulated by Italian Legislative Decree no. 231 of 2001), the recent introduction of the offence of private sector corruption was long overdue and was to be implemented also in Italy with the Framework Decision 2003/568/GAI of the Council of 22 July 2003.

5.3 Factors contributing to Information Security

The protection of company assets and resources cannot be achieved only through IT security products or solutions. It is therefore worth asking the question: what are the other factors that play a more or less important role in the Information Security Manager's achievement of security objectives?

It is essential that these objectives are all known and that none are neglected: these are precisely the areas in which, directly or indirectly, the Information Security Manager will need to operate in a balanced and coordinated manner.

The following chapters will discuss the various issues in more detail: these are mentioned here in order to give a simplified and schematic overview[2], to highlight that these factors operate together[3]. Recent studies and analyses confirm this, and show that in terms of security, the best results with the least cost (maximum efficiency of Security!) are obtained by operating in a coordinated and organic manner.

5.3.1 Principles and Policy

The Principles provide the basis for the actions of the Information Security Manager and define the protection objectives for the company at a high level. Among the principles there is the mission of the organisation function presided over by the Information Security Manager, the standards to which the company intends to be guided in defining the Information Security Management System and the areas of security intervention in order to:

1. Support the company business;
2. Protect the company business;
3. Promote responsible behaviour.

The principles are translated into practice by defining regulations and implementing standards and policies which, in addition to guiding behaviour, are also the vehicle that communicates the governing objectives and values of the company both internally and externally.

It is essential that Policies should be simple, clear and above all shared amongst the different representatives of ICT services in the company; for example, it is to be stressed how principles inspired to “Support” and to “Protect” the business of the company, may lead to conflicting business decisions (for example, when “Protecting”, it is often easier to prevent the use of unsafe services even if these are potentially profitable for the business). The involvement of the senior management of the organisation in defining Policies will also help the Information Security Manager in directing his/her actions towards the objectives for which he/she has received full consent.

It is the task of the Information Security Manager to check that the Policies cover all areas under his/her responsibility, and that for each policy the following are clearly defined:

- Scope of applicability;
- Objectives (the Principles!);
- Responsibility for preparing and updating;
- Distribution lists.

[2] Source ISACA: COBIT5 for Information Security (June 2012)

[3] We use the term “holistic” approach according to a theory for which the body constitutes an organised whole and not simply the sum of its parts.

Many companies tend to consider the definition of policies a mere formality, often because the policies need to be of a general nature and resort simply to the transposing of regulation models defined by international standards or other more or less authoritative sources. The policies, on the other hand, constitute a means of address which is much more useful to the Information Security Manager as they will be contextualized and therefore, discussed, criticized, shared, and modified by the management, and compared to the reality in which they will be applied.

5.3.2 Processes

Security Processes are aimed at defining a set of interrelated activities, aimed at achieving the goals set by company policy.

Operating according to a structure of processes will help the Information Security Manager to understand exactly his/her responsibilities and what he should expect from others, to measure results obtained in order to identify possible improvements (for example, by the plan-do-check-act approach illustrated in §6.1) and to motivate and justify choices made.

Within the Security function of the company, it is possible to identify two macro categories of processes which have different responsibilities, roles and skills:

- Governing Processes (Governance) aimed at defining the Principles, Policies and Processes and monitoring of results.
- Management Processes (Management) aimed at the planning, implementation, delivery and monitoring of activities related to IT security.

To know more, it is possible to refer to a Reference Framework providing a list of all the processes of IT Security and their connections, roles, etc.. These are authoritative Frameworks which can be freely downloaded from the Internet (ref.§6.5).

Business processes that aim to achieve the company's mission will be of greater interest to the Information Security Manager. The purpose of the Information Security Manager is to identify, together with the references of the above processes, the best ways to integrate with security, a “sustainable security”, which is both a guarantee of protection, but also adaptable to business needs. The resulting dialectic from this approach is not always conflict free, as there will be many cases in which the objectives of the references and the Information Security Manager will be different, but sharing the Principles and Policies described above will constitute the starting element to which the parties must refer in order to settle the differences.

5.3.3 Organisational structures

Within the organisational structure, the hierarchy of responsibilities relating to the processes is defined, responsibilities which contribute in varying degrees to the achievement of business objectives.

The Information Security Manager will almost certainly not be able to operate on the organisation chart of the company. However, knowing how the roles and responsibilities are defined will allow an understanding of how security can be made more pervasive in the various areas of the organisation.

In particular, the Information Security Manager may, for example, support a review of security responsibilities within various structures, in line with the integration of security in the context of business processes. The review of the distribution between operational and governing roles of security is particularly significant. This is often the subject of conflicting situations between those who manage the systems, infrastructure and the network, in relation to the function of company security. For example: Who is responsible for managing the firewall, and who defines its rules?

There is no best answer to questions of this nature. The authors of this document do of course have an opinion supported by experience and by industry standards, but this is not discussed here. The best suggestion is to define a management model which is consistent with the existing cooperative and efficient organisation and within which each structure has the appropriate know-how and sufficient skills to effectively carry out the tasks assigned ... including those for security!

5.3.4 Culture, ethics and conduct

This is one of the areas in which it is possible to measure the actual level of a company's attention to issues of security, from management to staff who carry out more operational activities.

First of all, this attention should be paid to regulatory compliance, whether relating to the protection of personal data ex Italian Leg. Decree 196 / 03, or of a more general nature such as the aforementioned (section 5.2) Italian Leg. Decree 231 / 01: this regulation can give a strong impetus to the definition of rules and information security, by means of:

- the definition of a Code of Ethics. Regardless of content, this activity is an important moment of sharing between the senior management of the organisation, with broad implications for increasing awareness and understanding of the security issues which are of greatest impact for the company;
- the revision of the organisational model, to establish the necessary monitoring bodies;
- the implementation of security measures, including measures of a technical, prevention and controlling nature.

Regardless of the level of involvement of the Information Security Manager in implementing these activities, as well as the level of maturity of compliance achieved at the time the Manager is appointed, the Italian law on “Administrative Liability” is a strong driving force behind the establishment of Principles and Policy for the protection of information assets.

In terms of “conduct”, it is necessary that the company defines a set of rules within which the staff can carry out their activities in full compliance with security criteria, consciously and without ambiguity. If the behaviour is negative, the contribution given by the Information Security Manager will be essential. Whatever the criteria, each employee of the company must have a clear understanding of the behaviour that can cause damage (but for which a degree of responsibility can be taken), and which types of behaviour cannot be adopted as they would violate the Policies established by the company itself, or because, quite simply, they do not comply with regulations. Clarity of this nature should allow each employee to carry out his/her assignment in the full knowledge that they are acting “correctly”, even when in terms of compliance with regulations and policies it may seem that they are in contrast with the needs of business.

For his/her part, the Information Security Manager should pay close attention to how regulations are perceived within the company. If security is too often seen as an obstacle to business, it may be appropriate to provide support for choosing solutions in accordance with regulations that do not hamper the competitiveness of the company; in more extreme cases, the Information Security Manager must evaluate whether it is appropriate for this set of rules to be reviewed.

Finally, the cultural aspect plays a crucial role in this process; firstly, because it will be easier for the Information Security Manager to interact with colleagues in other corporate structures where there is a greater awareness of information risk. But in more general terms because it will be easier to ensure compliance with the rules of the Policies and therefore Principles in a context where the staff is aware of the importance of the individual contribution to the security of the entire company, as well as the potentially negative effects of breaching one rule rather than another.

5.3.5 Information

Regardless of how relevant the ICT sector may be to the business of the company, it is now common knowledge that in the absence of IT system support, no company is able to support the business in an appropriate manner in the Internet age. The company may well produce goods, but will it be able to sell them? Or, will it be able to manage shipments or store the raw materials?

Information therefore has an essential value in any production environment, although it may vary in close relation to the time beyond which the unavailability of the information system becomes a critical event.

Even in these cases, it must be remembered that the secrecy of some of the information handled is of a critical nature, such as an innovation in the production process, the design of a component, and the list of customers.

All this shows how the contribution of the Information Security Manager is crucial to the business, and this is why information constitutes the main asset of any security strategy.

The Information Security Manager must remember that information is not only the subject of security, but is also an enabling factor. To operate effectively, the following information must be known:

- the scope to be protected and security objectives;
- budget available;
- expectations and agreements relating to Levels of Service;
- threats and vulnerability;
- incidents and problems;
- etc.

More generally, the Information Security Manager carries out his activities in a context governed by other actors: the management of operating systems, the network, development of services, etc. It is important that different ways of sharing information are established with these organisational structures, enabling the manager to be give the necessary support and simultaneously fulfil their duty to ensure the protection of company assets.

5.3.6 Services, infrastructures and applications

Technology at last! But as you can see, almost at the end!

We have nothing against technology, but we believe it is important to consider other factors that need to be taken into account because the Information Security Managers, often coming from a technology-related background, tend to place too much focus on this aspect. Furthermore, this is the area with the majority of products, and therefore suppliers understandably tend to focus on it too.

As for the factors described above, also in terms of technology we have to make a distinction between the technical solutions for security and the IT technology which is to be made and kept secure.

The former are the set of tools which the Information Security Manager uses to prevent, detect, manage and resolve security threats on a strictly technical level, even if he/she does not adopt solutions to support the security management processes themselves. In general, it is the responsibility of the Information Security Manager to establish how these tools should be configured and what kind of measures or functionality will be provided, as well as constantly monitoring the implementation of these decisions. It is easy to understand how the availability of numerous support tools may be not only an advantage but also a cost to be considered, as the company avails itself of the increasingly numerous and sophisticated instruments.

The task of the Information Security Manager is more complex in relation to services, infrastructure and the applications which, by the nature of the assigned mission, he/she has to help protect. It is essential to remember that security is (and should be), by definition, pervasive, and so the Manager will face problems related to very different technologies, tools and solutions according to the case in hand. It is important and necessary to intensify cooperation with the staff of the company dedicated to services which are to be protected, cooperating to identify on a case-by-case basis the solutions best suited to the security objectives to be achieved. The ability to detach oneself from the technological element can prove categorical if the Information Security Manager has to support the company on issues over which very often he/she will not have complete mastery.

5.3.7 People, skills and competences

The organisational structures introduce the human element - every organised structure has its own culture of information security. On a superficial level, the reader may be tempted to give little importance to this factor, but on the contrary, most of the longer-lasting and relevant results will depend on how the Information Security Manager works in this area.

Experience has shown that the human factor undoubtedly lies at the base of the problems, but nevertheless CAN be decisive in achieving the objectives of the company. In the opinion of the authors of this book, the Information Security Manager must focus primarily on this second aspect. But how?

Supported to a greater or lesser extent, training and awareness on security (ref. §6.6) may provide results not only in terms of increased awareness, but also motivation. This is difficult if staff is insensitive when faced with risks which may threaten their productivity, their results or the competitiveness of the company! Obviously the focus of the training is essential. There is no point talking to our colleagues about the risks of media attacks by hacktivists if our company is a leader in the field of fabric originating from eco-friendly materials, probably more palatable to the silent theft of patents by industrial espionage professionals.

Ensuring the participation of colleagues in the process of security is therefore essential, as much as is understanding the issues for which effort or changes are required in relation to the common working practices, in order to implement new protection measures. In fact, it is difficult to effectively maintain the technical measures on which we usually rely without a cooperative approach on the part of the people involved in the implementation of business processes!

That is why training, on a par with internal communication and sharing in general, should allow information on the Principles, the Policies (yes, even them!) to be shared together with the operating rules that must be followed.

Finally we can talk about the “executors”. Managing the role in information security means working in a complex and constantly evolving context. The work of the Information Security Manager and his/her specific department requires extensive expertise which must be consolidated and continuously updated. Perhaps more than other disciplines, IT security requires the right people in the right place!

6. THE FIRST 100 DAYS OF THE INFORMATION SECURITY MANAGER

6.1 Methodological approach

6.1.1 Objectives

The objective of guaranteeing an adequate level of information protection, in line with the expectations of Senior Management and the company mission, necessarily implies the adoption and upkeep of an Information Security Management System (ISMS), built up through an ongoing and long-term process of improvement.

In this sense, it is easy to realise that in the first 100 days, the Information Security Manager, while having the essential goal of setting objectives to be pursued and outlining a strategy, can initiate and address only part of all the required actions for improvement, making plans that these achieve results in the short term, while others can only be guaranteed in the medium to long term.

However, the key elements remains those tasks (so-called *quickwin*) that can achieve quick results, enabling the Information Security Manager to measure the effectiveness of his/her actions and highlight the validity of the choices made.

On the other hand, in order to define objectives and strategies, the Information Security Manager needs to quickly establish and get to know the setting, the main problems and most effective methods for solving these within the company, none of which are easily identifiable at the time of appointment.

A methodological approach is therefore needed, to enable the Information Security Manager to acquire this information and hence decide on the actions to start up, despite the initial gap in knowledge.

6.1.2 The PDCA model

The PDCA model is an efficient reference when defining an approach to deal with issues in a comprehensive manner. Better known as the "*Deming model*", taken from the name of its inventor W.E.Deming (1900 - 1993), this was proposed as a theory in the '50s originally in Japan, then spread to the United States and subsequently to the rest of the world.

According to Deming, organisations need to establish collaborative relations both with clients and suppliers, with the aim of continually improving the service offered and minimise errors and failures, through an continuous cycle of improvement. Any process can thus be seen as a cycle with four basic stages:

- Plan (design, plan);
- Do (act, produce);
- Check (control);
- Act (establish or correct and restart the cycle of intervention).

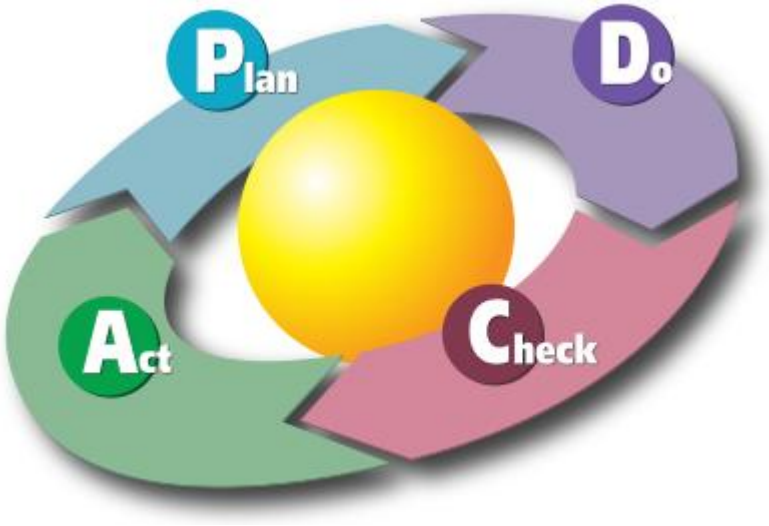


Figure 7 Diagram of the PDCA model - Wikipedia

Here it should be underlined that the concept of continuous improvement that lies at the base of this model implies that the four stages of the PDCA cycle should be continuously and constantly repeated. This also applies in the case where, at the end of any cycle, the planned objectives have been reached, as the initial context and "surrounding" conditions (company objectives and context, binding terms, market conditions, technological evolution etc.) constantly change over time.

In fact on each iteration, the model offers the following advantages:

- A clearer definition of the roles, tasks and responsibilities within the Organisation;
- Identification of personal weaknesses and the introduction of suitable corrective action;
- A reduction in costs, claims and disputes;
- The introduction of a tool for organisational improvement and optimisation of results;
- Adaptation to changes in the general setting.

