Cesare Gallotti

Information security

Risk management
Management systems
The ISO/IEC 27001:2022 standard
The ISO/IEC 27002:2022 controls

January 2026 version

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

Contents

Introduction ix

Acknowledgements xi

1 Introduction 1

I The basics 5

2 Information security and organization 7
2.1 Data and information 8
2.2 Information security 9
2.2.1 Confidentiality 9
2.2.2 Integrity 10
2.2.3 Availability 10
2.2.4 Other security properties 11
2.2.5 Impacts on CIA parameters 11
2.3 IT security and cybersecurity 12
2.4 Organization, processes, and functions 14
2.4.1 Processes 14
2.4.2 Functions 15
2.5 Processes, products, and people 16

3 Information security management systems 17
3.1 Management system 18
3.2 Information security management system 18
3.3 Certifications 19

II Risk management 21

4 Risk and risk assessment 23
4.1 What is risk 24
4.1.1 Positive and negative risks 24
4.1.2 Risk level 25
4.2 What is risk assessment? 27
4.3 Methods of risk assessment 30
4.3.1 Validity of the approach 30
4.3.2 Risk assessment software programs 31

4.3.3 Warning . . . 32
4.4 Who to involve . . . 33
4.4.1 Risk owner . . . 33
4.4.2 Facilitators . . . 34
4.5 Risk management documents . . . 34

5 Context and scope **35**
5.1 Context . . . 35
5.2 The interested parties . . . 38
5.3 The scope . . . 39

6 Risk identification **41**
6.1 Assets . . . 41
6.1.1 Information . . . 42
6.1.2 Other assets . . . 43
6.1.3 Who identifies assets . . . 44
6.2 Threats . . . 46
6.2.1 Threat agents . . . 47
6.2.2 Threat techniques . . . 49
6.2.3 Threats and the privacy risk . . . 50
6.2.4 Who identifies threats? . . . 51
6.3 Associating threats to assets . . . 51
6.4 Associating threats to consequences . . . 52
6.5 Vulnerabilities and information security controls . . . 52
6.6 Associating vulnerabilities with assets . . . 53
6.7 Associating vulnerabilities, controls and threats . . . 54
6.7.1 Alternative, compensatory, complementary, and aggregated controls . . . 55
6.7.2 Prevention, detection, and recovery controls . . . 56
6.8 Conclusion . . . 56

7 Risk analysis **59**
7.1 Methods of analysis . . . 60
7.1.1 Quantitative methods . . . 60
7.1.2 Qualitative methods . . . 61
7.2 The value of assets . . . 61
7.2.1 Evaluating information . . . 62
7.2.2 Evaluating others asset . . . 65
7.3 Evaluating the likelihood of threats . . . 67
7.3.1 What values to assign to threats . . . 68
7.3.2 Additional considerations . . . 69
7.3.3 Who assigns values to threats? . . . 70
7.4 Inherent risk . . . 70
7.4.1 Inherent quantitative risk . . . 71
7.4.2 Inherent qualitative risk . . . 72
7.5 Evaluating vulnerabilities and controls . . . 74
7.5.1 Identify ideal controls . . . 75
7.5.2 What values to assign to the controls . . . 76
7.5.3 Who assigns values to the controls? . . . 80
7.6 Risk level . . . 81

7.6.1 Quantitative risk level 82
7.6.2 Qualitative risk level 83
7.6.3 Conclusions 84
7.7 Further thoughts on aggregations 85

8 Risk evaluation 87

9 Risk treatment 91
9.1 Risk treatment options 91
9.1.1 Avoiding or eliminating risk 92
9.1.2 Increasing risk 93
9.1.3 Changing the likelihood of a threat (Prevention) 94
9.1.4 Changing the consequences (Recovery) 94
9.1.5 Sharing the risk 94
9.1.6 Retaining the risk (Acceptance) 95
9.2 The risk treatment plan 96
9.3 Choosing and implementing mitigating actions 96
9.3.1 Reviewing the action plan 96
9.3.2 The action plan 99
9.3.3 Effectiveness of actions 100
9.3.4 Monitoring the action plan 100

10 Risk monitoring and review 101
10.1 Operational risk assessment 101
10.2 Project risk assessment 102
10.3 Integrating risk assessments 103

III Information security threats and controls 105

11 Threat techniques 107
11.1 Intrusion into a site or premises 107
11.2 Intrusion into IT systems 108
11.3 Social engineering and frauds 110
11.4 Identity theft 112
11.5 Damage to physical equipment 112
11.6 Damage to IT programs 114
11.7 Theft of IT devices or physical equipment 115
11.8 Reading, theft, copying, or modification of documents on physical supports 115
11.9 Interception of electromagnetic emissions 116
11.10 Interference due to electromagnetic emissions 116
11.11 Reading or copying of IT documents 117
11.12 Unauthorized modification of digital documents 118
11.13 Processing of information against regulations 119
11.14 Malware 120
11.15 Copy and illegal use of software 121
11.16 Unauthorized use of external IT services 122
11.17 Unauthorized use of IT systems and services offered by the organization 122

11.18Information retrieval . . . 123
11.19Exhaustion or reduction of resources . . . 123
11.20Interception of communications . . . 125
11.21Sending data to unauthorized people . . . 126
11.22Sending and receiving inaccurate data . . . 127
11.23Repudiation of messages and documents by the sender . . . 128
11.24IoT, OT, IIOT . . . 128
11.25Artificial intelligence . . . 129

12 Information security controls 131
12.1 Documents . . . 132
12.1.1 Types of documents . . . 132
12.1.2 How to write documents . . . 135
12.1.3 Approval and distribution . . . 136
12.1.4 Archiving records . . . 137
12.1.5 Retention time . . . 138
12.1.6 Verifying and updating documents . . . 138
12.1.7 Documents of external origin . . . 139
12.2 Information security policies . . . 139
12.3 Organization for information security . . . 141
12.3.1 Organization . . . 141
12.3.2 Segregation of duties . . . 144
12.3.3 Project management . . . 145
12.3.4 Contacts with the authorities . . . 146
12.3.5 Threat intelligence . . . 147
12.4 Personnel management . . . 147
12.4.1 Personnel induction . . . 148
12.4.2 Termination and change of employment . . . 149
12.4.3 Competence and awareness . . . 149
12.4.4 Offsite work . . . 152
12.5 Asset management . . . 153
12.5.1 Information assets . . . 153
12.5.2 Asset identification, inventory and ownership . . . 157
12.6 Access control . . . 159
12.6.1 Credentials and identification . . . 160
12.6.2 Authentication . . . 160
12.6.3 Authorizations . . . 166
12.7 Cryptography . . . 172
12.7.1 Symmetric and asymmetric algorithms . . . 173
12.7.2 Hash functions . . . 174
12.7.3 Cryptographic protocols . . . 174
12.7.4 Cryptographic keys . . . 174
12.7.5 Legislation applicable to cryptography . . . 175
12.8 Physical security . . . 175
12.8.1 Site security . . . 175
12.8.2 Device security . . . 179
12.8.3 Physical archives . . . 183
12.9 Information systems operations . . . 184
12.9.1 Documentation . . . 184
12.9.2 Device and system configuration . . . 185

12.9.3 Change management 186
12.9.4 Malware 198
12.9.5 Backups 200
12.9.6 Logging and monitoring 202
12.9.7 Capacity management 206
12.9.8 Personal and portable devices 206
12.9.9 Data deletion 208
12.10 Communications security 209
12.10.1 Authorized services 209
12.10.2 Network segmentation 212
12.10.3 Network security 216
12.10.4 Exchanging information 218
12.11 Development and maintenance of IT systems 222
12.11.1 Acquisition of IT systems 223
12.11.2 Internet of things 224
12.11.3 Artificial intelligence 224
12.12 Supplier management 226
12.12.1 Agreements and contracts with suppliers 227
12.12.2 Selecting suppliers 229
12.12.3 Monitoring suppliers 230
12.12.4 Cloud computing and suppliers 231
12.12.5 ICT product acquisition and the outsourced software development 231
12.12.6 Insurances 232
12.13 Incident management 233
12.13.1 Roles and procedures 233
12.13.2 Incident management process 234
12.13.3 Incident management test 238
12.13.4 Vulnerability handling 239
12.13.5 Problem management 241
12.13.6 Crisis management 242
12.13.7 Digital forensics 243
12.14 Business continuity 244
12.14.1 Business impact analysis (BIA) 246
12.14.2 Business continuity risk assessment 247
12.14.3 Recovery objectives and strategies 247
12.14.4 Continuity plans 251
12.14.5 Testing and maintenance 252
12.15 Compliance 253
12.15.1 Current legislation and regulations 254
12.15.2 Contracts 261
12.15.3 Audit 261
12.15.4 Vulnerability assessment 263
12.15.5 Management system review 265

IV Requirements for an information security management system 267

13 ISO standards and the HLS 269
13.1 Specifications and guidelines . . . 269
13.2 The standards related to ISMS . . . 270
13.3 ISO/IEC 27701 . . . 271
13.4 The HLS . . . 271
13.5 History of ISO/IEC 27001 . . . 272
13.6 How does standardization work? . . . 274

14 Continuous improvement and the PDCA cycle 275
14.1 Continuous improvement . . . 275
14.2 The PDCA cycle . . . 276
14.2.1 Plan . . . 277
14.2.2 Do . . . 277
14.2.3 Check . . . 278
14.2.4 Act . . . 279
14.2.5 The fractal nature of PDCA cycle . . . 280

15 System requirements 283
15.1 Scope of the standard . . . 283
15.2 Normative reference of ISO/IEC 27001 . . . 284
15.3 Terms and definitions of ISO/IEC 27001 . . . 284
15.4 Context and scope of the ISMS . . . 284
15.4.1 The context of the organization . . . 284
15.4.2 The scope of the ISMS . . . 285
15.4.3 Information security management system . . . 287
15.5 Leadership . . . 287
15.5.1 Information security policy . . . 287
15.5.2 Roles and responsibilities . . . 288
15.6 Planning . . . 288
15.6.1 Management system effectiveness risks . . . 289
15.6.2 Information security risk assessments . . . 291
15.6.3 Information security risk treatment . . . 292
15.6.4 Actions . . . 294
15.6.5 Objectives . . . 296
15.6.6 Planning of changes . . . 302
15.7 Supporting processes . . . 302
15.7.1 Resources . . . 302
15.7.2 Competence and awareness . . . 303
15.7.3 Communication . . . 304
15.7.4 Documented information . . . 304
15.8 Operations . . . 305
15.8.1 Planning and controlling the operational processes . . . 305
15.8.2 Evaluating and managing risk related to information security . . . 306
15.9 Performance evaluation . . . 306
15.9.1 Monitoring, measurement, analysis, and evaluation . . . 306
15.9.2 Internal audits . . . 311

15.9.3 Management reviews 315
15.10 Improvement 316
15.10.1 Nonconformities 316
15.10.2 Corrective actions 319
15.10.3 Preventive actions 320
15.10.4 Continuous improvement 320
15.11 Annex A of ISO/IEC 27001 321
15.12 Bibliography of ISO/IEC 27001 321

V Appendixes 323

A Auditor management 325
A.1 The auditor is a guest 326
A.2 The auditor is a partner 327
A.3 The auditor is a supplier 328
A.4 The auditor is an auditor 328

B The first steps to implementing an ISMS 331
B.1 Identify the scope 331
B.2 Involve the managers 332
B.3 Manage documents 332
B.4 Improvement 332
B.5 Train the staff 332
B.6 Gap analysis 333
B.7 Implement the management system 333

C The management system certification 335
C.1 Actors 335
C.2 Path to certification 336
C.2.1 The contract 336
C.2.2 The certification audit 337
C.2.3 Recommendation and certificate issuance 337
C.2.4 Extraordinary audit 337
C.2.5 Periodic audits 337
C.2.6 Re-certification audit 338
C.3 Calls for tenders 338
C.4 Sector-specific standard certification 338
C.5 Privacy certifications 339
C.6 Accreditation for the management system certifications 339
C.7 Laboratories certification and accreditation 340
C.8 Product, services and processes certification 340
C.8.1 Certifications of personal data processing 341
C.8.2 Trusted service certification 341
C.8.3 Data center certification 341
C.9 Common Criteria (ISO/IEC 15408) 342
C.10 The myths of certification 344

D Change management requirements **345**
D.1 Functional requirements for access control 345
D.2 Connectivity requirements 346
D.3 Functional requirements related to cryptography 346
D.4 Monitoring requirements 347
D.5 Capacity requirements 347
D.6 Architectural requirements 347
D.7 Application software requirements 348
D.8 Service requirements 348

E Requirements for contracts and agreements with suppliers **349**
E.1 Requirements for product suppliers 349
E.2 Requirements for non-IT service providers 350
E.3 Requirements for IT service providers 351

F The ISO/IEC 27002:2022 controls **355**

Bibliography **363**

Introduction

My twenty-five readers may imagine what impression such an encounter as has been related above would make on the mind of this pitiable being.

Alessandro Manzoni, *The Betrothed*

The first version of this book was written in Italian and published 2002. In 2014, I produced a second edition, incorporating ideas developed during training courses, presentations, discussions with colleagues and friends, and meetings held while drafting ISO/IEC 27001:2013. Some views expressed in 2002 evolved through numerous audit and consulting projects.

The third version, featuring the Perito Moreno cover, was a minor update containing a few new examples and ideas that emerged during the development of ISO/IEC 27003:2017. It was translated with the assistance of Maël-G Perrie, who provided excellent work and suggested several technical improvements.

The fourth version, with the Giants of Sila on the cover, was written when the final drafts of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 became available. It was necessary to update descriptions of the information security controls. Additional updates were made regarding available technologies (IoT, OT, artificial intelligence), threats and accreditation schemes. The English version was supported by Simona Chiarelli, who delivered high-quality work, despite the very short timeframe.

This fifth edition, showing the Julian Alps on the cover, has been updated to reflect the entry into force of NIS2, the European Regulation on Artificial Intelligence and new editions of relevant ISO standards.

The first part of this book explains the fundamentals of information security and information security management systems.

The second part describes risk assessment with a balance of theoretical concepts and practical examples; calculations are not required to understand the principles.

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

The fourth part discusses the requirements of ISO/IEC 27001, based on my interpretation informed by committee meetings, training courses, and client discussions.

The early appendices contain short presentations delivered during training sessions.

The subsequent appendices are taken from operational checklists, and the final appendix provides a cross-reference between the ISO/IEC 27002:2022 controls and the related sections of this book.

Although this text relies heavily on ISO/IEC 27001, it is not an official guide for interpreting the standard: for that purpose, ISO/IEC 27003 should be consulted.

This book is designed for readers who wish to learn about information security or deepen their existing knowledge. Over the years, I have tried to answer the many questions I have been asked.

Some ideas may also interest experienced professionals and may serve as starting points for new discussions. Everyone has their own views perspective, and comparing these viewpoints benefits us all.