6.1.3 The PDCA model applied to the Information Security Management System

The PDCA model, as described above, is ideal in the Information Security Management Systems and to address general effective action for security governance, above all in those settings where levels of maturity are still limited.

However, the application of an approach based on the cycle to obtain optimal results needs to present suitable elements for contextualisation.

In the first place, it is necessary to understand how an approach based on the PDCA cycle to address the first tasks of the Information Security Manager must not be seen as the implementation of one single large cycle. In fact this idea would not make sense, and may even prove counter-productive, as on the introduction of new managerial roles within a company, the senior management expects immediate results.

The tasks that must initially be performed by the Information Security Manager will in fact vary (ranging, for example, from the set-up of organisational elements, which may also require various inter-departmental stages, to addressing technological aspects on the systems), and may require significantly different timescales for implementation. Therefore, to reason in terms of a single large cycle may lead to an exaggeration of implementation times with respect to those expected. It is more rational to adopt an approach assuming several "parallel" cycles, in which each type of task can be performed within its own process of improvement according to the Deming model until the relative objectives are fulfilled.

As an analogy, simply imagine the series of tasks required of the Information Security Manager as a set of gears, where in order to start all elements at the same time, each specific gear has a specific period of completion.

Figure 8 Gear set representing a set of processes

Thus the gears that work on the "highest" level (definition of objectives, organisation, etc.) are preliminary to the more timely gears, but also generally envisage cycles that last longer, as their effects are felt by and interact with many existing elements of the company. It is therefore critical to ensure that the senior management understands that the results expected from these elements remain in the medium to long term.

On the contrary, the gears working at the "lower" level, addressing more specific elements (for example regarding the configuration of perimeter protection equipment or the management of specific technical issues) can be useful to obtain immediate results, which highlight the goodwill of the ISMS approach.

Obviously these gears must necessarily interact, given that the completion of one also depends on the information obtained from the results achieved by the others.

Other aspects of the context to be considered by the Information Security Manager when defining the PDCA cycle include:

- the definition of concrete and measurable objectives of initiatives within individual PDCA cycles;
- programming and planning of moments of synchronisation between the cycles on different levels (the size of the gear teeth);
- definition of the methods of verifying and measuring results achieved in the various iterations of the PDCA cycles on various levels;
- the choice of significant information to be used to define objectives for improvement at the end of individual iterations.

The parallel actions of these various cycles that need to be defined and managed by the Information Security Manager can briefly be summarised in an approach that considers short term actions (tactical approach) and those in the medium to long term (strategic approach).

6.1.3.1 Tactical approach

The action of the Information Security Manager should always aimed at the accurate implementation of risk assessment initiatives, aimed at the prompt identification of the most critical areas and the definition of security initiatives that should be adopted as priority measures.

However, an approach based on an in-depth risk assessment may involve a time frame that is simply not compatible with the period of 100 days considered here, with the need of providing management with tangible results.

Therefore other factors to be taken into account for the definition of the various cycles may include:

- the identification of recurrent and/or significant incidents occurring in the latest period within the business setting;
- needs expressed by the senior management;
- aspects related to business tasks performed by company departments containing the most important data;
- studies on aspects of security and compliance for specific sectors;
- the sharing of benchmarks and experiences with subjects outside the company;
- the use of sector standards and best practices.

With regard the last point, the Information Security Manager may be able to identify some security baselines in sector standards or best practices, i.e. a set of checks/requirements to use as a comparative model with the organisational, procedural and technical security measures envisaged or to be foreseen at the specific company.

The baseline should be selected from those available on the basis of the following criteria:

- it must contain security checks that are uniform from a point of view of strength of the measures proposed;
- it must contain security checks in the procedural, organisational and technological areas, in order to withstand an effective check on site of security status.

In particular,

- in each area, the baseline must envisage checks on the contents of policies, processes, procedures and technical measures;
- the checks should be sufficiently granular. For example, this means that in a specific security area (e.g. authentication measures) separate checks will be available for the quality of passwords with respect to the criteria for changing the passwords themselves. In the event of non-conformities, this will enable quick identification of the type of problem found.

The Information Security Manager, after defining a baseline, must then verify completeness with regard to his/her company as well as the observance of conformity requirements established in applicable standards. In fact it must not be forgotten that the standards and security baselines available on an international level do not generally take into account the specific aspects of laws in individual countries.

Once the baseline is complete, the Information Security Manager can start an assessment (“gap analysis”) on the defined perimeter of the company, using the baseline check list. The perimeter may coincide with the entire dimension of the company, or may be limited to areas deemed priority zones according to the business performed.

The “gap” may be reduced, identifying less significant non-conformities with respect to the company's security objectives. All checks excluded from this preliminary selection will constitute the essential information for the start-up of the Plan phase of the first iteration in the security PDCA, in other words the objectives to be reached within the area of the lower level “gears”.

6.1.3.2 Long-term strategic approach

The tactical approach outlined above will meet the short-term needs and enable the correction of immediate problems. On the other hand, the use of a security baseline also enables the uniform application of minimum or reasonable security measures on a set company perimeter, but it does now also allow for the identification of initiatives that may have a high impact/effect or which derive from specific aspects of the company itself. To implement this level of initiatives, the Information Security Manager will need different tools, such as the approach based on the correct management of risks cited above. In this scenario, two types of medium- to long-term intervention can be identified:

- "structural" measures for the implementation of the Information Security Management System (ISMS);
- security measures dependent on the risk level in the context.

The first depend only in part on the results of the risk assessment, in other words on an evaluation of the relevance of the intervention, the effort that can be dedicated and the means of implementation. However, this document does not discuss the importance of these measures and the fact that they will be included in the company processes/services/technologies. Examples of these measures include:

- the integration of security measures within the life cycle of the software and services;
- audit procedures;
- the risk assessment itself;
- incident management;
- the adoption of measures for specific security solutions (such as network perimeter protection systems) and relative management processes.

The second type encompasses security initiatives depending directly on the context, which is more complex to identify and assess. For this reason, the choice of these needs to be backed up by a rationale based on risk management.

Examples include:

- the choice of reactive security solutions, such as the adoption of automated tools for Incident Management (e.g. SIEM systems), Disaster Recovery and Business Continuity;
- the definition of policies and models for security management normally burdensome or impacting the organisational structure (for example, the segregation of duties), processes (e.g. certification of the ISMS according to standards such as ISO 27001) and technological instruments (such as the segregation of group administration accounts: root, administrator, dba, etc.);
- the choice of security solutions and tools that address new technological trends and threats (e.g. mobile device management).

6.2 Establishing the conditions of entering the company and knowledge of the business

A newly appointed manager may be taken on with skills in ICT security (after being selected by another company to fill this post) or, though not an expert in the sector, may have an in-depth knowledge of the company, the people and its processes (already an employee in the same company).

The two scenarios involve two very different approaches in the first 100 days.

However, in both cases it is important to have a clear understanding of why the company has decided to invest human and financial resources in this role, and thus to understand "*why they have decided to create this role, and why they have specifically chosen me*".

There can be a host of very different reasons; obligations related to standards, the results of an audit in the regulated markets, a recently enhanced sensitivity of the company to security, the impression on senior management of some security disaster that happened to others, published in the press, or the effective involvement of the company in an IT incident.

The Information Security Manager must be familiar with all these aspects and must understand how much spending power and/or influence on expenditure he/she actually has or can have in the future, to be able to draw up a plan of action and establish some reasonable expectations for the management team.

If the Manager is already an expert in this area, he/she should prioritise improving his/her knowledge of the organisation, identifying the authorities and persons that most need his/her help, and establish solid relations with these where possible. This could be achieved for example, through a win-win strategy where as well as doing good for the company, both stakeholders benefit from intervention in security.

In this regard, the Manager must always take into account that the "weight" security must be justified, not only with an improvement to this issue itself, but also through the identification of aspects for improvement as part of the enterprise objectives of the stakeholders concerned: greater operating continuity, increased ability in IT governance, enabling technologies for the Cloud, the use of mobile devices, social networks, etc.

A useful recommendation in these cases is to create both formal and informal moments for liaising not only with the manager's direct staff but also with the remaining personnel/stakeholders. The organisational structures of various companies can differ greatly, but for simplicity's sake we can say that the Manager, within his/her own scope of competence, should first of all interact with those in the company who deal with the following areas:

- IT Operations: those responsible for the operation of the telecommunications infrastructure and the server rooms managing the application servers and databases, as well as the personnel work stations and support equipment (e.g. printers, etc.), with whom the Manager should continuously interact to ensure an adequate level of security of the infrastructures.
- Application development: those who manage maintenance, production and development of application systems in line with the business needs of the company, with whom security personnel should maintain reciprocal and frequent relations to ensure the integrity, confidentiality and availability of company information managed on these systems.
- Legal: those who deal with legal conformity of the company, which normally do not have Information Technology skills, but who are familiar with the various laws and regulations to be observed by the company (such as Italian Leg. Decree 196/03 on Privacy, Italian Leg. Decree 231/01 on the Administrative Liability of Companies, Italian Law 262/05 on the Protection of Savings, etc.) with whom it is not expected to achieve the synergy and improvements envisaged (for example, in the definition/analysis of security clauses in contracts with suppliers and clients).

- Risk management and information protection: those who deal with assessing and addressing the main business and potentially IT risks in important assets of the company, and with whom cooperation is fundamental.
- Audit: those dealing with audit and inspection procedures within the business and IT processes, with whom it is useful to share critical information arising from inspections, as well as the relevant plans of action.

The Information Security Manager should also interface with those dealing with business issues, and those providing support to business activities in the company, such as

- Commercial and Sales departments: for the protection of information stored in client management systems (CMS), one of the most important company assets;
- Research and Development departments: for the protection of projects and research results;
- Production areas: for the analysis of aspects of system availability and aspects of protecting information associated with the company production cycle;
- Marketing: for example in the case of all activities that envisage company presence on the web and in social networks (a case requiring an additional contribution from the Community);
- Administration and Finance: for an understanding and comparison of the economic aspects of risks and security;
- Human Resources: for the definition of resource selection criteria, courses and methods for raising awareness of IT security, and for the protection of information on employed personnel.

Another important role is also played by the presence of possible outsourcers who support the company in the completion of business processes and the provision of IT services (such as the outsourcing of the data centre and application management on certain systems), with whom the Information Security Manager inevitably has to liaise to evaluate possible security risks underlying the outsourcing relations and to define the most appropriate protection measures.

Further on in this document, some information will be provided on how to conduct an assessment of the current situation, with a description of some of the best practices and security measures to be evaluated and implemented in relation to the business context.

6.3 Analysing the current situation and drafting a plan of action

Regardless of the company motives and past professional experience that led to the appointment, the first objective of the Information Security Manager to be addressed is establishing the current state of company security.

Only a concise but clear and comprehensive overview of the current security situation can in fact provide the elements necessary for drafting a short-term sustainable strategy in line with the business objectives, with the industrial plan and expectations of the management (which is no small feat).

It is therefore necessary to give absolute priority to the drawing up of a plan, aimed at retrieving all information required to ascertain the “state of health” of company security and consequently to identify and plan any corrective actions that may be needed.

Given the time available, this investigation cannot and must not go into excessive detail, but should be limited to acquiring the essential information needed to understand whether, how and by whom organisational, procedural and technological solutions are managed, according to their relevant impact on ensuring company information security.

To reach the results outlined above, a working approach is typically approached through the following five planning phases:

Figure 9 Approach phases

A further description of the activities to be performed in each phase is provided further below in this document.

6.3.1 Quick Assessment

The objectives of a quick assessment consist in obtaining a clear illustration of the company maturity with respect to factors that contribute to effective security management and the identification of protection measures currently adopted. This assessment should be carried out with the awareness that Information Security does not only depend on technical elements and technological solutions, but also, if not above all, on organisational and procedural aspects.

The main difficulties that generally arise when conducting a quick assessment are the identification of elements to be analysed, the methods of conducting this investigation and the organisation and use of the gathered information to ensure their utility in subsequent activities.

Elements for analysis

In line with what has been outlined previously in this document, we maintain that the macro areas for analysis should coincide with the factors contributing to the effective management of security, as illustrated in paragraph 5.1, in other words:

- principles and policies;
- processes;
- organisational structures;
- culture, ethics and conduct;
- information;
- services, infrastructures and applications;
- people, skills and competences.

Methods of conducting the analysis

With regard to how to make this assessment, it is recommended first of all to retrieve and consult all documentation available in the company (policies, procedures, organisational and technological solutions, etc.) in order to start acquiring, autonomously, as much information as possible on the current situation. Meetings should then be planned to address “dark” areas and more details relevant to the case in hand, with the reference personnel involved in security management. These meetings could be to a certain extent formal, according to the degree of organisational complexity.

The next task will then necessarily be to identify the various roles and reference personnel to be interviewed, with the compilation, purely for work convenience, of a matrix representing the mapping of environment-department-reference-role similar to that illustrated below, in which the point where the Environment line intercepts the column stating the Position involved (HR, ICT, etc.) the name of the reference and his/her position should be noted. The following table shows a theoretical structure of this type.

Environment	Area of intervention	HR	ICT	Operating lines	Sales	Security
Principles and policies	Point 1					
	Point 2					
Processes	Point 3					
	Point 4					
Organisational structures	Point 5					
	Point 6					
Culture, ethics and conduct	Point 7					
	Point 8					
Information	Point 9					
	Point 10					
Services, infrastructures and applications	Point 11					
	Point 12					
People, skills and competences	Point 13					
	Point …					

Table 1 Matrix of relations between elements and departments to involve

Once the documentation available has been analysed, identifying the referees, it is important to then start the prompt acquisition and examination of information through a series of work meetings (max. 3-4 participants) to discuss results. This task could be completed, depending on the size and complexity of the company, within a time span of 2 to 4 weeks.

Organisation of information

Lastly, with regard to how the information is collected and organised, for subsequent analysis, a questionnaire would be the ideal means to deal with and organise the most relevant aspects of each area of investigation, and their relative links with one another. This will then enable an analysis of the various aspects, which can be conceptually grouped into seven factors contributing to information security and for example detailed according to the following hypothesis:

Environment	Object of assessment	Result
Principles and policies	• Presence of a document addressing information security • Existence and structure of elements governing aspects of information security • Collection and mapping of standards and requirements necessary for the various business processes • Analysis of privacy aspects in the various company processes and information systems • List of data handling processes and distribution of tasks and responsibilities • Methods of executing and tracing audit inspections • Definition of confidentiality agreements	

Environment	Object of assessment	Result
Processes	• Check of level of definition and formalisation of processes for managing aspects of information security 1. Manager 2. Working referee 3. Company structures involved 4. Level of company risk (high, medium, low, zero) 5. Type of data handled (sensitive data, client's financial data, personnel data, etc.) 6. Databases used (with location on the servers) 7. Applications used 8. Relationships with other company processes 9. Requirements and/or presence of any standards and/or certification 10. Any dependency on external suppliers • Inspection of the same elements also for the existing main business processes in relation to the definition and formalisation of their main aspects	
Organisational structures	• Definition of roles and responsibilities (with potential checks on formal aspects) • Verification of formal designations of information security responsibilities	
Culture, ethics and conduct	• Presence of a company code of conduct • Typical conduct with regard to security 1. Is attention paid to security issues in daily company practices? 2. Do personnel observe the policies and principles of security? 3. Are personnel in possession of sufficient information and are they encouraged to adopt conduct in line with this information? 4. Is each member of personnel made responsible with regard to the protection of company information? 5. Do managers take care to identify and respond to requests received? 6. Does the management proactively support and pre-empt any new demands, with due notification to the company? 7. How does the company respond to these demands? 8. Does the management establish frequent collaboration between company structures for the development of security policies? 9. Does the executive management fully perceive the value of business security? • The presence of operating procedures guiding the activities of personnel (e.g. ISO 9000) • The need for and/or presence of standards and/or certification that define procedures and codes of conduct • Methods of communication with personnel (notice boards, circulars, emails, etc.)	
Information	• List of accesses to the information system (e.g. only company LAN, the Internet, VPN, extranet, etc.) • List of equipment for protection of company accesses (e.g. Firewall, proxy, VPN, etc.…) • Network topology (Segregation of AdS, VLAN, etc.…) • List of network devices and their location • List of servers with their matrix of use with the processes • End Point Security tools • Data protection systems (e.g. DAM) • Anti-intrusion systems • Presence in the company of an IAM and/or Role Management system • User authentication methods (login and password, strong authentication, OTP, single sign on, etc.) • Criteria and means to guarantee integrity and availability of data (redundancy of servers, back-up, disaster recovery, etc.). • Tools for the definition of security policies for Servers, Networks, end points, mobile devices (tablets, smartphones, etc.…)	

Environment	Object of assessment	Result
	• Methods of managing removable media (Management of removable media, issues of media for Information handling procedures etc.) • Rules for managing the life cycle of deeds and hard copy documentation (production, reproduction, archiving, disposal etc.) • Methods of exchanging information (Policies and procedures for the exchange of information, inter-exchange agreements, security of media transport, security of electronic messaging, business information systems, etc.)	
Services, infrastructures and applications	**Assets** • Inventory • Table of correspondence with identified company processes	
	Physical and environmental security • Methods of protecting company rooms (armoured doors, barred windows, etc.) • Methods of access to company rooms (door with badge entry, receptionists, etc.) • Methods of access to specific areas by personnel (e.g. CED) • Methods of access by external personnel to company areas (e.g. escort badge, escort, registration of general data and/or documents, etc.) • Layout of equipment and related protection • Security of wiring • Equipment maintenance • Security of equipment off site • Decommissioning or safe re-use of equipment	
	Continuity management • Collection and mapping of standards and requirements necessary for the various business processes • Risk assessment	
	Monitoring and audit procedures • Presence of a log system and relative protection • Presence of an analysis system and correlation of events • Presence of a system for monitoring system use • Log protection • Separation of administrator and operator logs • Fault log	
Control and improvement system	**Security incident management** • Presence of security incident management procedures (logical and physical) • Presence of a company database storing security incidents	
People, skills and competences	• Degree of knowledge of personnel on security issues • Presence of personnel training interventions on security and privacy issues	

Table 2 Potential contents of the quick assessment

Useful advice in defining the questionnaire may be found in the “Key Questions” of the “Essential Actions” described in detail in the chapters below (§6.4).

6.3.2 Analysing results

This phase aims at identifying, on the basis of information acquired through the quick assessment, the current situation, highlighting the critical areas as well as identifying and prioritising the interventions to be implemented in order to deal with the failures found.

The attribution of priorities to the interventions is a key factor in the entire process.

Any error in assigning a priority will spread over the subsequent activities, risking the consequent definition of a plan of action not completely in line with the situation found, generating a false sense of security within the company and exposing the workforce to expensive and embarrassing repercussions. Therefore the definition of clean and applicable criteria for assignment is essential. For the exclusive purpose of an example, and in no way detailed, priorities can be attributed according to the importance of the area of intervention, in terms of:

- priority for the business department;
- related company risks;
- constraints of standards;
- necessity of immediate solutions.

It should be highlighted that the criteria and priorities are not set in stone, and as such should be reviewed periodically and amended where deemed necessary when new or sudden events arise, such as a security incident or the issue of a new standard, to avoid the risks outlined above.

From a methodological point of view, it is recommended to conduct the analysis on all areas of the questionnaire (environments) in which critical aspects have been found, assigning a priority class to each of these, e.g. High (H), Medium (M), or Low (L), based on the established criteria and noting the results in a table similar to the version below, where the listed criteria are shown as an example.

Subject	Area of intervention	Priority for the business	Company risks	Constraint of applicable standards	Need for immediate solution
Principles and policies	Area of intervention 1	L	L	**H**	**H**
	Area of intervention 2	M	L	L	M
Processes	Area of intervention 3	**H**	L	L	M
	Area of intervention 4	**H**	M	L	L
Organisational structures	Area of intervention 5	M	**H**	M	M
	Area of intervention 6	L	**H**	M	**H**
Culture, ethics and conduct	Area of intervention 7	L	**H**	M	M
	Area of intervention 8	M	**H**	L	M
Information	Area of intervention 9	M	L	**H**	M
	Area of intervention 10	L	L	**H**	L
Services, infrastructures and applications	Area of intervention 11	**H**	**H**	M	L
	Area of intervention 12	**H**	**H**	M	M
People, skills and competences	Area of intervention 13	**H**	L	L	M
	Area of intervention 14	**H**	L	L	M

Table 3 Example of priority assignment

An analysis of this type of table provides an overview of the situation in hand and constitutes a valid working support for the subsequent phase of planning interventions (Remediation Plan), providing at the same time a clear understanding of the current situation and the problems that need to be dealt with in the future.

The identification of interventions required involves the preparation by the manager according to the methods outlined in the following chapters, of the “security baseline”, i.e. the set of checks/requirements originating from sector standards and best practices, which need to be put in place in the company in order to achieve the set security objectives.

In fact this baseline enables the manager to make a gap analysis, i.e. a comparison aimed at determining any gaps between the situations found in the quick assessment phase and that envisaged by the baseline itself, thus leading to the identification of any gaps in the selected interventions put in place to fulfil security objectives.

It is worth noting that gap can be reduced by implementing the relative check/requirements established by the baseline, but also through the definition of an acceptable level of residual risk, i.e. gaps that by their very nature, specific context or the presence of alternative checks, are not deemed relevant for the purposes of achieving the established security goals.

The phase of analysing results should last no longer than two weeks, depending on the complexity and size of the company, and should conclude with a list of the Remediation actions on which a feasibility study is required (next phase), which should naturally be placed within the scheme illustrated above (§Table 3).

6.3.2.1 Feasibility Study

Once the Remediation action list has been prepared, each single item needs to be weighted with a feasibility study aimed at determining, also only in terms of quality, the impact of the remediation actions in light of a series of fundamental constraints:

- **Orientation of senior management:** the management may have expressed, for the short-term future, a tendency more towards “make” interventions rather than “buy” approaches, i.e. preferring the use of working resources rather than making investments;
- **Skills:** in-house skills, even if in the first place evaluated as infinite capacity, are directly linked to training. The combination of these two elements may require a preliminary training session before that of remediation, and thus cause a shift in planning;
- **Budget:** the availability of a budget, both in terms of finance and resources, can be defined in more or less detail as required, thus setting appropriate constraints for the case in hand. In more structured companies, the budget can be allocated by project/year and in this case needs an evaluation with the managers of individual projects of the existence (or not) of the Security requirements to be met. In smaller organisations, the budget can be simply allocated by macro area, or even by expense item. In this case, negotiations and checks on residual availability should be carried out at various meetings, bearing in mind that revisions may be necessary to funds already shared and “promised” to business departments, or more simply may require a revision to priorities. This consideration applies to the financial component, but also to human resources. In fact a company policy may prevail, in which the company tends more to “make” interventions, having in-house skills that meet requirements, but already allocated to other projects.

Once the Information Security Manager has clearly identified the impact of the above constraints on the single remediation actions, he/she will be ready to draft a schedule of activities backed up by the relative rationale, to submit to the top roles for certification.

Previous sections have already described the top roles involved in ICT Security issues (§6.2), who then need to be consulted again for the phase of priority selection and definition. Ideally this would mean the identification, for each remediation task, of the body most at risk in the event of cancelling or re-scheduling an intervention, in order to request an evaluation of such actions.

The most effective methods is undoubtedly a meeting, where the list of activities is presented, with the following information:

- description of the activity;
- estimated time for implementation;
- internal resources required, even only on the level of team leaders, in the event of “make” solutions;
- the budget amount to be allocated, divided between capex and opex;
- feasibility, defined simply as YES/NO, on the basis of an analysis of the existing constraints;
- any hindering constraint (other priorities, lack of budget, lack of in-house skills, etc.).

6.3.3 Structuring lines of action

On completion of the quick assessment, the analysis of results and the feasibility study, the Information Security Manager will have identified the areas of intervention and activities necessary to improve overall levels of security in the company, establishing the effort required to implement these interventions, while the only remaining task is to draw up the list of things to do before the 100 days are over.

On the surface, this task could not seem to be simpler, but in practice, implementation is far from easy. Drafting of this list could in fact take a significant amount of time, considering not only the specific economic impact of each single intervention.

While on the one hand it is advised against pushing off with an initial plan of action that requires considerable investments for implementation, it is nevertheless fundamental that the plan addresses the main issues, known or perceived by top management, regardless of the type and entity of effort required (obviously within limits).

In fact it is important to take into account that the interventions decided upon will constitute the first package of security measures that the top management will need to evaluate and approve, thus representing your working “business card”, on which the future professional esteem and trust in your role as Manager within the company will be based.

The interventions to be implemented must be planned so that they lay the foundations for a programme of improvement in company information security in the medium to long term. In other words they should not only address technology but also organisational and procedural aspects of the latter, as well as work factors concerning the management of security within the company.

An essential task in the preparation of a plan of action in line with company objectives is the correct evaluation and consideration of aspects concerning the very nature of the company, such as:

- the market where it works: each industry has its own specific business, which in turn has its own specific security needs
- progress; the security strategy also has to take into account, if not above all, the availability of company resources; fewer resources means tending towards a strategy aimed at increasing efficiency of processes and security solutions already in place (while still dedicating resources to implement actions deemed more “urgent”). Vice versa, greater availability of resources enables the definition of a line of action aimed at consolidating and increasing efficiency, for example through investments in new technologies, and in security overall.
- Dimensions: the larger the company, the higher the number of internal positions, which to a greater or lesser extent perform (or must perform) security tasks, making management of these more complex.
- belonging to a group: guidelines, programmes, standards and solutions for security are generally defined by the head of the group, and all group companies are thus required to observe these, adopting suitably “localised” solutions, also in consideration of the Italian standards scenario.
- a culture in the area of security: the greater the awareness of security issues the more easy it will be to introduce organisational solutions and sophisticated technologies into the company. But at the start it will be more complex to identify the actions needed to increase efficiency and sustainability of security, and vice versa
- defining the priorities of the areas of intervention: as identified by the Information Security Manager during the phase of analysing results.

On the basis of these considerations, some criteria among those resulting from the feasibility study can be defined to enable the identification of actions not to be implemented, those to be implemented in the short term (presumably within the first 100 days of work) and those to be planned for implementation in the medium to long term.

The criteria for selecting and defining the priorities of interventions should enable the classification of the latter by categories, thereby simplifying the subsequent evaluation of the opportunities to implement these actions and within which time frames. Purely as an example, interventions could be classified in the following categories:

- *Quickwins*: this class refers to all actions that make a significant contribution to improving overall security and to be implemented in the short and/or very short term. This category also includes interventions classed as urgent
- *Complex but important*: this category represents the group of interventions that despite their complexity and/or significant quantity of resources needed for implementation, still need to be completed at the very least in the medium term
- *Nice to have*: these are interventions that by their nature are not fundamental in achieving security objectives but would contribute to an improved management of security
- *Simple but who cares*: as it says, this category includes interventions that are reasonably simple to implement and require a modest amount of resources, but at the same time are not in themselves of great interest to the company. This type of intervention is usually excluded from the implementation plan

This type of classification of interventions enables the drafting of a “magic quadrant” (see figure below) providing a graphic representation of the following:

- importance of the intervention for purposes of an effective system of managing information security (contribution to security)
- the period within which the intervention should ideally be implemented (normally in the short, medium or long term)
- an indication of the entity of resources that the company needs to make available to implement the intervention, illustrated by the size of the circle representing the i-th intervention (the greater the size, the more resources needed)

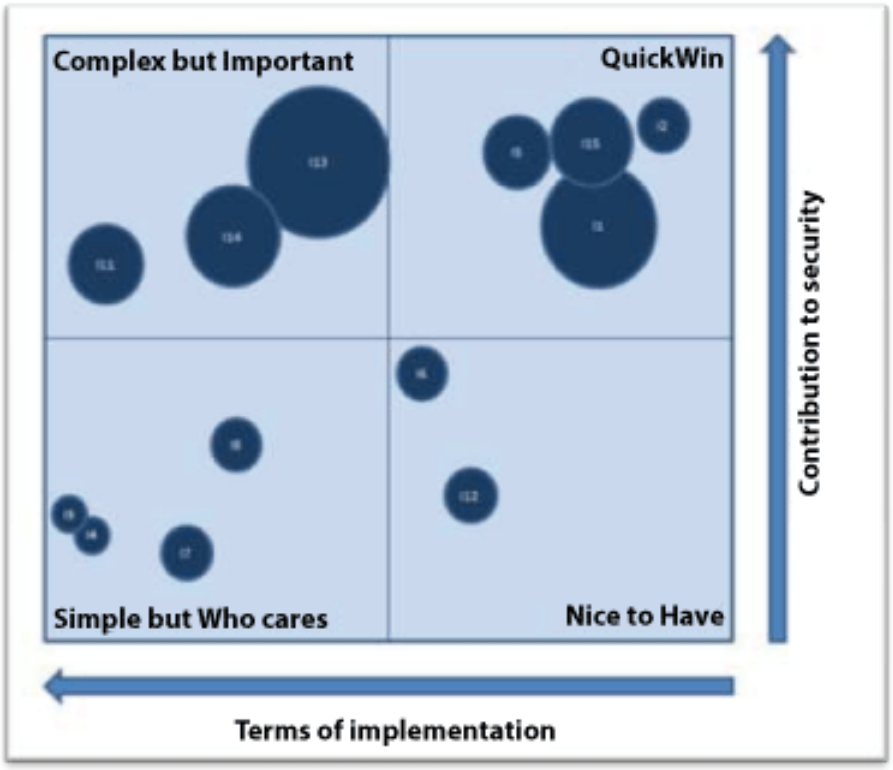


Figure 10 Quadrant classifying the intervention activities

A quadrant, together with the additional information obtained from activities conducted during the entire analysis phase, will put the security manager in a position to be able to draw up an operating plan for security, essentially based on the most objective possible rationale.

Here we should stress the importance of “planning” the various activities which comprise the operating plan so that not only the result is guaranteed, but that there is also, where applicable, optimisation of the resources used - a factor always in favour with the senior management.

6.3.4 Sharing

The last stage in this assessment is the presentation of the lines of action resulting from the project.

This is a fundamental opportunity for final approval of the results obtained with their contribution, in terms of time and content, to raise awareness of Security issues and encourage loyalty of the senior roles required for support during the implementation phase.

The presentation of these results should at the very least focus on the following aspects:

- Joint evaluation of the short, medium and long term

  The manager should send the set of actions envisaged in the plan, not as a Project but as a stable Process, in order to ensure the development and maintenance of a Security management system that is efficient, effective, documented and measurable.

- Comparison of mapped/planned interventions with evidence of deviations

  The Manager should highlight that the short-term plan envisages the prompt implementation of interventions mapped as necessary (due to budget, priority and resources), and that the medium and long term plans will then be implemented;

- Modifications to the code of conduct

  The Manager should stress how evolutions in the Plan require parallel evolutions in conduct within the company, achievable with the involvement of all company members and the planning of facilitator actions such as:

  - prompt communication of initiatives;
  - training aimed at the strengthening of awareness;
  - dissemination of clear and simple rules;
  - incentives and rewards, also visible if not financial, linked to achieving objectives;
  - collection of proposals for initiatives aimed at improving the entire Security Management System.