The book does not cite the standards directly for copyright reasons, and in some cases to ensure the text remains more meaningful and clear.

Some definitions have been modified slightly from the official versions to improve clarity; additions are shown in brackets and deletions are indicated with ellipses.

Acknowledgements

I would like to thank the following people for their support in writing this book. I am proud that they dedicated their time and energy to me.

- Max Cottafavi - a governance, risk, and compliance expert with whom I have exchanged ideas for many years; he reviewed drafts and contributed helpful suggestions;
- Roberto Gallotti - my rigorous proof-reader and source of ideas; although he does not considerd himself an information security expert, he is a professional from whom I would have liked to learn more;
- Stefano Ramacciotti - with whom I discussed information security during SC 27 meetings; he also contributed to parts of the text;
- Monica Perego - the first "plumber of privacy," and one of the most respected privacy consultants; I am honored to consider her a friend, and grateful for her suggestions that improved this book.

I would also like to thank Franco Ruggieri, Pierfrancesco Piastrello, Francesca Lazzaroni and the "Idraulici della privacy" for their valuable discussions and feedback.

For the 2026 edition, I thank Luca Caldarelli, Matteo Celardo, Marco Gemo and Pierluigi Stefli for highlighting errors that have now been corrected.

Stephen Hanson reviewed the English edition. He also gave me lot of new text to provide an improved clearity.

It is our hope that these improvements support both newcomers and experienced practitioners in deepening their understanding of information security and the management system approach on which this discipline is built.

Finally, I would like to thank all clients, colleagues, and participants who have shared ideas, debates and learning experiences over the years. Our field evolves rapidly, and none of us holds all the answers.

Contacts

Please visit https://www.cesaregallotti.it to report errors or suggest improvements.

For my newsletter (in Italian and English), instructions are available on the website. I'm also active on LinkedIn (in English).

Warning

All web links in this book were verified on 20 December 2025.

Chapter 1

Introduction

What [...] there was to be interpreted in "Play nice"?

John Nive, *The second coming*

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

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

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

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

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

As you can see from this simple example, security is never absolute. Fort Knox is not resistant to a large meteorite.

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

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

the second part of the book.

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

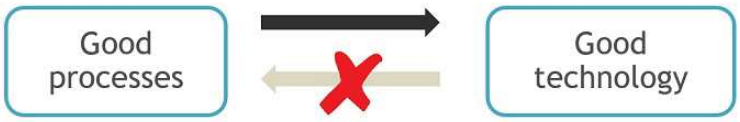

Figure 1.0.1: Processes and products

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

A bit of history

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

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

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

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

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

2. the increase in people and connecting devices over the Internet (itself not designed for security [144]);

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

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

5. the use of more and more suppliers and increasing relations with external actors.

All these events increased awareness of information and computer security.

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

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

Methodologies and practices for information security were introduced to help companies. Among the most important initiatives are those related to IT products and systems security (COSEC of 1983, ITSELF of 1991, Common Criteria of 1994 and the NITS Special Publications[1] issued since the early 1990s), information security (BS 7799 of 1995, whom history will be the subject of section 13.5) and information security risk assessment methodologies (CRAM of 1987, Marion of 1990 and Mehari of 1995) [26].

In the years 2000, many Countries promoted initiatives for the IT networks and Internet security (and spread the terms *cyberspace* and *cybersecurity*). Initially, the USA issued important legislation (it is important the Cybersecurity and Infrastructure Security Agency Act dated 2018), started specialized agencies (in 2018 was born the Cybersecurity & Infrastructure Security Agency, but previously operated the NITS and the NSA) and programs for reducing the IT risks in the critical infrastructures (in 2013 started the work for the publication of the NITS Cybersecurity Framework). Later, other Countries followed the example; the EU, that already created in 2004 the ENISA (European Network and Information Security Agency, today European Union Agency for Cybersecurity), approved the NIS Directive in 2018 and the Cybersecurity act in 2019.

On the other hand, the citizens rights in the digital world were considered more and more important. In this case, the EU was usually the first promoter with the Privacy Directive in 1995, followed by the GDPR in 2016 (see paragraph 12.15.1.9) and followed by many Countries, China included. The EU started in 2018 the "New Deal for Consumers", for improving existing legislation, e.g. for the e-commerce and the protection of consumers. Other initiatives considered the IT security for products, including medical devices and machinery.

These norms usually require to the organizations to assess the information security risks and treat it with adequate security controls. This approach improves the information security in general, but also increased the bureaucratic burden on many organizations.

In the same years, an additional novelty was prominent and it includes Internet of Things (IoT), Operational technology (OT) and home automation. It is the digitalization and connection to Internet of devices and tools, more and more copious, with limited capabilities, but it is usually connected to complex ICT networks and with active wi-fi connections. Nowadays, these devices are everywhere: in homes and offices with smart TVs, "smart" home appliances, equipment (in many cases used for the safety of people), plants, gas, power and water distribution networks, transportation, roads and railways. The list is endless and includes technologies very different from each other. For the ease of connection, low costs and diversity of technologies, these devices are hardly controllable by organizations.

It is in this context that the security widened its scope. Now it is not only for the security of information, but for all the devices that can be attacked with

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

IT tools. These devices are very important for productivity, but very difficult to configure and very easy to attack. Potential impacts are no more on information, but on the physical security, the safety of people, the quality and availability of products in the manufacturing sector and the reliability of several services.

Since 2020, organizations must also take care of the high number of people that work remotely. This has impacts not only on information security from a technological point of view, but on the management of work itself.

Another novelty is the growth and availability of the artificial intelligence. This is a tool that needs to be designed so that people and goods are safe. It is a tool that can be used for threatening and for defending IT systems too.

In the 2020s, numerous regulations became applicable especially in Europe, in the wake of the GDPR of 2016. Some examples are the Data Act, the NIS2 and the CER Directives and the AI Act. At the national level, other regulations have been further promulgated, the supervisory authorities in turn regulate and sanction. Standardization bodies continue to publish standards (one of the latest is ISO 56001 on innovation, almost an oxymoron).

Some criticize this approach because it blocks innovation (and the Trump administration in USA tried to withdraw as many regulations as possible); others support it because it protects consumers and nations. Organizations, in all this, must find ways to monitor requests and make their adoption efficient and as useful as possible.

It should be noted that regulatory hypertrophy requires, to implementers and verifiers (e.g. auditors), the availability of numerous skills, often lacking. This is leading to further inefficiencies that will hopefully be resolved in the near future.

Part I

The basics

Chapter 2

Information security and organization

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

Thomas Stearns Eliot, *The rock*

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

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

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

[1] https://en.wikipedia.org/wiki/Library_of_Alexandria.
[2] www.contribuenti.it/cartellepazze/cartellepazze1.asp.
[3] http://edition.cnn.com/2003/WORLD/europe/09/28/italy.blackout/index.html.
[4] news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm.
[5] https://www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak.

- in September 2013, the Alpitour (Italian tour operator) network experienced a breach, and some links were made to redirect to malicious websites[6];
- at the beginning of 2013, Spamhaus' anti-spam services were blocked by an attack[7];
- in the end of 2019, an organization had many of its documents spread in the streets because of a wind blow[8];
- in May 2020, EasyJet was attacked by criminals who stole EasyJet's customers data, including credit card details[9];
- in March 2021, the OVH data centre in Strasbourg was unavailable due to a fire[10];
- in August 2021, the COVID-19 vaccine booking systems of the Lazio region in Italy were unusable for four days because of a ransomware[11];
- in October 2021, Facebook, WhatsApp and Instagram were unavailable for 6 hours due to an incorrect system configuration[12].