6.4 What to do: the current and essential issues

The previous chapters have highlighted the complexity of the context in which the Information Security Manager currently has to implement his/her role and assigned responsibilities.

Rapid developments in IT paradigms within a company environment, the emergency of new elements of a social and cultural nature in the use of technologies, the significant scope of the reference standards to be taken into account (both on a national and international level) and an increasing number of heterogeneous threats only go to show how specific elements can determine each specific business case in order to outline targeted strategies and protection solutions.

Therefore, while the head of a production company expanding business abroad may focus on the protection of critical data exposed to foreign partners (formulas, drawings and other secrets), the interest of a company with a strong on-line presence and trade on the Internet may above all aim at protecting its services from unknown hostile parties.

Given the intrinsic link with the evolution in business of individual companies, it is therefore impossible to establish priorities of the areas of security to monitor, also bearing in mind their number and the constraint of the 100-day time scale as considered in this document.

At the same time, to think of succeeding in equal measure across all areas is effectively a chimera, above all when adding in the factor of the current economic context in which resources are increasingly dwindling.

For all these reasons, the approach hypothesised above suggests an initial phase in which the specific initial situation is identified, in full awareness of the security manager's specific scope of competence, the relevant demands and priorities, in line with the vision and objectives of the company business.

These considerations include:

- what are the processes, activities, and services of strategic value to the company and the relative information?
- which critical elements characterise them in terms of technology, human resources, procedures, organisational aspects?
- which aspects mostly torment senior management regarding security, in relation to the set short/medium/long term objectives?
- what innovative elements are being focussed on?
- which external factors could have impact on these elements?
- which solutions achieve and guarantee a happy medium between security and overall costs[4]?

These could therefore significantly influence choices of measures, interventions and the design of security aspects.

But presuming the right choices have been made on the basis of these aspects, is it possible to identify a set of areas for special focus by the Information Security Manager in the first 100 days?

The Community, on the basis of the skills and experience of its members, acquired from a broad-reaching portfolio of clients in terms of size, category and specific sectors, believes that the identification of this “minimum” and “essential” set of security interventions is possible, or at the very least useful to give rise to a diligent logic and increased awareness on how to proceed.

[4] In this case “overall costs” refer to direct costs (investments, management costs, etc.) and indirect costs (related to losses, fines, etc.). For more details on this subject, refer also to the document Return On Security Investment (ROSI) published previously by the Community.

Therefore, the following section outlines the selected areas of intervention, providing a concise and schematic description of each, and highlighting the following:

- the most relevant elements to consider in each area of intervention;
- the key questions to ask (and put to the competent company referees), also in relation to drawing up a check list to determine the initial situation by means of the quick assessment described previously in this document;
- the performance indicators can be considered to keep the effectiveness of the adopted actions and solutions under control;
- which company subjects should be, to varying extents, involved in managing this area;
- an estimate of the possible state of progress within the time frame considered, in close relation with the proposed approach, which envisages the implementation of several parallel PDCA cycles;
- a list (not definitive) of sources to rely on.

This effort is not aimed at replacing the best practices or international recommendations, which are cited where appropriate, but rather at simplifying the work of the reader in this short interval of the first 100 days.

The identified areas of intervention are grouped by type as follows:

Set-up of management tasks	• Security policies: what's in place and what needs doing • Management of compliance with standards • Data classification • Asset Inventory
Reinforcing technological aspects	• Adopting and/or configuring perimeter protections • Wireless network security • Patch Management • Hardening • System Vulnerability Checks • Protection against malware and minimum safety measures
Management of access to information	• Managing access to data and IT resources • Digital Identity Management
Effective incident management	• Incident management

6.4.1 Security policies: what's in place and what needs doing

Description	Security must be governed and based on macro-principles, shared by the top roles in the organisation, who should provide the reference framework for all adopted practices and behaviour. These macro-principles must be approved in the security policies formally adopted by the organisation (ref.§5.2.1).
Key questions	Are any policies already adopted? What is the degree of coverage of these policies with respect to the best practices (e.g. ISO/IEC 27001) and standards (e.g. Privacy, Italian Law no. 231/01, etc.)? How is application verified?
Important	Without policies, security of the organisation would be assigned to extemporaneous and sector-based initiatives, potentially at great cost, which without harmonisation and a global vision, could lead to a waste of resources when other aspects have not been taken into account. An analogy is the case of installing an armoured door in a plasterboard wall.
Points of focus	In the case of brand new policies to be drafted, the senior management should be involved in the process. Without the explicit and committed support of senior management, the operation would end up being purely cosmetic, with no real effect on organisation security. In the case of already established policies, the degree of penetration and their level of application should be checked, as well as any gaps remaining after application.
Metrics	To check the state and degree of coverage of the policies adopted with respect to the checks envisaged in international reference standards and best practices (e.g. the standard ISO/IEC 2700) 1 (degree of coverage) and the requirements as specified in standards of current legislation (standards on the protection of personal data (privacy, Italian Law no.231/01 etc.).
Visibility / stakeholders	Requiring the involvement and approval of all senior management, obviously with maximum visibility. Without a clear support from the top, the definition of policies is just an exercise in formality, with no practical value.
Planning	The definition and checking of policies is fundamental for an evaluation on the level of security and to define subsequent actions. This is therefore necessary very early on, and when the situation requires further actions, even including the issue of new policies (or amendments to existing versions), this procedure must be implemented as soon as possible. The Quick Assessment (§6.3.1) must also verify the presence/degree of policy implementation.
Reference standards or international best practices	• ISO/IEC 27001 • http://www.sans.org/security-resources/policies/

6.4.2 Conformity management

Description	Conformity (or compliance) refers to the series of activities aimed at ensuring that certain requirements are met, in line with the requirements of application standards of a specific organisation (regulations, laws, standards and internal policies), evaluating the potential risks and costs of non-conformities, comparing them with those envisaged to meet requirements, and lastly to prioritise, fund and start up all corrective actions deemed necessary. Some Italian reference standards for those who deal with information security include the "Privacy Code" (Italian Leg. decree 196/03) and the law on administrative liability of companies (Italian Leg. decree 231/01), already discussed above (§5.2), while on an international level there are the international security standards PCI DSS (Payment Card Industry Data Security Standard) which, while not compulsory by law, are contractually required by the managers of payment circuits, and lastly the international standard ISO/IEC 27001:2005 Information Security Management System. (§6.5.1).
Key questions	What specific standards should the organisation refer to? What is the starting situation and priority corrective actions to be implemented? Have ICT security reference frameworks been chosen (§6.5)? Are there adequate means to protect the most critical information (such as that related to research and development or significant data in terms of privacy, such as a client's personal information)?
Important	Non-conformity with reference standards may lead above all to consequences of a legal nature, or in the case of sector regulations, the loss of authorisation to supply a certain type of service or business. In the case of the reference framework for the ISMS, non-conformity of one or more parts may constitute evidence of weaknesses in the security management system, which should be solved as soon as possible.
Points of focus	The effective needs for data protection must be analysed, taking into account that with the disappearance of the company perimeter and the exponential growth in the volume of data exchanged, the loss of information constitutes an increasingly high risk for all organisations. It is therefore necessary to contemplate how we can survive a "breach" without damage (for example encoding the most important information, so that the data taken can nevertheless not be used by the hacker).
Metrics	Once the set of standards has been identified for reference, it is important to monitor conformity on a regular basis, and not just at the times of periodic audits.
Visibility / stakeholders	Protection of intellectual property or other critical information for the business should be an area easily understood by the senior management. Vice versa, the importance of complying with other standards, such as that governing privacy, may not meet with immediate acknowledgement by company management (even if in the case of personal data there is the potential obligation of notification in the case of loss or theft, with obvious repercussions on the image or reputation of the companies involved).
Planning	In the first thirty days, there is the priority to evaluate the starting situation, to then plan the most important corrective actions in terms of conformity, defining the priorities of interventions on the basis of associated risks.
Reference standards or international best practices	• Italian Privacy standards: http://www.privacy.it/codiceprivacy.html#allegatob • EU Data Protection Directive:http://en.wikipedia.org/wiki/Data_Protection_Directive • PCI DSS: http://en.wikipedia.org/wiki/PCI_DSS • ISO/IEC 27001:2005: http://en.wikipedia.org/wiki/ISO/IEC_27001 • Italian Leg. Decree 231/2001: http://www.camera.it/parlam/leggi/deleghe/01231dl.htm

6.4.3 Data classification

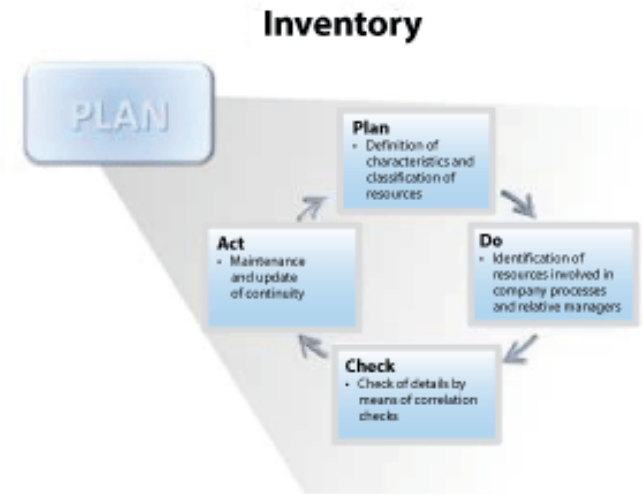
Description	The classification of data involves the examination of the various types of data present in the organisation and the evaluation of their relevance from a point of view of integrity, availability and confidentiality. This classification should take into account external constraints of the law (for example the Italian Privacy Law), deriving from the context (data classified or not, in terms of national security, classifications used by clients) and internal constraints deriving from the relevance for the organisation (intellectual property, patents, offers, costs, public image, etc.). The classification of information should be documented and kept up to date, so that it can be used for tasks such as risk assessments and the choice of adequate counter-measures.
Key questions	Is there an updated map of all data handled by the organisation? Can we estimate a degree of coverage? Is this map associated with an attributed value of data importance?
Important	Ignorance of the type of data handled may have consequences that span over a long period, from the “simple” and low level economic damage (excessive expenditure to protect data of little value) through to consequences of a legal nature (loss or dissemination of sensitive healthcare data). This is an essential task, without which there would be difficulties in organising risk assessments and evaluating the security measures adopted or to be adopted. This is indispensable before transferring services to the Cloud.
Points of focus	This task cannot be performed by the Manager alone, and needs the involvement of the managers of individual departments, who are the effective owners of the data.
Metrics	• On the annual repeat of the risk assessment, the lowest level of organisation exposure should be highlighted. • Level of classification coverage with respect to data present in the company.
Visibility / stakeholders	The data owners must be involved. Consequently a strong commitment from the manager is also needed here, without which classification would be difficult to apply, and above all maintain. The return of this activity is virtually invisible. As in the case of life insurance, which one hopes never to actually to cash in on, the correct handling of data serves to avoid consequences if something goes wrong. Having all data correctly backed up or aligned on the DR site to guarantee availability to the users or to protect the confidentiality of health records does not produce an immediate financial return, but failure to do so, in the event of an incident, could cause loss of image or even legal, civil and penal consequences. The classification will also help the Information Security Manager in his/her choices (and in the proposals to management) of security initiatives on the basis of relevance of data managed in the various areas, in particular highlighting the possible of selective intervention on the ICT thereby avoiding potential waste.
Planning	It is first of all essential to define an Information Classification policy based on the specific context of the company and applicable standards. The policy should be followed by behavioural measures and a revision of processes and procedures to align them with the rules of information management in conformity with the classification itself. Numerous PDCA cycles can follow for the classification and to ensure uniform management of the data through to the single system/application/user/data. It is a vastly complex and hard task, even lasting several years, starting from a vision at the highest possible level to then gradually be refined over time. But it is also an essential task, without which there would be difficulties in organising risk assessments and evaluating the security measures to be adopted now and in the future. If not already present in the organisation, in the first 100 days it is only possible to plan this, identifying and involving the stakeholders and the time frames for its first release.

	This is indispensable before transferring services to the Cloud.
Reference standards or international best practices	• https://wiki.internet2.edu/confluence/display/itsg2/Data+Classification+Toolkit • ISO/IEC 27005 (data are “assets”) • ISO/IEC 27001 (Objective A.7.2) • NIST SP800-60 (http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf)

6.4.4 Inventory of Assets

Description	The inventory activities enable the identification of all company ICT resources, whether physical, technological or logical and relevant to business, associating each with the references of formal responsibility in terms of management and security as well as the specific information used to make up the technical and security profile. For example, an inventory may include: • the work stations, with the users assigned to each (and therefore the processes in which they are used) and the software installed (operating system, applications); • servers, associated with services that they support; • software licences; • network equipment; • network sockets, with location and connected systems; • databases; • document repositories; • … The inventory can be seen, even before considering it a security tool, as a means of improving IT management efficiency, especially when integrated in instruments designed for this purpose (IT asset management tools) and/or with help desk tools, or even with network and system management tools. In fact the inventory must be a working tool, which has very little to do with a general inventory of assets for accounting purposes, probably already present in the company.
Key questions	• Does the company adopt centralised system and network management tools? Can these tools integrate an inventory component? • Has an IT asset inventory process been defined? Have the company roles involved been identified for this process? • If it exists, does the inventory specify the formal responsibility of each ICT resource. • Is there a process for inventory maintenance and updates? • Does the inventory specify, in association with each ICT resource the critical level of the latter?
Important	This activity is preliminary to an effective protection of company ICT resources, as it enables: • identification of all relevant assets for the company; • identification of organisation subjects or structures who decide on the aims and methods of management and protection. • prompt and effective identification of the IT resources associated with a security event; • verify the correspondence of resources present with company standards; • Support of the processes for risk management and business continuity.

Points of focus	Within the business and IT processes all significant assets must be clearly identified (for example on start-up of the IT risk assessment of the application systems) in terms of: • importance for company business; • potential impact following the lack of or insufficient confidentiality, integrity and availability; • interdependence/relations with other assets (for example, if the systems are part of an application architecture, etc.). For this purpose, it is necessary that the inventory of all resources (materials and information) are suitably managed in order to safeguard the company's IT assets. The inventory of relevant resources includes all information necessary to retrieve the latter following any incident or disaster. In particular it is necessary to specify: the type of resource, format, location of the back-up information, information on the licence and the company value. In order to promote the uniform approach of the Business Units involved, even when distributed across various group companies, the following types of resource are identified below: • information, the use of which contributes directly to the achievement of company objectives; • programs, which serve to manage information and thus indirectly contribute to the achievement of company objectives (for example application modules and components of the operating system); • infrastructures, which like programs support management of information and indirectly contribute to the achievement of company objectives (for example networks, servers and technological systems). To guarantee effective management of protection, each IT and information resource must be formally associated with an “owner” (i.e. according to ISO terms, the “manager” and not necessarily the owner), i.e. to a subject or body that deals with the maintenance, classification, management and security. For this purpose it should be pointed out that although the implementation of specific security checks can be delegated by the owner to another working subject (for example operating system management personnel), this practice does not imply the transfer of formal responsibility for protection.
Metrics	Percentage of resources classified by type. The resources may be excluded either because the process does not yet cover all areas, or due to a failure in the process itself, where the resources that should be classified are effectively not. However, it is important also to evaluate the effective use of the inventory in the management processes, without which the inventory would remain in use and serve simply unto itself. For this reason, it may also be useful to evaluate how many activities (such as calls to the help desk) effectively make use of the inventory.
Visibility / stakeholders	The inventory activity lies at the foundation of correct management of IT and information security, and also contributes to effective measurement of the state of security/risk, aiding improved planning of control activities and enabling targeted actions or interventions when necessary. This is a support activity that in itself only allows limited visibility for the owners of company processes, as it focuses on technological components. Process owners are mainly involved as regards the identification of databases and document repositories. Vice versa, there is significant involvement of IT system management, which can easily make owners the main users, even more so than Security Managers. In fact, the support of the IT manager is fundamental to produce the inventory, and in being able to gain advantage from this same document, this manager can become the main sponsor of the initiative. Vice versa, if IT management is not convinced of the utility of this initiative, it may well turn out to be completely ineffective.