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

2.1 Data and information

Before discussing data and information, we'll provide the definition present in previous versions of ISO/IEC 27000. In the latest versions, this definition is no longer reported because you can find it in ordinary dictionaries[116].

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

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

[6] https://securityaffairs.com/18230/cyber-crime/ibm-x-force-2013-mid-year-trend-risk-report.html.
[7] www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.
[8] https://www.linkedin.com/pulse/idiot-wind-attack-cesare-gallotti/.
[9] https://www.bbc.com/news/technology-52722626.
[10] https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU.
[11] https://www.computerweekly.com/news/252505057/Possible-ransomware-attack-hits-Italian-vaccine-booking-system.
[12] https://www.theguardian.com/technology/2021/oct/05/facebook-outage-what-went-wrong-and-why-did-it-take-so-long-to-fix.

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

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

More rigorously, *data* are raw elements—numbers, symbols, or facts—that gain meaning only when processed or interpreted. *Information* is data placed in context, organised in a way that provides relevance and value.

This difference is also evidenced by the representation of the four types of knowledge [105]:

- *data*: this indicates the set of individual facts, figures, sensory impressions, etc.;
- *information*: organized and meaningful data;
- *knowledge*: information received and understood by a single individual;
- *wisdom*: the ability to make connections between pieces of knowledge to enhance decision making.

2.2 Information security

ISO/IEC 27000 [81] provides the following definition.

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

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

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

These are often referred to as *CIA parameters*.

2.2.1 Confidentiality

Some incorrectly equate information security and confidentiality.

Common sayings in ICT include "a secure computer is shut down or, better yet, broken" and "the only truly secure system is powered down, smothered in a concrete block, sealed in a room with walls shielded with lead, and protected by armed guards, and even then, you might have any questions about" [27]. Obviously, this approach doesn't take into account the availability of information.

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

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

Example 2.2.1. In a company, employee information is always controlled, but some people have access to it such as the appointed physician, management, executives, certain public agencies, the accountant, and the legal department.

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

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

Example 2.2.2. The characteristics of a new car model have to be kept confidential. At design time they must be available to designers, at production times to workers, but in the end, when cars need to be sold, information must, albeit partially, be made publicly available.

2.2.2 Integrity

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

Example 2.2.3. Richard Pryor, in 1983's Superman III, manages to steal money from his company after having altered the accounting system.

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

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

2.2.3 Availability

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

Example 2.2.4. The "delay" depends on various factors: milliseconds in the context of equity stock exchange, seconds in the context of an e-commerce website, a few minutes in a bank branch.

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

Example 2.2.5. Backups improve the availability of information, but increase confidentiality risks because data are duplicated and they can be stolen.

2.2.4 Other security properties

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

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

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

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

The *traceability*, that supports the *accountability*, is the possibility to know who has or had access to an information and who modified it. It is possible to see that the data needed for tracing an information must be part of the information itself, thus traceability can be seen as a special case of the integrity.

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

2.2.5 Impacts on CIA parameters

Each event can have an impact on one or more parameters.

Example 2.2.6. Table 2.2.1 links examples of events with CIA parameters.

People may disagree on which parameters can apply to an example. The first thing to determine is whether a parameter is assigned according to the direct or indirect effect of the event: in case of stolen passwords, as happened to Sony in 2011[14], the direct effect only affects confidentiality, but it may later concern integrity (if those passwords are used to modify the data) and availability (Sony had to lock the site for several months).

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

[13] https://www.bbc.co.uk/news/world-europe-27388289.
[14] attrition.org/security/rant/sony_aka_sownage.html.

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

Figure 2.2.1: Events and CIA parameters

2.3 IT security and cybersecurity

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

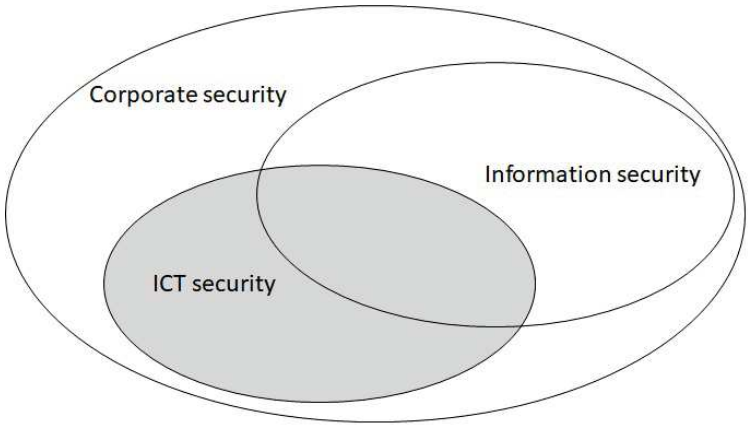

Figure 2.3.1: Information security and ICT security

Example 2.3.1. In 2016 Finland apartments were left without hot water for a week because the heating system had been subject to ICT attack[15].

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

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

Example 2.3.2. In 2021 an unidentified attacker gained access to a water treatment plant's network in Florida (USA) and modified chemical dosages[16].

This attack had impacts on dosages'information, but someone classifies it as relevant for industry security, not information security.

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

Over the years, many have tried to justify the use of the words "cybersecurity" and "cyberspace" in science without finding a shared or rigorous solution, which has spread confusion and false expectations. It is important to understand the key point of the issue: surely cyber-security is about ICT systems, not only the ones that handle actual information (i.e. documents and tables), but also configurations as well. These configurations are very important in many cases: gas and electricity distribution networks, cooling and heating systems, industrial and house systems, et cetera.

A good definition is the following one[17]:

> *cybersecurity*: securing things that are vulnerable through ICT.

This excludes the physical and environmental security for ICT systems.

The definition of the NIST, the institution who made popular the term with its *Cybersecurity framework* o CSF [110] is too generic: "The process of protecting information by preventing, detecting, and responding to attacks". It must also be said that the security measures proposed by the CSF are basic cyber security measures.

Cybersecurity includes the security of:

- *Internet of things* (IoT), including devices used in plants (*Industrial IoT* or *IIoT*) and for home automation;
- *Operational technology* (*OT*), that includes the *industrial control systems* (*ICS*), that includes the *supervisory control and data acquisition* (*SCADA*) used in networks that control electricity gas water and so on distribution networks;
- home automation systems.

In these fields, the term *resilience* is preferred to *availability*, even they are similar, but the latter is used for information and the former for equipment.

Someone includes in the cybersecurity the security on the Internet, including phenomena such as online bullying (*cyberbullying*).

[16] https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/

[17] https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information.

2.4 Organization, processes, and functions

According to ISO standards, we'll use the term *organization* to indicate every form of enterprise, company, institution, association, agency, etc.

Another definition is that of *business*: many standards distinguish between *business activities*, which are those that directly contribute to production or service delivery, and *support activities*. In some texts. the term *business* refers to people who are not involved in the management of ICT systems.

We won't use that term in this book because information security is relevant for both business and support activities.

Organisations operate through processes and functions. Understanding these helps identify where information is created, processed, stored, and transmitted.

2.4.1 Processes

This definition comes from ISO/IEC 27000.

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

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

Example 2.4.1. Consider the process of training staff. The inputs are the training needs and the output is the improvement of the employees' skills.

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

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

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

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

The control can be performed daily by individuals and their managers and periodically through checks or effectiveness and efficiency measurements. The ISO 9000 [69] standard gives:

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

Example 2.4.2. Test results, costs, and manager and trainee satisfaction

can all be used to measure the learning management process.

Characteristics of processes:

- each input is from internal functions or external entities, such as customers, suppliers and partners;
- tools are used for each task in the process (e.g. forms and means of communication for administrative tasks; machines and plants for manufacturing activities; software for computing systems);
- responsibilities are assigned for each task;
- there are established procedures to control the process;
- each process has outputs and each output has recipients, i.e. internal or external functions.

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

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

2.4.2 Functions

An organization is structured into *functions*. Functions describe organisational responsibilities and areas of expertise. Examples include HR, IT, finance, procurement, and operations. Functions are shown in organizational charts.

Processes describe how functions interact with each other or within themselves, as shown in figure 2.4.1.

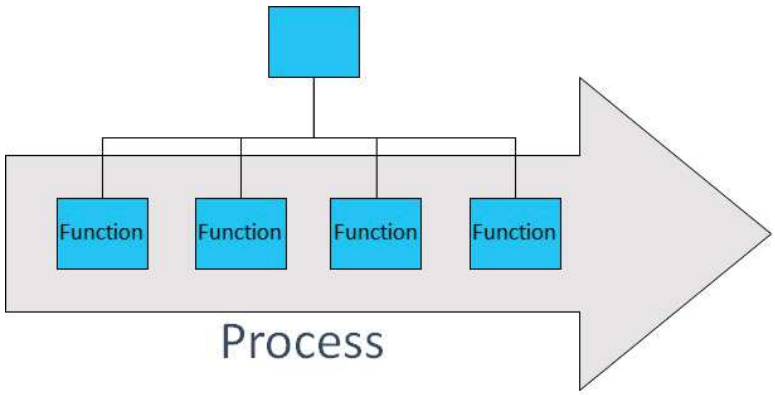

Figure 2.4.1: Process and functions

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

Example 2.4.3. For the training process, impacted functions may include the trainees' manager, the HR office, the finance department, and the purchasing department.

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

2.5 Processes, products, and people

Information security depends not only on technology but also on the interaction between processes, products, and people. Well-defined processes guide behaviour, appropriate products support the processes, and competent people ensure these are executed effectively. Qualified suppliers are always needed. These are the four Ps: processes (or procedures), people, products and partners.

Example 2.5.1. A race car in the hands of a newly-licensed driver wins no prizes and would presumably be dangerous because the driver has poor knowledge of procedures, lacks experience, and probably overestimates his or her abilities.

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

None of the four Ps is the most important: all must participate in a balanced way to achieve the goal.

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

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

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

Chapter 3

Information security management systems

Comme de longs échos qui de loin se confondent
Dans une ténébreuse et profonde unité,
Vaste comme la nuit et comme la clarté,
Les parfums, les couleurs et les sons se répondent

Charles Baudelaire, *Correspondances*

Information security can be achieved by using appropriate organizational processes. Processes are necessary to determine a desired security level, identify deficiencies, decide how to remedy them and with which products, establish deadlines, appoint those responsible for the remedial operations, train staff, and maintain the adopted solutions.

Example 3.0.1. When considering installing turnstiles for access to offices, an organization would try to determine if they provide the intended security level, which technologies to adopt that take into consideration applicable laws and regulations, which vendor to hire for the installation, what kind of contracts would be drawn up regarding maintenance, how to enable and disable employee access, and how to react in case of failure.

Obviously, acquiring good security products does not guarantee the achievement of intended results. There are many cases where tools are purchased but then go unused because they cannot be integrated with systems already in use or because no one is adequately trained to install and maintain them.

These processes are not isolated and independent but are related to and interact with each other.

Example 3.0.2. Returning to the example of turnstiles, it becomes obvi-

ous as more processes interact with each other that risk analysis is required when assessing needs and investing in management and training.

For active turnstiles, even more processes are involved: access control, personnel management to determine who is allowed access, supplier management for maintenance activities, incident management in the event of a fault or alarm, and periodic verification of the turnstiles' suitability.

In this chapter we define *management systems* and *information security management systems*. We also present considerations about their planning and implementation.

3.1 Management system

As mentioned above, these processes are mutually interrelated and interacting, which helps make sense of the following definition from ISO/IEC 27000.

> *Management system*: set of interrelated or interacting elements of an organization to establish policies and objectives and [interrelated or interacting] processes to achieve those objectives.

This includes the need for planning when establishing policies, objectives and processes and when making sure that objectives are being met. Senior management are expected to set policies, objectives, and processes and to be actively involved in their operation and feasibility.

Abandoning theory and switching back to practice, we can say that:

- every organization has a purpose (*mission*);
- an organization's management system is its set of organizational practices (processes) and tools to achieve its purpose;
- these processes and tools are interrelated;
- each organizational change, though potentially small, can have impacts on many areas of the organization itself, its customers, its suppliers, and its partners, due to the interrelationships between processes;
- when implementing changes, their impacts following their planning should be monitored.

3.2 Information security management system

In an organization, not all activities are dedicated to or concerned with information security. In fact, read the following definition derived from ISO 9000.

> *Information security management system (ISMS):* part of a management system with regard to information security.

An organization's management system may also encompass quality, environment, safety, and health of workers.

It is important to define the scope of each management system, their relationships, and their overlaps, to avoid treating unrelated matters or unnecessarily multiplying the efforts.

Example 3.2.1. Information security does not cover, if not marginally, credit risk, corporate brand protection, physical security, or safety of workers. Those are other disciplines, requiring different skills and handled by other management systems.

Fire prevention is a core subject of information security, physical security, environmental protection and worker safety and health. It must therefore be addressed in a manner that avoids doing more work than necessary and ensures that the measures taken suit everyone's needs.

For an ISMS it is very important the role of top management, because it is the owner of ISMS. It must show leadership, use it as a tool to have control over the set of interrelated and interacting elements and ensure it is effective (i.e. achieve the information security objectives).

3.3 Certifications

How can we be sure that appropriate processes have been adopted, that the staff is prepared, and that the products and services used are reliable? Assessments need to be carried out to answer these questions by a third, independent party, in turn controlled by reliable authorities.

Assessments include collecting and analyzing evidence, in order to evaluate it objectively and in compliance with the rules. The end result can lead to certification.

In the context of information security, there are certification schemes for processes (the most important one is based on ISO/IEC 27001 [82], which is more extensively described in Appendix C)), products (most importantly the one based on ISO/IEC 15408, *Common criteria* [71, 72, 73], services and individual [55] certifications.

Certification is meant to reasonably assure that:

- decisions are taken by competent individuals;
- employees use verified and reliable products;
- implemented procedures and processes are reliable.

Only by measuring our confidence in a product, service, person, or process, can we be reasonably certain that things are moving in the right direction.

The certification system has flaws too, the first of which is that certification bodies are paid by the same entities that require certification. The fact remains that these mechanisms contribute to greater security.

Part II

Risk management

Chapter 4

Risk and risk assessment

I'd call that a bargain
the best I ever had.

Pete Townshend (The Who),
Bargain

In this part, we'll explain risk and risk assessment, which will help to decide how to treat it. The stages of risk assessment are shown in Figure 4.0.1 and they are:

1. risk identification;

2. risk analysis;

3. risk evaluation.

Before going through these phases, it is important to understand the *context* and the *scope* in which risk is assessed and then treated. All these phases and the risk monitoring one form the *risk management*. Respectively chapters from 5 to 9 discuss those two stages.