Planning	From a business point of view and in the implementation of the relative Information Security Management System (ISMS), the inventory activities become part of the Planning phase: it is thus functional to the effective planning of any interventions required. However, within this inventory a complete mini Deming cycle develops, which envisages the consecutive completion of the phases shown in the figure below.  **Figure 11IT asset inventory management cycle** The inventory is thus preliminary to the effective completion of other interventions. Planning of the inventory should be among the first activities to be put into action, for completion as soon as possible. It must be considered that this is an activity that may require considerable time and resources, and therefore great care must be taken in the planning phase, before starting with the Do phase.
Reference standards or international best practices	ISO/IEC 27002:2005, *Information technology - Security techniques – Code of practice for information security management* • A.7.1.1 – Definition of the inventory • A.7.1.2 – Definition of Ownership

6.4.5 Adopting and/or configuring perimeter protections

Description	The term Perimeter Protection basically means all technologies that have anything to do with the protection of the business perimeter. The main technologies include Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems and Virtual Private Networks. The aim of these technologies is to enable remote access to company resources only to users/processes/applications explicitly authorised for this purpose. In this module we give particular emphasis to Firewall technology.
Key questions	• Is there are company policy, known to personnel, that indicates the legitimate applications of Internet connections and email? • Is the border between private domain and public business domain clear and well defined? • Are all access points to your network accounted for? • Which instruments are used to ensure that all access is in line with the Company Security Policy? • How is the life cycle of firewall rules implemented, and in particular how is a request for modifications to these rules managed? • How often are firewall rules checked? • Is there an Intrusion Detection and/or Intrusion Prevention system? • How are the logs of all perimeter systems handled? • Is there a centralised Log Management system?
Important	An accurate application of the best practice in company IT Perimeter Protection enables: • the identification and reduction of vulnerabilities of the company network before they are detected and exploited by potential hackers; • increased awareness of potential threats to which the company network may be susceptible; • quicker response times to incidents; • measurement of the effectiveness of Perimeter Security processes; • automation and strengthening of controls for perimeter security; • integration between people, processes and technologies in the complete life cycle of events that impact Perimeter Security. Failure to implement a correct Perimeter Security Policy and the relevant mechanisms for its implementation leaves doors open for access to the entire company IT system, with potentially devastating consequences for the entire enterprise.
Points of focus	One fundamental point of focus is the revision of the process of change management of all security policies applied to the perimeter protection systems. For example, the following need to be verified, as a minimum requirement: • is there a process for managing the life cycle of the rules implemented on the perimeter protection systems?; • is a formal process envisaged for requesting, reviewing, approving and implementing changes to rules? • are all changes to rules authorised and has a procedure been defined on what to do if unauthorised changes are discovered?
Metrics	There are a variety of metrics regarding Information Security in general, which can be grouped as follows: Process Security Metrics, Network Security Metrics, Software Security Metrics and People Security Metrics. As examples of Security Metrics applied to perimeter protection, the following can be considered: • How many accesses to the perimeter are successful and how many fail? • The number of identified and/or blocked incidents; • The number of “port probes” found; • We can also consider the number of tickets opened by the users (or requests to the help desk) for problems of access via the firewall to the Internet, often an indicator of some problem in the policies or in the configuration.

Visibility / stakeholders	The main stakeholders in perimeter security are the senior management and those responsible for each department that uses the company network, and last but not least the final user. The main effort to enhance visibility of the work carried out/under way above all regards the Business Stakeholders. With these it is necessary to demonstrate that: • investing in a perimeter security policy with adequate means is actually more financially viable than implementing all measures necessary to recover after an IT incident that impacts the company perimeter (Quickwins); • a perimeter security policy, with adequate mechanisms and the relative metrics, may contribute to providing a set of annual data that will enable the choice whether to equip ourselves (or not) with an insurance policy that covers the risks associated with the IT systems (complex but important).
Planning	In the first 100 days there needs to be a shift in the classic PDCA model, which when intervening in a contest that is already operative, will start the first cycle right from the Check phase. This is a relatively short cycle, which could also be completed within the first 100 days, and which is worth starting immediately, both due to the critical nature of possible unauthorised access from the outside, but also because this is not a very complex activity and is reasonably visible (Quickwin). 1. In the Check phase, all Network Security Assessment tasks should be started, with a revision of the security rules applied to the perimeter protection systems; 2. In the Do phase, all measures should be implemented to solve any inconsistencies between the company security policy and the non-compliant security measures/mechanisms resulting after the check phase. 3. The Plan phase then involves the introduction of possible additional technologies to improve or revise the associated security processes; 4. In the Act phase, a pilot project should be identified, within which the new and more comprehensive perimeter protection system is to be developed and tested. After 100 days, the pilot project will then be extended to the entire network infrastructure.;
Reference standards or international best practices	• "Implementing a Network Security Metrics Program", GIAC, http://www.giac.org/paper/gsec/1641/implementing-network-security-metrics-programs/103004 • "Audit/Assurance Program: Network Perimeter Security", Cobit 4.1, https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=WAPNP • "Firewall Checklist", SANS Institute, http://www.sans.org/score/checklists/FirewallChecklist.pdf • "Playing by the Rules: Performing Firewall Audits", Infosec Institute, http://resources.infosecinstitute.com/firewall-audits/ • "Security Configuration Guides", National Security Agency, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml • "Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit", ISACA, http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf

6.4.6 Wireless network security

Description	This technology is widely adopted in companies, for a broad range of purposes: from wireless connectivity in meeting rooms, to automation in the warehouse by management of bar code readers or similar, through to the production line for the connection of sensors otherwise impossible to reach using traditional Ethernet wiring. Unfortunately, the technology 802.11a/b/g/n is not risk-free if not implemented correctly, following a detailed risk assessment. Even after such an assessment, we nevertheless still have to make comprises due to the limited support that many terminals offer with respect to security functions. It is also very difficult to effectively manage guests, consultants and rotas between colleagues.
Key questions	• What security mechanisms have I envisaged for connection to my WiFi network? • Is access based on a simple static shared password? • Is the protocol used easy to attack? • Is the wireless network in bridging with the internal network? • Can all company resources be accessed from the wireless network. • Is there only one Wireless network, or several networks depending on the functions required? • Do guests have a dedicated network? • Has host isolation been used in the guest network. • Does a monitoring mechanism exist? • Does somebody check the data collected by the monitoring mechanism? • How do I manage the issue of unauthorised access points, i.e. “rogue APs”?
Important	A wireless network not configured properly, or the presence of a rogue AP enables direct access to many company assets, data or services, entirely bypassing many protection tools (e.g. firewalls, IPS, and even malware prevention tools). The use of a static shared password among colleagues prevents blocking access to someone who leaves the organisation. Failure to use a dedicated network for guests enables temporary guests to permanently access company resources, even from outside the physical perimeter of the company.
Points of focus	To have a clear, up-to-date and usable Wireless User policy. To thoroughly avoid the use of networks without authentication and encryption or with obsolete mechanisms (e.g. WEP). To segment the WiFi network from the wired network, to then create different wireless networks, not bridging with the internal network, for the different processes (e.g. one for offices, one for the warehouse, one for a production system, one for guests). Dedicate a network correctly configured for guests, with expiry-based access, limited to only authorised resources (e.g. the Internet). Keep the WiFi network monitored.
Metrics	• Number of external users temporarily authorised. • Number of unauthorised attempts at access. • Number of WiFi network analysis activities for intrusion purposes. • Number of security incidents (including the diffusion of malware) occurring via systems connected to WiFi networks.
Visibility / stakeholders	As this is a basic technology of the infrastructure, this is perceived as a non-strategic facility. The return to visibility is only obtained when security mechanisms do not introduce significant constraints affecting usability by users, performance or stability of the network.

Planning	In the early days a careful risk assessment is necessary in relation to the use of WiFi networks, if not completed previously, verifying the policies effectively applied. In view of the results obtained, it would be possible to organise amendments to the policies with the implementation of urgent remedies (e.g. if the network uses WEP, this should at least be updated to WPA2/PSK). In this phase it is possible to plan the subsequent implementation of measures such as a NAC, the use of the Enterprise version of WPA2 or the use of OTP for access to the WiFi network.
Reference standards or international best practices	• http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf • https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guideline_with_WiFi_and_Bluetooth_082211.pdf

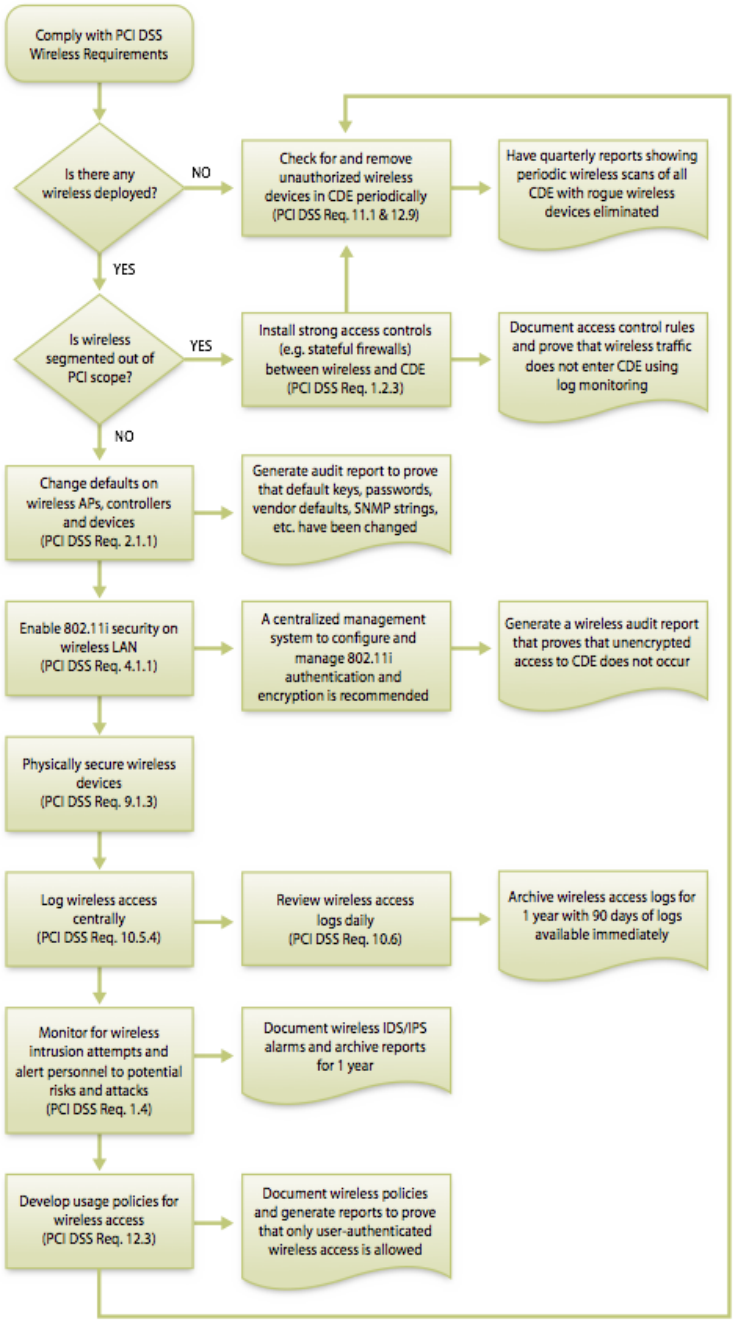


Figure 12 An example of implementing security measures on wireless networks according to PCI-DSS standards

6.4.7 Patch Management

Description	The Patch Management process includes the activities of identification, acquisition, checks and installation of patches, i.e. corrections to software and firmware aimed at solving issues related to security and/or specific functions of application products as well as information and processing systems.
Key questions	• If present, does the patch management process set up in the company use an approach that covers the phases of identification, acquisition, compatibility checks and operation installation? • Does the organisation adopt an adequate patch management instrument in relation to the dimensions of the IT? • How often has there been a security incident due to lack of system updates? • How many times have errors during system update phases caused interruptions to services or other faults? • During execution of the process concerned, does the company balance the needs of security with the objectives of usability and availability?
Important	After defining the intervention priorities, the Patch Management process should be applied according to the evaluation of critical factors in information systems of the organisation.
Points of focus	The choice of instruments supporting patch management main depends on the architecture and applications present rather than on the Management System adopted for Information Security. With regard to client stations, a revision of the patch management process should be performed only together with that of configuration management, in order to guarantee the possibility of performing updates on the entire fleet of company work stations with minimal impact. **Figure 13PDCA cycle applied to patch management: Plan phase** Among the main aspects related to the project concerned, the following are worth highlighting: • constant updates to the inventory of software installed on the company information systems; • the presentation of the level of synergy between the process concerned and the activities related to the IT risk assessment and management.
Metrics	Depending on the maturity of the organisation in the area of Information Security, different types of metrics may be applied. In ascending order, these metrics take the following into account: • the level of process implementation, measuring the relative evolution/progress; • the level of operativity, efficiency and effectiveness; • the entity of the impact on the organisation's mission; • More in detail, examples of implementation measures include: • the percentage of servers with applications automatically entered in the inventory according to the correct implementation of the Patch Management process; • the percentage of work stations (fixed and mobile) involved in the process concerned.