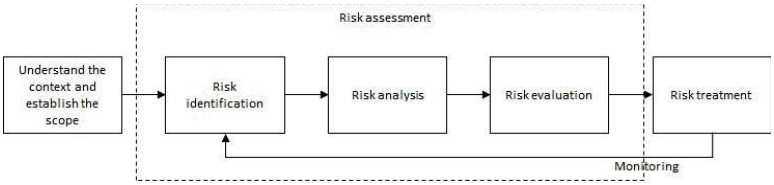

Figure 4.0.1: The stages of risk management

The last chapter of this Part deals with monitoring and re-assessing risk, tasks that are necessary because the risk needs to be managed over time.

4.1 What is risk

To talk about risk assessment and risk treatment, we must first define risk using ISO/IEC 27000.

> *Risk*: effect of uncertainty on objectives.
>
> Note: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Risk is not inherently negative; it includes both threats and opportunities.

In information security, risk concerns the possibility that confidentiality, integrity, or availability may be compromised. Understanding these risks helps organisations determine appropriate controls.

Uncertainty is due to *events*, the consequences of which may be positive or negative.

Some consider *impacts*. They are immediate, like direct costs (see paragraph 7.2.1), while consequences include the short, medium and long term ones. In the risk assessment, it is better to evaluate consequences than impacts.

We can identify the *perceived risk* but not the *actual* one, thus making all assessments automatically subjective. The techniques of risk identification, analysis and evaluation should not try to represent an objective reality but to render the most complete and relevant results that can be reported to other parties.

4.1.1 Positive and negative risks

Risks can generate negative effects, such as:

- reputational damage due to negative and public domain events;
- loss of market share because of competitors' actions, including lower prices, innovation and espionage;
- loss of competitiveness due to the rising cost of raw materials;
- slower production due to a supplier closing down;
- reduced cash flow due to issues in debt collection;
- costs due to compliance to new regulatory requirements;
- economic losses due to strikes, acts of sabotage or terrorism arising from the social and political climate;
- reputation damage or loss of customers or cash flow due to defective products and services.

Risks can have positive consequences. We refer to the events that generate them as *opportunities*. Positive consequences and opportunities can be:

- improvement of brand due to a timely adaptation to new regulatory requirements;
- an increased number of customers thanks to high innovation;

- an improved reputation and productivity because of good employee management.

Some risks could be either positive or negative. For example:

- a new customer can have positive consequences, especially on sales, or negative consequences if it turns out to be a bad payer (the Italian public administration is known for its late payments and many businesses have failed because of this[1]);
- an innovation, the opening of a new store, or the addition of a new production line can have positive consequences if appreciated by customers, or negative consequences if they don't bring in enough revenue to cover their costs;
- any change or reorganization can improve the effectiveness and efficiency of processes but can also limit their effectiveness or frustrate the staff.

Information security risk deals only with negative effects. Opportunities related to the management system will be addressed in section 15.6.

4.1.2 Risk level

To understand how to act in response to a risk, we need to determine its level, which is a measure of magnitude. ISO/IEC 27000 has the following definition.

> *Risk level*: magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

Intuitively:

- the more severe the consequences of a possible event, the higher the perceived risk;
- the more likely the occurrence of a negative event, the higher the perceived risk.

Assigning risk levels enables prioritisation and supports the choice of appropriate treatment actions.

ISO/IEC 27001 uses the term *likelihood* and not *probability* to prevent it from being interpreted as an invitation to calculate the risk in quantitative terms (section 7.1). In this book, on the other hand, we use it often because it may be more intuitive.

Consider, as an example, in the context of air travel, bringing luggage onto a plane: the risk of theft is higher if the luggage contains valuable objects or if the airline or airport is known for the high number of thefts.

You can represent this relationship with a mathematical formula, where the risk r is proportional to the probability p of an event's occurrence and its consequences i (traditionally, the term *impact*, and thus the letter i, is used):

$$r \propto p \cdot i. \tag{4.1.1}$$

[1] https://www.economist.com/business/2012/06/23/unhealthy-delays.

When you check your bags at the airport, the risks are not limited to those related to theft, but also to others such as loss or delay in receiving it; in this case the probability and consequences will be different. Thus, the risk depends on the event or threat t and formula 4.1.1 is corrected like this:

$$r(t) \propto p(t) \cdot i(t). \tag{4.1.2}$$

The more valuable the luggage, the higher the risk: risk increases if the value of the objects affected by the threat does. These objects are referred to as assets and marked with the letter a (see paragraph 6.1 for the official definition). The risk of the bags being stolen (threat) is directly proportional to the probability of theft $p(t)$ and to the consequences $i(t, a)$. Formula 4.1.2 must therefore be rewritten like this:

$$r(t, a) \propto p(t) \cdot i(t, a). \tag{4.1.3}$$

If your baggage does not have a lock, it is more vulnerable and the risk increases. The risk therefore depends also on the vulnerability v and its severity $s(v)$. The more significant the vulnerabilities, the higher the risk. Formula 4.1.3 can then be rewritten like this:

$$r(t, a, v) \propto p(t) \cdot i(t, a) \cdot s(v). \tag{4.1.4}$$

If you apply security measures (or controls) c to your bags (by adding a padlock or taking out an insurance policy for example), the risk of theft decreases. The strength of security controls $r(c)$ is the inverse of the vulnerabilities (if your bag has a lock, it is less vulnerable), so we get the following formula:

$$r(t, a, c) \propto \frac{p(t) \cdot i(t, a)}{r(c)}. \tag{4.1.5}$$

Controls can modify the probability of success of a threat (if you use a padlock) or its consequences (if you have an insurance policy). Thus, probabilities and consequences are dependent on c and formula 4.1.3 can be rewritten as follows:

$$r(t, a, c) \propto p(t, c) \cdot i(t, a, c) \tag{4.1.6}$$

A lack of control is a vulnerability. We can replace controls c with vulnerabilities v and get this formula:

$$r(t, a, v) \propto p(t, v) \cdot i(t, a, v) \tag{4.1.7}$$

From what has been said, we can list the parameters of risk assessment:

- the context;
- the asset and its value, on which depends the consequences;
- the threat and its likelihood or probability;
- the vulnerability and its severity or the security control and its strength.

Luggage can be stolen, lost, damaged, or delivered late. With several suitcases, these threats can have different consequences depending on the suitcase involved. The risk related to luggage then consists of multiple individual risks

because there are different threats with different consequences on assets. That's why some use the expression "risk map".

Once we have calculated the risk level, we must make decisions to address it or treat it. Again, using the example of stolen property, the possible decisions are:

- prevent theft and not bring bags;
- reduce the potential consequences of theft and embark only part of the luggage;
- avoid the risk of theft of luggage at the airport and take the train;
- eliminate the risk and travel without any luggage (a very difficult hypothesis to realise);
- share the risk with an insurance company and take out an insurance policy;
- accept the risk and embark the luggage.

Acceptance or non-acceptance of the risk depends on the level of acceptability set by each one: some always embark all the bags and some try to bring as many carry-ons as possible into the cabin.

Each choice does not eliminate the risk, but it may introduce new ones: carry-ons can be stolen too, theft occurs on trains too, and the insurance company might fail and not pay the amount due.

All these concepts are fully described later, in the context of information security.

4.2 What is risk assessment?

First of all, here is the official definition from ISO/IEC 27000.

> *Risk assessment*: the overall process of risk identification, risk analysis, and risk evaluation.

In simpler terms, risk assessment is a set of activities designed to identify risks (i.e. assets, threats, and vulnerabilities), calculate the level of risk, and decide which risks, if any, are acceptable.

The purpose of a risk assessment is to understand where the organisation is exposed and to determine which risks require mitigation. It provides a structured approach for decision-making and supports compliance, operational resilience, and effective resource allocation.

The definition doesn't just apply to information security risk assessments; it is general and could also be applied to the analysis of strategic risk, financial risk, occupational safety risk, project risk [123], privacy risk, etc.

In our case it is more accurate to use the term *information security risk assessment*, though, for the sake of brevity and when there may be no confusion, we shorten it to *risk assessment* in this book.

The purpose of a risk assessment has to be clear in order to identify appropriate methods.

Figure 4.2.1 is the representation of an organization through Anthony's triangle [140] (note that in other contexts, such as the military, these terms have different meanings).

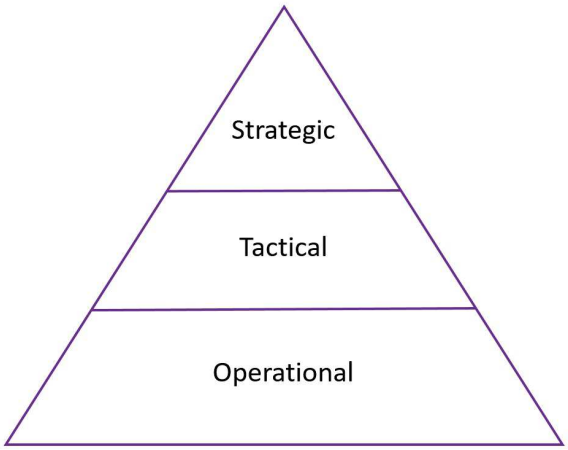

Figure 4.2.1: The pyramid of Anthony

- At the strategic level, data estimates are needed in order to set an approximate direction with long-term perspective (a few years);
- at the tactical level, figures are required, rounded and quite timely, in order to get information on the performance of operational tasks and make medium-term decisions (a few months);
- at the operational level, data must be accurate and in real time, as it serves to keep day-to-day activities afloat.

To create an information security management system, we need to identify its elements, in particular the processes and their relationships, and make decisions regarding security measures. For example, it is necessary to assess the risk to identify: how information security processes shall be, the obligations to require to employees, how privileged credentials shall be used and their strength, what transmissions needs encryption, what communication channels to use in case of emergency, the kinds of software that don't need preventive security tests, how retain logs.

This is at strategic and tactical levels, so you need to have aggregate and not particularly accurate data. To paraphrase the principle of Occam's razor, it is useless to have more data than necessary when making a decision.

Therefore, a risk assessment only needs a low level of detail, even when the value of the information to protect is high: very detailed risk analyses provide too many unnecessary details for strategic and tactical-level decisions.

Having the pretension to completely describe the reality and identify in detail every asset, threat and vulnerability would be a complete waste of work: risk identification will only result in a model of reality, and can never represent it correctly and in complete detail. To illustrate this, Korzybski (although in another context) said that the map is not the territory and Magritte that a drawing of a pipe is not a pipe.

Example 4.2.1. In an organization, after 6 months of meticulous data collection for the information security risk assessment, the security officer noticed that the organization had undergone many changes which required another run at the risk assessment.

The changes, however, were carried out without considering the risks related to information security, further demonstrating how useless the work was considered.

Those who want to do an "accurate job" confuse purpose (having elements to decide) with its means (have a detailed risk analysis).

It is smarter to begin with a mildly accurate analysis at the tactical level. This could highlight the need for further investigation at the operational level, for example of some computer systems (servers, network devices, applications, PCs, portable devices such as mobile phones, smartphones and tablets), functional areas, or services, all of which can be then analyzed in more detail. Methods include *vulnerability assessments* (paragraph 12.15.4) and *gap analysis* with respect to best practices. Note that these methods are not risk assessments because they only report vulnerabilities.

Example 4.2.2. In a large organization, information for a risk assessment was gathered at the level of each organizational function. The result was a useful but excessively large amount of information. In addition, the different representatives had different standards for what should be gathered, which led to a strong heterogeneity in the results.

The analysis didn't reveal the issues at a tactical level, such as a lack of policies for managing physical keys and of a common approach for storing information and performing backups and business continuity tests.

With another, more useful, approach, they initially identified risks related to internal common policies, some of which had shortcomings and didn't respect the desired security level; then they analysed the risks of most critical entities considering the needs of more specific policies; finally, they studied the remaining areas using a gap analysis, namely checking if they had implemented the common policies and intervening when necessary.

Some researchers [98] say that less accurate analyses give equally significant results as more accurate ones, except results are less optimistic and therefore more cautious, which is certainly not a bad thing when it comes to security.

Other types of risk assessment, also required by some authoritative references, require a more operational approach, different from the one presented in this part of the book. For example:

- to assess the risk of technological vulnerabilities identified with a vulnerability assessment or from threat intelligence reports, it is necessary to assess the possibility of exploiting them, and therefore the likelihood and consequences of a successful attack, to obtain a level of risk and the urgency of applying updates, patches or workarounds;

- to assess the supply risk, it is necessary to assess the criticality of individual supplies and the possible negative events that may impact them,

to identify the characteristics that suppliers must have, the contractual conditions to be imposed and the initial and periodic checks on suppliers and supplies.

4.3 Methods of risk assessment

In this book we present an approach to risk assessment, based on assets, threats and vulnerabilities (or countermeasures), as evidenced by the formulas of paragraph 4.1.2. This is common to many approaches (for example Octave [4] and Mehari[2]).

The reason is because this approach is easy to explanain and it is required by some supervisor authorities, even if its obsolete.

Others propose methods apparently not aligned with this approach. However, if you analyze them carefully, these methods always involve the same classic parameters, even though they use different terms (for example, *scenarios* instead of assets or categories of asset, or *events* or *risk scenarios* or *fault cases* instead of threats) and starting points: the classic approach starts from assets, then identifies threats that may have consequences on those assets; the "event-based approach" starts from threats, then identifies assets that may be impacted by them.

Example 4.3.1. Many organizations use an approach based on the importance of information not of the assets that process it.

When looking closely at this method, we realize that information (i.e. assets) and threats are analyzed to calculate the level of inherent risk (paragraph 7.4). From this, we can then choose security measures. In other words, they assess assets, threats, and countermeasures.

The classic approach, if applied as-is, leads to a risk analysis for each asset and has been used only in information security at least since 1980, when information security was very different from now. This is the reason we don't recommend the classic approach.

In this book, the approach is very similar to the classical one, but it requires independent evaluations of assets and threats.

Today, for a risk assessment at a strategic and tactical level, and considering that organizations usually manage IT systems and processes centrally, it can be useful to consider the organization as a single asset. This approach must always be accompanied, at an operational level, by a detailed knowledge of the IT infrastructure and the tools used to manage it, as illustrated below.

4.3.1 Validity of the approach

A *valid* risk assessment method must have the following characteristics:

- *completeness:* all assets, all threats, and vulnerabilities must be taken into consideration and grouped at the right level;

[2] https://clusif.fr/services/management-des-risques/.

- *repeatability:* assessments carried out in the same context and under the same conditions should give the same results;
- *comparability:* assessments carried out at different times in the same context must make it possible to determine whether the risk has changed and how;
- *consistency:* if assets threats and vulnerabilities have higher values, the level of risk must be higher.

The approach should then be simple enough to apply consistently yet robust enough to support meaningful conclusions.

4.3.2 Risk assessment software programs

There are many software programs on the market to carry out risk assessments. They help users in identifying and assigning values to assets, threats and vulnerabilities, and process reports on the risk level.