	Examples of measures regarding effectiveness and efficiency of the process include: • the frequency of checks adopted for the hosts in order to eliminate the risk of missing updates; • the frequency of updates to the inventory of applications installed on the host; • the minimum/medium/maximum time required for application of the patches to a set percentage of hosts; • the percentage of stations updated within X days from the official release of a specific patch, the percentage within Y days, and the percentage within Z days (for example with the values X, Y and Z set at 10, 20 and 30); • the average percentage of hosts fully subject to patches in a set time interval, and the percentages of the latter according to the critical levels (e.g. highly critical, medium critical and non-critical); • the percentage of patches applied completely automatically, partially automatically and manually. Examples of measures related to impact include: • an economic evaluation of avoidance of costs (due to intrusions and disservice linked to systems not updated) obtained from the organisation following implementation of the Patch Management process; • the percentage of budget used by the competent organisation structure for executing the patch management process applied to specific class of information systems.
Visibility / stakeholders	Patch management is a technological activity that is not normally largely visible outside the scope of IT management, apart from when implementation demands translate this task into activities that need to be performed by users. On the contrary, it is an activity that involves a significant part of IT management and which therefore the information security manager does not perform autonomously. In fact, as already mentioned, it is often integrated in instruments for system management and therefore from an operating point of view it is not performed by the Manager, who simply has to define and check policies.
Planning	It is possible and necessary to immediately review the patch management process, renegotiating the responsibilities of all actors involved. There will subsequently be the need to identify possible constraints and prerequisites that will enable effective implementation of the process in the future (support tools, asset inventory etc.) planning necessary actions over time, probably well beyond the first 100 days. In the meantime, two parallel actions must be started up: • the definition of temporary measures to be put into place pending implementation of the patch management process in the future; • a substantial “clean-up” in the various environments (database servers, application servers, client systems, etc.) verifying the update status and planning of patch installations as necessary. Ideally it should be possible to complete these actions within the span of 100 days, again depending on the current update status of the systems, thus enabling the presentation to the management of concrete results from this joint action of the various roles involved in the secure management of IT systems.
Reference standards or international best practices	• ISO/IEC 27002:2005, Information technology - Security techniques – Code of practice for information security management • NIST SP 800-40, Guide to Enterprise Patch Management Technologies • NIST SP 800-55, Performance Measurement Guide for Information Security

6.4.8 Hardening

Description	Hardening consists in making the configuration of a system the most “resistant” with respect to standard or pre-configured versions. This is an activity performed by personnel assigned for system management, on the basis of check lists drawn up by the security department, with the following objectives: • to increase the level of system security (firmware, operating system (OS), basic software or middleware) by acting on the basic configuration, disabling components not necessary and all services of no use to company business, installing updates, plug-ins, security services and any other software deemed necessary on the basis of international best practices in security; • guarantee that the systems, from operation through to their decommissioning, meet the requirements of the security check lists and comply with legal obligations.
Key questions	• Is the company equipped with secure configuration guidelines /check lists for the different types of OS, DBMS, web/application server etc. that are used? • Before making a server or work station available, is a secure configuration process envisaged? • Are periodic checks envisaged on the secure configuration of server systems? • When a new type of OS (or new major release) is introduced in the company, is the issue of relative secure configuration guidelines envisaged? • Is documentation envisaged for secure configuration activities performed on individual systems? Are cases documented and managed where a hardening measure envisaged in the guide lines has not been applied to the systems? • Is the system perimeter known on systems where secure configuration activities have been performed? Is there a hardening plan in the company?
Important	The purpose of hardening is to reduce the attackable area of systems and vulnerabilities present, often sufficiently serious as to consent even an outdated malware or automatic tools to successfully hack company systems. Although the company has other security measures to prevent this type of attack (e.g. antivirus), they may not be effective on vulnerable systems, where at most they may be able to contain the effects or limit the potential spread of the malware on other systems.
Points of focus	The check lists must be compiled to trace the tasks effectively performed. The activity should be repeated periodically, to verify that the system still corresponds to the relative check list. The efficiency of the activities should be checked periodically, for example by means of Vulnerability Assessments on the systems. In the absence of a previously defined process, hardening should be envisaged on all used systems.
Metrics	Percentage of systems conforming to the check lists. Percentage of check list controls not implemented. The company can measure the benefits of hardening with automated vulnerability assessment tools, listing the vulnerabilities present on the system before and after the activity. A good hardening activity must ensure VA results without high or medium class vulnerabilities. In any event, hardening is an activity that covers aspects of prevention (e.g. disabling unnecessary services, even if not vulnerable at the time) which do not lead to immediate benefits other than in terms of risk reduction.

Visibility / stakeholders	Hardening is also a technological activity without significant visibility outside the area of IT system management. The hardening activity applies first of all to the new systems put into operation, and therefore must be strictly coordinated with management of IT operation, which will presumably be carried out on the basis of the check lists supplied by the Security Manager.
Planning	It is important to start up this activity as promptly as possible, at least on the most critical systems, probably at the same time as the clean-up of systems not updated and in line with patch management procedures. However, it is generally more complex and burdensome as a task, and usually takes much longer. PLAN: selection of the types of OS/middleware with most priority/distribution, the issue of a hardening plan DO: implementation of hardening activities on the first system perimeter CHECK: Vulnerability assessment of systems on which ACT hardening has been performed: revision of check lists and planning of necessary corrective action on perimeter systems
Reference standards or international best practices	• HD NIST guidelines: http://web.nvd.nist.gov/view/ncp/repository? • NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems • NIST SP 800-70 National Checklist Program for IT Products—Guidelines for Checklist Users and Developers

6.4.9 System Vulnerability Checks

Description	The vulnerability checks of company IT systems, both as basic software and middleware applications and / or databases, provides important information when planning any infrastructure measures to protect the business. The common understanding of Vulnerability Assessment (VA) is as an activity mainly carried out through automated tools that scan the IP network to see if any situations arise in terms of vulnerability patching, exposed services, accessibility to the machines or applications. The Penetration Testing (PT), on the basis of information gleaned through the VA, aims to test the possibility of exploiting a vulnerability through a specific intrusion attempt (exploit) which can be performed in part by automated tools and in part manually
Key questions	• Does the company provide services on the Internet or web application which expose company data and/or customer data? • If a patch cannot be installed, what other protective measures are provided? • What level of logic separation and security is provided between the front-end and back-end of my services? • Are my perimeter protections able to detect hacking attempts based on known techniques?
Important	VA and PT are not intended to replace the necessary technical measures and security processes designed to prevent incidents, nor should be they construed as a support to patching and secure configuration activities which should, even alone, ensure a satisfactory level of reduction in risk exposure. Just like the audit, they are an important means for checking whether these processes are properly implemented along the entire perimeter of IT systems.
Points of focus	The VA and PT activities can be performed autonomously by the company, although periodic feedback through third-party verification is recommended. The tests can therefore be carried out in either “black box” or “white box” mode (these differ according to the information on systems made available to the hacker), alternating between the two modes on the basis of what results are required to support security. Penetration Testing requires the utmost care in establishing the engagement modes since it may damage or disrupt operational systems.
Metrics	• Number of critical level vulnerabilities detected • Number of critical services deemed vulnerable • Average time of patch availability for the vulnerabilities detected
Visibility / stakeholder	The activity can constitute a means of awareness for the IT areas involved, and a measurement and historical analysis of the results can validate the results of any actions taken (definition / revision processes with an impact on security, integration of new perimeter protection tools, etc. ...). With regard the management, the results of a PT can be either a user-friendly instrument to highlight the need for interventions and therefore the resources needed to carry them out, or a way to highlight the effectiveness of security management.
Planning	The suggestion is to plan at least a first VA, preferably accompanied by a PT, within the first 50 days so as to have an overall picture of the state of IT systems. It is good practice to then plan a subsequent VA and PT, downline of the first planned actions so as to have an initial means of comparison. The activity could be arranged periodically, depending on the degree of company exposure.
References to the international standards or best practices	• ISACA - IS Auditing Procedure: P8 Security Assessment - Penetration Testing and Vulnerability Analysis (http://www.isaca.org/Knowledge-Center/Standards/Documents/P8SecAssess-PenTestandVulnerabilityAnalysis.pdf) • COBIT (IT Governance & Control): http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

6.4.10 Protection against malware and minimum safety measures

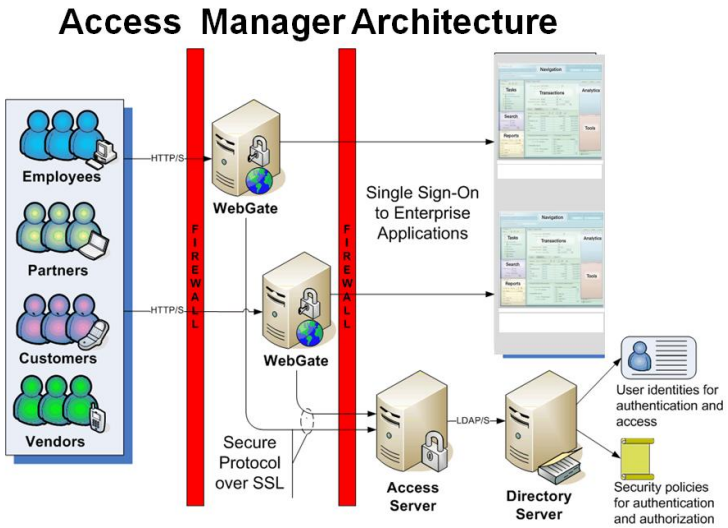
Description	Apply specific protection measures to protect the managed information on the critical assets of the company, such as minimum measures established by legislation on the protection of personal data, anti-malware controls, and intrusion detection/protection.
Key questions	• What information could the hackers want to obtain? What type of data does the company deal with? • Are the company devices and system regularly updated? • Are malware detection and intrusion detection systems present? • Is antispam software and antivirus software installed?
Important	The lack of appropriate security measures, could lead to the following: • The lack of a minimum configuration policy on systems that can be used as points of access, to install malicious software or unauthorized services; • Systems that have not been updated, which would allow an attacker to exploit the vulnerability to gain unauthorized access to systems; • Ineffective system configurations for preventing and controlling the malware and attacks based on known security techniques.
Points of focus	• Perform a thorough analysis of the current status of the company (ref.§6.3.1); • Define a priority scale of the problems detected. Plan which problems will be resolved immediately and which will be resolved in the coming months; • Adopt basic security measures (e.g., rules of password formulation and blocking) required in order to make external or internal intrusion attempts of the system more complex; • Security measures must comply fully with the company business requirements and regulations (for example, the “Minimum Measures” in Annex B of Italian Legislative Decree 196 / 03 - ref. Section 5.2); • Define mechanisms, instruments and monitoring procedures for tools and security measures; • Support the training of staff in terms of security.
Metrics	In order to demonstrate the added value achieved using the practice, the following need to be quantified: • the number of infected hosts; • the number of systems whose anti-malware software is not updated; • the number of infections which have been detected and resolved; • time spent resolving the infections; • the systems that have been adjusted from the date of appointment of the new Information Security Manager.
Stakeholder visibility	In general, management understands the need to put the measures described for the protection of information in place, even though management may see the problem as one which is easily resolved exclusively through technological means. The Information Security Manager will therefore also have to demonstrate the added value of actions which are of a procedural and process nature in support of technical countermeasures, as well as the effectiveness of regular audits for checking and resolving, where necessary, any problems encountered.
Planning	This activity also needs to be undertaken within short time-frames, particularly with regards the adjustment of anti-malware tools. Generally, this type of adjustment can be brought up to a good level in a short space of time. Furthermore, a reduction in the number of detected infections is easy to measure and is immediately visible (QuickWin). The complete adjustment, particularly in terms of the minimum measures required by Annex B of Italian Legislative Decree 196 / 03 may require more time and more careful planning and will require a wider involvement of IT management.
Reference standards or international best practices	• http://www.sans.org/critical-security-controls/control.php?id=5 • http://cve.mitre.org/

6.4.11 Digital Identity Management

Description	The set of technological, procedural and organisational measures to ensure compliance with company policies and regulations relating to user management on infrastructure components, systems and applications, from the moment users are registered up until the registrations are deactivated. These measures include checks to verify that the person with a virtual identity for gaining access to a certain IT resource is not just identified and authenticated by the company, but is also authorised and suitable traceable. These measures are generally related to the technological aspect, charged to IT, but still aimed at ensuring compliance with the resource user policies and company data. **Figure 14 The real identities are mapped on different digital identities which are then associated with the rights of access to different resources**
Key questions	• Is access to the company's Web applications controlled by a centralised Authentication and Authorization system? • Do users need to be authenticated each time they use Web applications by entering different credentials for each application system? • Is there is a mapping of company applications used by personnel, internal or external resources? • Have tools for credential managing tools for access to IT applications been prepared? • Is there an archive of credentials for access to IT systems and applications? • If an employee leaves the company, how are his/her credentials for access to systems disabled (de-provisioning)?
Important	The authentication and authorisation mechanisms for access to applications and / or systems can help avoid situations in which a user can access company resources with accounts which have not been recognised and authorised. Centralisation into a single User Management system for Access Authentication and Authorization makes it easier to implement minimum measures and appropriate measures for regulatory compliance in the areas of password management, access logging and audit reporting. Furthermore, it simplifies the monitoring of significant events for security (e.g. brute force password).
Points of focus	The more the business systems of the company are exposed on the Web, the more important it is to increase the level of protection by introducing centralised control mechanisms of access credentials, capable wherever possible of defining policies based on user type.

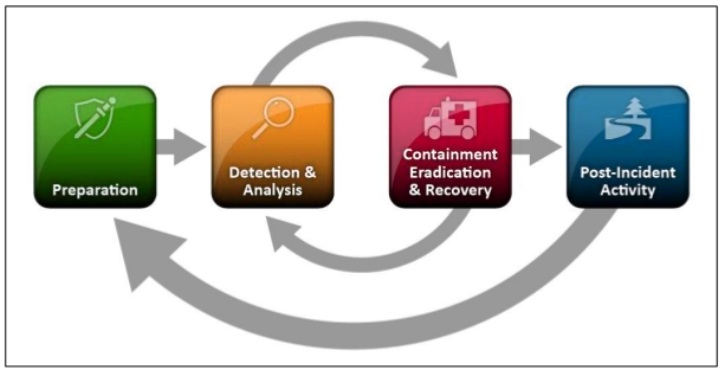
Metrics	• The number of applications that benefit from the function of the centralised authentication for accessing systems • Promptness in preparing reports for Audit departments • Number of authentication attempts using incorrect passwords • Level of automation and speed of execution of the activities for creating, modifying and removing users from the system • Charges resulting from password reset activity • Availability of proactive systems reporting the abuse of identity for access to systems
Visibility / stakeholder	The introduction of a centralised Authentication and Authorization system in the company allows numerous benefits in terms of operational management to be obtained, and is a definite advantage for IT. The visibility obtained with regards the rest of the company depends primarily on the ability of making provisioning / de-provisioning processes, password management and profile management access to data, systems and applications less burdensome.
Planning	It is reasonable to assume the start-up of a serious assessment within a short time frame in order to have a clear view of user management. On the basis of the findings, a plan must be established regarding all the corrective actions necessary to control user management with this plan then becoming a strategic asset of the ISMS of the company. This activity is somewhat extensive but it can probably be planned within the first 100 days.
References to the international standards or best practices	• ISO/IEC 24760-1:2011 • Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts • http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57914

6.4.12 Managing access to data and IT resources

Description	In current terminology, access management refers to technologies and processes that govern and implement the assignment of rights for access to IT resources of the company for internal and external users. In a vision oriented towards business processes, with an organisational and not strictly IT based focus, access management consists in determining the model with which the use of IT resources is assigned to users on the basis of their role within or outside the company.  **Figure 15 Example of the architecture of access management for access to services displayed through a web portal**
Key questions	• Has the company defined an Organisational Structure including the hierarchy of roles, names of managers within the structure and the allocation of human resources assigned to each organisational unit? • Have Job Descriptions been formalised to identify the tasks and responsibilities related to organisational roles? • Is there is a mapping of company applications used by personnel, internal or external resources? • What guarantees are in place that resources have access only to the applications envisaged by their role / task? • For example, if the Active Directory is used as the LDAP of the credentials, what tools are used to track the possible definition of shared network Share and the corresponding permissions assigned to users?
Important	The governing of access privileges on IT resources (applications and /or systems), if properly implemented through the definition of Roles, helps to ensure that situations are avoided where, for example, a customer care user can access data regarding salaries.
Points of focus	Involve all stakeholders (Audit, HR, Business), not just IT components. Deal with the project in phases, balancing technical components with organisational components. In general, from the technological point of view, many of the essential components for implementing policies in managing the access of resources are already available in the basic software and middleware components, although they may not always be enabled or correctly configured. Wherever possible, address the technical solutions to a model of centralised account management and their corresponding access privileges to resources.
Metrics	• Number of attempts to access unauthorised resources from the user profile. • Promptness in preparing reports for Audit departments • Number of systems/applications which are integrated with IT resource access management solutions. • Number of attacks which have resulted in the loss of data and interruption of services before and after the adoption of measures to control access to IT resources.

Visibility / stakeholder	The installation of a complete access management system, together with user management (§6.4.11) is certainly complicated but it is essential since it involves different stakeholders. The visibility that this can provide, as a return of the commitment, is therefore high due to the interest it can raise within the entire company: • Human Resources Management must be able to provide IT guidelines on the allocation of permits issued on the basis of the task of the individual employee; • Auditing must have tools available to verify and certify that the guidelines are correctly applied; • The Business Units can reap the benefits in terms of efficiency and speed in obtaining access permits for their employees; • IT would certainly have clear advantages in terms of streamlining operations resulting from the use of technology to support user management, but above all it would have the opportunity to redistribute and share the responsibility for certification that its use is appropriate for the actual owner of the IT resources, which are primarily the Business Unit and Management.
Planning	It is reasonable to assume the start-up of a serious assessment within a short time frame in order to have a clear view of user management. On the basis of the findings, a plan must be established regarding all the corrective actions necessary to control user management with this plan then becoming a strategic asset of the ISMS of the company. This activity is somewhat extensive but it can probably be planned within the first 100 days.
References to the international standards or best practices	• ISO/IEC 24760-1:2011 - Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts • http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57914

6.4.13 Incident management

Description	Faced with the real possibility of a security incident, it is appropriate to deal with the problem by implementing policies beforehand which enable effective management of these events. The first phase of the incident management process is called Preparation. In this phase it is advisable to make a preliminary assessment of any procedure in place and the level to which it complies with industry standards. The phases will then be structured as follows: • Detection and Analysis, to evaluate and understand the nature of the incident which could refer to the following categories: Unauthorised access: libel and threats, theft or disclosure of information, theft or loss of devices, denial of service, inappropriate use, virus and malware; • Containment: suggesting the correct containment methods and the possible acquisition of digital evidence of the crime which can then be used in Courts of Law; • Eradication and Recovery: to apply the possible countermeasures necessary to remove what may have generated or left the incident in the affected systems and restore correct operation; • Post-Incident Activities: to document the incident (report containing the symptoms detected, the activities performed and results achieved) and particularly to prevent the incident from happening again in the future (lessons learned); • Event closure - registration in the trouble-ticketing system of the intervention and event closure.  **Figure 16** **Incident Management Process phases - NIST SP 800-61**
Key questions	• Is there an active trouble-ticketing system in the company able to track incidents and measure the quality of IT services? • Is there an Incident Response Policy? • Has a Crisis Committee been identified and formalised at company level? • Are there both managerial and HR representatives in the Committee? • Has the role of the single point of contact / spokesperson for the Crisis Committee been formalised? • Have contacts with the CERT (Computer Emergency Response Team) been established or have advisory services for incident security and support been acquired (for example, integrated in products of intrusion prevention)? • Are there resources in the company able to perform Computer Forensics? Does the company prefer to delegate the task to specialist external companies?
Important	The proper implementation in the company of an Incident Management Process is critical as it allows a response to a crisis situation appropriately without panic - which could even exacerbate losses of an economic nature. The ability to analyse an incident allows those responsible for the IT attack to be traced and therefore enables the company to pursue and obtain compensation for damages incurred. It is enough to consider the damage to the public image of numerous Italian companies following attacks by hackers, in particular those of 2011.

Points of focus	It is appropriate that all interventions relating to incident management are tracked by a specific trouble ticketing system used in incident management. From an operational point of view it is advisable that an on-call service is activated (through communication channels considered safe) for managers involved in the incident management (or the Crisis Committee). From a procedural point of view, the task of analysing digital evidence gathered during the incident management process, must ensure that all digital evidence which is found and analysed is considered: • Admissible: to be used in Courts of Law • Authentic: or closely related to the digital media which has been detected • Complete: correlating all possible information • Reliable: without raising any doubts as to authenticity • Credible: allowing anyone to reconstruct the process that led to their detection with the same results
Metrics	It is possible to adopt generic metrics within the area of Incident Management (for example, the number and type of incidents, category of impact and economic damage, the percentage of resolved situations within the set time scale, service levels, etc.) which may evolve into the field of Information Security Management according to the rules, functional specifications and specific use cases. Examples could include the number of countermeasures, time for identifying these countermeasures, number of security incidents classed according to their level of severity, the number of incidents that have caused service to be interrupted or downgraded, the number of security checks performed and vulnerabilities identified during the penetration test session, attempts to gain unauthorised access, violation of the policies defined, system resilience in the face of attacks, etc. The continuous measurement of these indicators, through the dimensions expressed both in absolute and relative values, will be evaluated and subject to continuous improvement in order to define the so-called “security posture” of the processing infrastructure.
Visibility / stakeholder	The involvement of management of all sectors is essential, in particular for the setting up of the Crisis Committee. Incident management activities are highly visible as they allow indicators to be obtained on the level of protection offered by the security systems and procedures.
Planning	Planning depends on the presence or lack of a pre-existing incident management procedure and by the presence of a trouble-ticketing system. If not present, there should be an initial phase, which can also be completed within the first 100 days, for the set-up, the appointment of the Crisis Committee and Management approval. After this, service can start with the collection of indicators for future improvements (Check - Act).
Reference to international standards or best practices	• NIST SP800-61 - Computer Security Incident Handling Guide • SANS Institute Incident Response Methodology, • CoBit, ISO27000, ITIL V3

6.5 Long-term strategy

We have already mentioned both the tactical (§6.1.3.1) and strategic (§6.1.3.2) approach. The content outlined up to this point, within the first 100 days of the appointment of the Information Security Manager, addresses the “tactical” actions (and those deemed essential) for maximising the effectiveness and speed of response to the problems which are probably seen as more pressing for the company when the Information Security Manager starts work.

At the same time, the Information Security Manager is responsible for setting goals and therefore a long-term strategy, a task which involves establishing objectives that can (and should) take root right from the beginning of his/her actions, in parallel to the “essential” actions already started (§6.4).

Once this has been clarified, the question of how to implement it remains. Undoubtedly a method, methodology, operating mode, procedure, framework, or similar is needed.

Does there have to be a framework (which implies a methodology) closely related to information security? Not necessarily. The Information Security Manager may find him/herself operating in a company whose processes are well organised and managed according to ISO 9001, and therefore can use this system to find meaningful answers to the first three activities outlined above. Depending on the type of company, he/she could be working on a model of risk management dictated by Basilea, rather than with other different approaches.

The focus at this point is to give the information security management system an organisational structure. The risk is that a parallel system could be created, a system which is isolated and seen as a system of control or at best, prevention. In other words, a system which is barely integrated, regarded as a necessary burden, a cost.

What can help an Information Security Manager from the outset, or once he/she has reached this point in giving the information security management system an organisational structure without incurring the previous risk? Experience teaches us that this is a very real risk.

Management systems will come to the aid of the Information Security Manager which may be more or less specialised for the purpose. Now the ability of the Information Security Manager, in order to avoid the risk of isolating his/her system, lies in checking that in the company management system, with reference to the set targets, there are already potential procedural synergies, which can introduce and support the vision and operation of information security. This check must be extended to the broader field of IT governance processes (now often involved in the governance process) and the possible relationships and integrations.

While one of the objectives is to certify the security management system, for example for reasons of liability to third parties or internal stakeholders, it is clear that the adoption of ISO 27001 is recommended together with the various corresponding standards. But in doing so we must also take into consideration the relationship between this system and the system of governance. If this is not structured or fully developed, ISO 27001 should be accompanied by a broader action. Often there is a dormant ISO 9001 that should be reinstated. Otherwise, for companies with a particularly customer-oriented business, ISO 27001 should be seen within a perspective of processes guided by ISO 20000.

In more mature and structured organisations, accustomed to reasoning with concepts driven by governance, for example COBIT, the Information Security Manager might find even more synergistic aspects.

Let's look at an example: we have both ISO 27001 and COBIT 5: it is clear that if you do not know anything about COBIT 5 but you have to obtain certification of the Information Security Management System, the most direct route is obviously not through the adoption of COBIT 5. And it is equally clear that if COBIT 5 has already been adopted, it nevertheless does not replace ISO 27001. Therefore, certification of the ISMS can not be seen as a simple add-on to a system managed with COBIT 5.

But if COBIT 5 gives me a “vision” and “substance” of security, such as process management, if I use COBIT 5 to monitor gaps in my security and therefore the actions for improvement, and if I use COBIT 5 to activate the risk assessment and keep this in line with my business, and allow COBIT 5 to guide me in the organisation, control and evaluation of conformity of my IT processes, even if in a general sense, it is obvious that it will be simpler to achieve the goal of ISO 27001 certification.

This example shows how important it is to have a holistic approach, where among the most important references of knowledge are the standards ISO 27001 and ISO 20000. The latter has been increasingly structured as a standard organisational process, not only specifically related to IT.

In this approach the Information Security Manager can find precise indications on how to plan, operate, which tools to use (check-lists, indicators), and how to monitor and improve the business entrusted to him/her.

In this way, the Information Security Manager can face his/her task with the “end in mind.” We can quote from the famous “The 7 Habits of Highly Effective People” by Stephen Covey who wrote: “It's incredibly easy to be trapped in the wrong activity, a task that exists for its own sake, to work harder and harder to climb the ladder ... If the ladder is not leaning against the right wall, every step we take will only get us to the wrong place faster. We can be very busy, we can be very efficient, but we will also only be effective when we start thinking with the end in mind.”

6.5.1 Setting-up an Information Security Management System

10 steps in 100 days. For those accustomed to the Deming cycle this could be the framework within which we restore the PDCA circle (ref. §6.1.2). For the geometry of a given unparalleled event π, it is less complex if the circle to be built is an Information Security Management System (ISMS) in accordance with ISO 27001. There is no need therefore for $\sqrt{(\pi)}$ but an approach supported by specific policies and a well-structured framework

Taking into account the considerations expressed in the previous paragraph, in the next 10 steps we will follow the approach of ISO 27001, as if in a virtuous spiral where planning (Plan), implementation (Do), control (Check) and improvement (Act) follow one another to fill the system. The human factor, the state of awareness and professionalism are essential here.

6.5.1.1 Step one: together with Management define the security goals resulting from company strategies and according to the constraints of compliance.

This means establishing the criteria in relation to risk assessment together with Management. In other words, the height at which the bar is to be placed must be established in a clear, conscious and shared manner. It is an important decision that may be subsequently revised on the basis of the results of the ISMS but which cannot be ignored at the beginning.

This step is important because this first task will give rise to communication, or rather “the Communication” which will be used to obtain the commitment of senior management, the owners of this decision, to define a high-level policy to manage information security.

The definition and approval of this policy is needed by the Information Security Manager to build an Information Security Management System which is intended to reduce risk, respond to incidents, carry out appropriate checks, ensure legal compliance, etc. regarding the processes of the entire company. If, as a goal, certification of the system as a part or as the whole system falls within company policy, the Information Security Manager will also verify compliance of the system with procedures and certifiable standards.

6.5.1.2 Step two: understand which information is to be protected

What we need to protect is information that has value to the company in relation to business services promised but also as established by Management. The business services and support services should therefore be assessed from different perspectives, economic, public image, legal, etc., At this stage it is good to involve the heads of the departments and define a scale of values to be indicated. Check whether there are functional connections between the services and then, for each service define the relevant information, the classification, location, assets and technologies adopted. Then obtain a map where components are all graded. Finally, define who is the holder / owner / manager of the specific structure (data, machine, technology, etc.).

6.5.1.3 Step three: define the threats, vulnerabilities, impact.

The first part of this step is easy because there is ample literature to be associated with a certain type of property, its threats and vulnerabilities. The second part is much more demanding, the definition of the impacts, which must be in relation to the company environment. We must try to give a credible and understandable value to those who are in charge. An impact of € 5,000.00 is clear to everyone, a "SERIOUS" impact is less so.

6.5.1.4 Step four: analyse and weigh up the risks.

Here an almost dangerous variable comes into play, dangerous because it is a determining factor when estimating the level of risk: probability. It may be useful if before asking when a threat might happen, we ask ourselves if a threat is actually possible. Could the threat appear within the context of reference? Does it actually exist or is it a case study? Does it exist because the ability to implement the threat has been proven? Is there the intention? In other words, is there any reason to assume that someone may have the intention of causing a threat, or that the random possibility of a threat occurring cannot be excluded? Is there experience, a historical memory in a significant passage of time, of the threat occurring? And again, for the company, can that information be a premeditated objective? Without going into any philosophical issues, an approach of this kind will help to distinguish between:

- the possibility: this refers to the existence of something in an absolute sense. This is qualitative and the answer to the question "Is it possible?" can only be Yes or No.
- the probability: this refers to the existence in a relative sense and is quantitative; to the question "is it likely?" Yes or NO is not a sufficient answer because we will immediately want more information, "How likely is it?" And this response greatly influences the risk estimate.

Another important element at this stage, which will be crucial for the practical actions to be implemented, is that the risk scenario is described and made clear in the least academic way possible, in a manner appropriate to the reality of the company. This allows communication, from which real feedback can be obtained Communication should not be a final fact (I carried out the analysis and here are the results) but a dialogue (in the form of an interview) with process managers together with the analysis.

6.5.1.5 Step five: inform, raise awareness and train

In the first 100 days we must focus on informing, ideally before asking. We have to work to convince sponsors of the importance of ensuring information security, and that this is essential to good business.

6.5.1.6 Step six: understand the situation.

This is a question of assessing the degree of maturity and application of the organisational and technical countermeasures deemed necessary by the company. Given the tactical approach already in place, envisaging a quick assessment, it is then possible to evaluate whether this activity should be integrated with tools and methodologies that allow the reproduction and comparison of results over time: in this sense, ISO 27002 and Table D.1 (Classification of controls) of ISO 27006 may be useful as guidelines.

6.5.1.7 Step seven: manage the risk.

In normative terms, we should say “deal with the risks” but the ideal approach here is to try to work within a framework of developing opportunities rather than constraints or prohibitions. The Information Security Manager must be convinced and must convince others that managing risk creates value for the company, and therefore should act with this objective in mind. Identifying the correct countermeasures to allow maximum risk, without exceeding the limits set by the ISMS. This is the effectiveness of Management System implementation.

6.5.1.8 Step eight: measure.

We have already mentioned the strategy in detail during the “tactical” phase of the Information Security Manager. Each activity carried out should be measurable and measured in order to gauge whether security requirements are met. Furthermore, these measurements will provide an objective parameter for reporting to management and for involving them in the most important choices that will need the maximum consensus and shared responsibility within the company. In addition to the parameters specified in detail in the “essential issues” (§6.4), the standard ISO 27004: 2009 could prove a useful guideline.

6.5.1.9 Step nine: keep track of security-related events and show an ability to respond to incidents.

Effective incident management procedure and possible corrective actions must be based on and refer back to the risk assessment, where the threats are identified. Feedback is crucial for the improvement.

6.5.1.10 Step ten: review.

Not a one-off event but an open and ongoing discussion involving management and process managers as a method of monitoring, of sharing the effectiveness and alignment between the ISMS and the business strategies.

The review should serve not only to report on the situation but also to ensure system continuity. It is the virtual closing of the circle of continuous improvement, and starting again from a higher point, it is renewing the proven (by results) commitment of senior management (§6.7).

6.6 Training and awareness- raising

Training and awareness is critical in ensuring that all staff are able to carry out their activities safely, while understanding and applying company policies.

6.6.1 Training

Training is mainly aimed at technical staff. In a typical company, many specialised activities, including those which are security-related, are outsourced. In this case it is not so important that internal staff have detailed expertise on issues that will actually be managed by suppliers. It is more important that staff are able to govern and manage IT security, and therefore have a broad understanding of the overall issues and problems. It is clear that internally managed assets may require a more vertical skill although it is not usually enough to make a proper assessment, for example, of risks related to new threats or of the adequacy of solutions adopted or proposed by suppliers.

Some training may be already defined in the early days, but most training activities should act as a support to the planned measures, and therefore be scheduled together with or after other ISMS activities.

It is important to remember that there are now numerous channels available for training which is not carried out in a classroom, such as webinars and other on-line training methods. Although they can be less effective than classroom training, they are definitely an effective way of dealing with general themes that do not require in-depth study sessions or of providing an overview of a topic to then assess the need for more traditional training. The cost of these is also considerably lower, and therefore will be less likely to be cut for budgetary reasons.

It is also possible to schedule a method of verifying the acquired skills[5], enabling the company to measure the effectiveness of investments made.

It is also useful to remember that in some companies, usually depending on the availability of human resources, training funds from business associations also exist (e.g.. the Italian associations Fondimpresa Confindustria) to be distributed according to precise rules but often compatible with the requirements that we are illustrating here.

6.6.2 Raising awareness

In a medium-sized company, generally less structured than a larger one, the effectiveness of the security mechanisms is particularly linked to the cooperation of the staff and management. The review process of security management can be a good opportunity for initiating activities aimed at raising awareness, with the dual purpose of increasing the effectiveness of interventions and generating more support for the business. For this reason, it may be useful to start an awareness raising activity in the early stages of the project, limited to the more general themes, or as soon as company policies are clear enough for them to be communicated effectively.

The success of an awareness-raising activity depends largely on the ability to convey a message that can be effectively implemented by staff. For this reason, it is not enough simply to use the material available on the Internet[6]here the message must be adapted to the company, interacting with staff to verify its effectiveness. Exercises can also be useful (e.g. sending spear phishing messages) and short sessions for clarifications with company personnel. The awareness raising activities will need to be repeated periodically; effectiveness can be assessed on the basis of user behaviour on the occasion of threats, for example, the reporting of suspicious mail, or exercises.

Training and awareness- raising is dealt with in section A.8.2.2 of the standard ISO / IEC 27001.

6.7 Reporting on the 100 day results

Here we are almost at the finish line of the one hundredth day. It is time to assess our work, collect ideas and report the activities, achievements and future plans to senior management.

Regardless of the tool that will be used to prepare our report (word processor, presentation program, etc.) we must keep in mind that, in order to create an effective report, it is important to be clear about what you want to say so as not to risk providing inaccurate or unsupported information, which would have a significant negative impact on our personal and professional credibility. It is therefore necessary to carefully consider the matters to be discussed and messages to be transmitted in order to organise our information according to the criteria of credibility and reliability.

[5] For example, Stanford University has produced on-line introductory encryption seminars which include tests during lesson time and final exams; courses such as these, completely free of charge, can be easily followed subject to availability of staff time. https://www.coursera.org/crypto/auth/welcome

[6] See for example the ENISA website, http://www.enisa.europa.eu/activities/cert/security-month

When we are ready to prepare the so-called “report” for senior management, one of the main aspects requiring careful consideration and evaluation does not, as one might expect in the first instance, refer to the contents (results, “technicalities”, strategies, timelines, etc.) of the report itself, but rather the techniques and language that we will use to illustrate the results of our work.

Language and presentation technique must be such that it allows us to convey what we want to communicate in a direct and clear manner, without the risk of being misconstrued or, worse still, being misunderstood by our stakeholders.

Using terms, indicators or information which are unclear or not “directly intelligible” to the those representing management is likely to create confusion, divert attention and reduce the level of interest in what you want to communicate, detracting from the importance and benefits of what has been done and ultimately risking the invalidation of all the efforts made in these first 100 days, however significant and effective they may have been

The evaluation of our work and consequently of our professionalism, as simplistic as it may seem, will not fall foul of an estimate of the day-to-day activities or objectives, which have been more or less laboriously achieved in this short period of time, but will be based almost exclusively on how we can make people understand (and appreciate) our efforts via the report to be prepared and presented to senior management.

It is therefore appropriate to produce indicators, data and information in a “language” which is familiar and easily assimilated by our interlocutors in order to focus their attention on issues that from time to time we will be illustrating. This will give us two different results, firstly actively involving them and secondly enabling them to immediately appreciate the value that has been added to the business (direct or indirect) as a result of the actions carried out.

To give a practical example of the importance that technique and language play in the preparation and presentation of a report, we consider the case of having to illustrate to a business-focussed management the added value of a new policy and new solutions implemented in order to fight malware. In this specific case, the preparation of a “technical” report, which illustrates a myriad of numbers (typically represented by the number and/or the trend of incidents resulting from malware) associated with names, most of the times unpronounceable (typically names of servers, clients, and/or otherwise of the various types of equipment in the IT infrastructure of the company) will simply confuse everyone. Yes, everyone - including us - as, at best, we would find ourselves in the position of having to explain why there are still a large number of incidents, why one server has been victim of more incidents than another device, why despite the “huge” investments made there are still so many infections, etc. It is obvious that reporting methods such as these will hardly help others perceive the contribution we have made to the company by wisely setting up anti-malware tools. To achieve this goal, we must ensure that the messages to be communicated to our stakeholders are, as we said, in a “language” they understand, or in this case, in a “business” language. With this premise in mind we will have to identify those indicators which, by their very nature, will be intelligible and able to give an equally clear perception of how security has actively contributed to the overall improvement of business performance. With regards the present case, by way of example and without limitation, certain indicators may be of interest, in percentage terms or in absolute value:

- Reduction in security operating costs
- Reduction in IT operating costs
- Reduction in the downtime of services / critical business data
- Increase in the overall performance of the company
- Lowering of some of the most relevant security risks

A further point to be considered, and one which is almost obvious in its simplicity, is the purpose of the final report. The report has the ultimate purpose of transmitting information or providing information on a certain topic. To be effective it must be ordered, otherwise what we say may well be interesting and correct but our stakeholders will most likely have great difficulty in understanding the sense of the report, in grasping the messages it contains, potentially undermining what has been done so far.

Once we have established the language and technique to be used to convey these messages, we need to define the logical path that will make our report effective, and that will illustrate the results obtained in a manner that is:

- ordered
- direct
- clear
- brief
- complete
- objective (as far as possible)

In defining this type of path we must not make the mistake of assuming our audience's knowledge. Having controlled security for 100 days, we are aware of every tiny aspect which relates to the objectives, the analyses carried out, the activities implemented, the problems faced and the results achieved, but the same cannot be said of a management representative who, after having assigned this task more than three months ago will have moved on and focused on his/her own tasks, and must now be provided with a report on what has happened in that period of time. This does not mean that we need to prepare a detailed list of what has happened; more simply, we need to focus on significant events, which if not disclosed immediately, could lead to distractions or misunderstanding.

When drafting the contents of the sections identified we can use the following basic rules:

- use an appropriate style, or rather a style which is suitable for both the content and the recipients;
- use precise language which can be easily understood;
- use linear sentences, avoiding too many subordinate clauses;
- use adverbs and abstract words sparingly;
- avoid rambling;
- use charts and tables in moderation;
- only use technical terms if the report is destined for those familiar with the field.

Finally, when organising information and data that will form the core of our report, it is advisable to group arguments and information in sections so that the order of the presentation can be quickly modified without running the risk of having to revise parts of the report several times. By way of example but without limitation, the following sections could be identified:

- “Introduction”: providing an example of the information helping you to introduce precisely the topics covered in the rest of the report
- “Context”: showing information and data which can give a brief representation of the starting point in a clear and concise manner. The contents of this section are none other than a summary of the results of the analysis carried out on the information gathered with the quick assessment (ref. §6.3.1).

- "Objectives": in which we concisely illustrate our set objectives in the short, medium and long term. It should be noted that the objectives in question must originate from sharing the actions identified at the end of the feasibility study with the senior management. These actions will include the organisational, procedural and technological interventions to be implemented to improve the overall level of security of the company (ref. §6.3.2.1).
- "Lines of action and intervention plan": where we illustrate the lines of action which have already been shared with senior management and the intervention implementation plan (organisational, procedural and technological) to be put in place in order to reach the objectives outlined above. In this section, particular emphasis will be given to the metrics identified in the course of the analyses carried out. Metrics, in fact, serve to support the security manager and management in the subsequent process of assessing the adequacy of security initiatives implemented with regards to predefined targets. Furthermore, the use of metrics allows the company to assess the functions gained from investments and provides quantifiable data that can be used as a support for future investments (for a further discussion on security metrics refer to the document "ROSI v2.0").
- "Approach": in which the methodological approach used, or that will be used, is illustrated in order to identify the objectives set and, more generally, management methods in a time of security. In this section, we will illustrate, in brief, the PDCA approach (ref. §6.1.2)
- "Points of focus": to illustrate and share the critical, organisational and/or technological, aspects which may jeopardize the successful implementation of the action lines and, ultimately, the achievement of goals. The purpose of this section is to obtain the necessary commitment from senior management and the necessary resources to address the critical issues which have been highlighted.
- "Results": this sets out the main results achieved in the first 100 days of operation. In this section we can illustrate the benefits obtained following the implementation of QuickWin identified at the end of the phase for defining lines of action (ref. §6.3.3)
- "Next Step": providing a summary of the actions to be undertaken in the medium term.

Finally, be sure that some simple tips, along with your experience and professionalism will enable you to overcome your hesitation when you first meet with senior management, all that remains for us to do, is wish you....a hundred more days like this !

7. ANNEXES

7.1 Brief overview of international security standards

Standards governing the area of ICT security are so great in number that it would be impossible to consult them all. For this purpose, we recommend a reference document produced by the European Network and Information Security (http://www.enisa.europa.eu/) entitled:

Shortlisting network and information security standards and good practices
Version 1.0, January 2012

This document, free to download from the ENISA web site, in fact contains a list of the main Standards and Good Practices and is structured as follows:

- it is produced by a European Community authority and thus also constitutes a reference for Italian companies;
- it is sufficiently up-to-date (January 2012) with periodic integrations and amendments envisaged;
- it also provides statistics on use;
- it contains direct links to a multitude of freely downloadable material.

Some of the standards worth the special attention of the Information Security Manager include:

1. ISO/IEC 27001/2 [I23, I24]
2. ISO/IEC 24762:2008 Guidelines for ICT and disaster recovery services [I12]
3. ISO/IEC 27005 Information security risk management [I25]
4. ISO/IEC 27011 Information security management guidelines for telecommunications [I26]
5. BSI BS25999-1 Business Continuity [I10]
6. ITU-T X.1051 (02/2008) [I29]
7. ITU-T X.1056 (01/2009) [I18]
8. ITU-T X.800 (1991) [I21]
9. ITU-T X.805 (10/2003) [I31]
10. ISF Standard of Good Practice 2007 [I34]
11. CobiT [I27]
12. ITIL Service Support [I15]
13. ITIL Security Management [I15]
14. IT-Grundschutz-Kataloge [G10]
15. KATAKRI (FI) [G5]
16. NIST SP 800-34 [G29]
17. NIST SP 800-61 [G30]
18. FIPS-200 [M50]
19. UK NICC Minimum Standard ND1643 [M46]
20. PCI DSS 1.2 [I28]

The ENISA site also provides other updated information on information security, such as lists of the main threats, security trends, etc.

8. AUTHORS AND CONTRIBUTORS

8.1 Team leaders and editors

Luca Bechelli, CLUSIT - Freelancer - member of Clusit Management and Technical/Scientific Committee

Jonathan Brera, KPMG Advisory – Manager Information Risk management. CISA, CISM, CRISC, L.A.ISO27001, L.A. BS25999 / ISO22301, Prince2 Foundation, member of ISACA and AIEA

Andrea Mariotti, Ernst & Young - Director IT Risk & Assurance Services, CISA, CISM, CRISC, Lead auditor ISO27001, Lead Auditor ISO20000, member of AIEA and AIPSA

Claudio Telmon, CLUSIT - Freelancer - member of Clusit Management and Technical/Scientific Committee

Alessandro Vallega, Oracle - Security Business Development Manager, member of Clusit Management Committee, Coordinator of Oracle Community for Security

8.2 Authors and contributors

Riccardo Abeti, Studio Legale Abeti - Member of Executive Committee and Chairman of Commission “New Technology, Personal Data and Communication Law” of the European Lawyers' Union. Specialist in the law of new technologies.

Roberto Anzanello, AUSED / Electrolux IT Solutions - Technical specialist IT Security Infrastructure Team EMEA

Orlando Arena, SafeNet - Regional Sales Director, Italy, Malta, Greece & Cyprus

Pasqualino Baldassarre, NexSoft - ITC System Integrator - Project Area Manager

Massimo Bazzani, Alfa Group - Delivery Manager in SEC Consulting, Security Division of ALFA GROUP

Bruno Bernardi, CSQA Certification - Manager of Technologies and ICT Security Division

Angelo Bosis, Oracle - Sales Consulting Senior Manager

Riccardo Canetta, SafeNet - Regional Sales Manager, Italy

Paolo Capozucca, SEC Alfagroup - CEO of SEC Consulting, (Security Division of ALFA GROUP) Italian associate of COMSEC, Member of AIEA, Milan chapter of ISACA, member of CLUSIT.

Andrea Castello, CSQA Certification - Manager of Certification schemes, Technologies and ICT Security Division

Giuseppe Cusello, Alfa Group - Presale Manager in SEC Consulting, Security Division of ALFA GROUP

Alfredo Esposito, Infocert - Information Security Manager

Sergio Fumagalli, ZEROPIU - VP, marketing, external relations and partnerships. Manager of consultancy services on Privacy, co-author of “Privacy guida agli adempimenti” (Privacy: a guide to requirements), Ipsoa 2005

Francesca Gatti, AUSED - CISA, CGEIT, AUSED Management Council, Coordinator of Security and Compliance Observatory of AUSED.

Martina Girolimetto, CSQA Certification - Marketing & Communication

Andrea Goisis, ZEROPIU - Advisory & Presales Specialist

Vito Guerriero, KPMG Advisory - Project Leader, Information Risk Management. CISA, CRISC, L.A.ISO27001, CobiT 4.1 Foundation, ITIL v.3 Foundation, Prince2 Foundation, member of ISACA and AIEA

Andrea Longhi, Management consultant - Security Governance, Business Continuity, Risk Management, Compliance. LA ISO27001, CSA member

Roberto Obialero, ADS - Automated Data Systems - Business Development IT Security & Infrastructures, GCFA, GCFW

Alessio Pennasilico, CLUSIT - Security Evangelist @Alba S.T., Managerial and CTS Clusit, Managerial AIP.

Alberto Piamonte, AIEA - IT Governance Methodologies, COBIT5. AIEA councillor and Research Director.

John Mario Ramaioli, Banca Popolare di Milano - Information Technology Management, Manager of Security and Operative Continuity Area. Abilab Board of Directors

Enrico Ronchetti, Kelyan - Database Architect & Data Security Architect

Giuseppe Russo, Oracle - Chief Technologist and Security Top Gun, Oracle Italia

Marco Sanseverino, KPMG Advisory Senior Security Consultant, Information Risk Management CISSP, L.A.ISO27001, CobiT 4.1 Foundation

Fabio Saulli, BSC Consulting - Business Unit Manager IT Security Area

Giulio Spreafico, AIEA - Engineer, IT Governance consultant, Security, Business Continuity and Privacy, certified CISA, CISM, CGEIT and CRISC by ISACA, IS Auditor and AIEA instructor.

Vittorio Torre, NexSoft - IT GRC Manager. CISSP, CISA, ISO 27001 LA

Maria Cristina Vicini, BSC Consulting - Northern Area Manager, expert in Digital Identity, Database Security, DLP, Mobile Security, Privacy and other issues in the Information Security area.

Proofreading by **Claudio Telmon**

The first 100 days of the Information Security Manager

http://100days.clusit.it | Licence CC BY-SA 3.0 IT

Oracle Community For Security