These programs can be useful in very large organizations because they allow to organize people's activities and to gather all the collected data. They are also helpful when the people involved in the risk assessment (including consultants) are not real experts and need a tool to guide them step by step.

Unfortunately, these programs have flaws that you should be aware of.

The first flaw is that the amount of data to be entered is often huge, making the process quite time consuming. This doesn't guarantee accurate, useful or valid results either.

Example 4.3.2. In an organization, there was an active project to introduce turnstiles at the entrance and to conduct a major review of authorizations in IT systems. Nevertheless, the results of the risk assessment only showed the poor awareness of staff and no issues related to physical access or to the authorizations of IT systems.

The risk assessment had been carried out by collecting many precise data, as demanded by the selected software program, and had required several months of work. Despite that, evidently, the assessment failed in providing useful results to justify the undertaken projects.

The second flaw, common to many products, is the secrecy of the calculation algorithm. In this way, if results show an unacceptable risk, it is impossible to understand the reason, thus convince us of results' validity.

The third defect is the initial product configuration. Often, questionnaires and security measures consider only a specific type of organization. The most popular software for risk assessment, namely CRAMM, during the 1990s was parameterized by studying British mid-sized companies; many other programs are parameterized for large or very large organizations. The configuration is often inappropriate for the context in which the risk is assessed.

The fourth flaw is the difficulty of reconfiguring these tools. This is especially true when we want to change the parameters or add new threats or vulnerabilities.

Example 4.3.3. Many banks assess the risk related to Internet banking. The threat of phishing often goes unnoticed by commercial products and, though it is a very real threat in this context, cannot be added because the product used for the risk assessment does not have this function.

The fifth flaw is that users of commercial software tend to adopt it in a mechanical way, even when they should adapt the method to their own organization. Tools should not replace professional judgement. The value of a risk assessment lies in the discussion, shared understanding, and informed decisions—not in the software alone.

Another flaw, especially in the "compliance" (GRC, *Governance, risk and compliance* software, more and more used since the Twothousandtwenty years, is that often they actually are check lists of information security controls and nothing more.

Obviously, software can be useful to collect data and carry out the necessary calculations. A spreadsheet may suffice and be easily configured as needed.

4.3.3 Warning

What follows is based on proven theories concerning risk assessment, not always related to information security. In fact, the most widely known and advertised approaches to information security risk assessment provide very accurate and detailed reports, preferably aided by commercial software sold by consultants or vendors.

In regard to the qualitative methodologies presented below, some of the ideas were drawn from the experience gained by using a simple spreadsheet available freely on the web [53, 54].

I recommend studying different methods to then decide what to use or if there is a need to develop a new one, tailored to your specifications. There are a few methods in catalogues publications [92, 43]. Some of these methods are not related to information security, but may provide useful ideas for those who want to learn more and develop new solutions. Methods dedicated to information security contain all the steps described in this book, although sometimes using alternative terms, aggregating stages, or proposing different algorithms.

Example 4.3.4. An example of an alternative approach ("event-based approach") is based on a variation of *fault tree analysis*. This approach requires analyzing threats and their consequences without apparently identifying assets in detail.

Nevertheless, to identify threats we need to know which assets can be exploited (e.g. public wi-fi, web applications or a computer network exposed on the Internet) and what security controls, necessarily linked to the asset, are needed to counteract them.

Risk assessments may become bureaucratic if they are overly complex or detached from operations. Organisations should avoid excessive detail that obscures decision-making. The goal is clarity and practical understanding.

4.4 Who to involve

A meaningful risk assessment requires participation from those who understand the organisation's operations, systems, and context. All interested parties should then be involved in the risk assessment: employees, managers, customers, suppliers, and partners.

The following chapters describe other roles to be involved.

Of course, everyone should only know enough to give their input at different stages of the risk assessment.

The involvement of staff, customers, suppliers and partners can be useful to:

- identify the risk (i.e. assets, threats and vulnerabilities);
- assess the risk, by sharing each other views and perceptions;
- evaluate the risk;
- establish the risk treatment plan, because they have to contribute to the planning and implementation of actions;
- reduce the misunderstandings on the actions to be implemented;
- reduce resistance to change;
- have positive consequences on the image of the organization as perceived by its customers, suppliers, partners and staff.

When people are involved, it is good to be aware of the *Dunning-Kruger effect*: people with limited competence in a particular domain overestimate their abilities. To be aware also of competent people [61]: "Expertise in one field does not carry over into other fields. But experts often think so. The narrower their field of knowledge the more likely they are to think so". To be aware also of the *argumentum ad vercundiam* (appeal to the modesty), that is, an argument considered reliable because an expert say so, when the expert is not expert in that field but "modest people" think that its expertise can span in all fields of knowledge.

The following paragraphs focus on two particular roles because they will be important in subsequent chapters.

4.4.1 Risk owner

One figure required by ISO/IEC 27001 is the risk owner, the definition of which appears in ISO/IEC 27000.

> *Risk owner*: person or entity with the accountability and authority to manage a risk.

In other words, risk owners ensure that appropriate controls are defined, implemented, and monitored.

The term "risk owner" is used by ISO/IEC 27001 for alignment to ISO 31000, that doesn't use "Top management". Since he or she must have spending power for managing the risk, the position often coincides with that of top management (paragraph 12.3.1.1). The top management may ask other functions to make

proposals regarding managing the risk and the accompanying costs or to coordinate related activities. Top management is always ultimately responsible for risk.

In all cases, risk owners should be identified at a hierarchical level with appropriate decision-making and spending powers, because they must decide which security controls to implement and maintain.

If information is kept, stored, sent or processed by suppliers, outsourcers or by other entities, the risk owner should be internal to the organization and may coincide with the referent of the relationships with these external entities.

If a risk covers multiple areas of the organization, decisions should be made regarding how to arrange the relevant decisions between different risk owners, or a risk owner could be appointed at an overarching level of the hierarchy.

4.4.2 Facilitators

Facilitators guide the process, conduct the meetings and ensure that discussions remain structured, objective, and aligned with the chosen approach. They help clarify terminology or assumptions.

Some risk assessment approaches [4] explicitly require the use of facilitators to coordinate the activities for the description of the context, the scope identification, the risk identification, analysis, evaluation, and treatment. alisi, ponderazione e trattamento del rischio.

This role is often covered by one or more external consultants. Internal personnel with adequate expertise could also perform these tasks, aided by their more thorough knowledge of the organization.

4.5 Risk management documents

For the risk management, as we will see in the next chapters, several documents are produced. These documents provide evidence for audits, support decision-making, and enable continuous improvement.

Some of them include the description of deficiencies and vulnerabilities and therefore must kept as confidential. It important to remember that these documents are shared between several persons.

Appropriate security controls must consequently be applied in particular for access control (section 12.6) and on the exchange of information (paragraph 12.10.4).

As it will be detailed later, several documents are produced. Some of them also report lacks and vulnerabilities, therefore, they must be kept confidential. It must also be remembered that those documents can be shared between several people.

Chapter 5

Context and scope

> *JAQUES. All the world's a stage,*
> *And all the men and women merely players.*
>
> William Shakespeare, *As you like it* (II, 5).

This chapter describes the preliminary steps to risk assessment. These include an analysis of the context in which the organization operates, because it changes some risks.

The scope of the risk assessment may be the entire organization, include outside parties or be reduced to a more limited perimeter (for example, only services offered to customer).

5.1 Context

This definition from ISO 9000:2015 should help.

> *Context of the organization*: combination of internal and external issues that can have an effect on an organization's approach to developing and achieving its objectives.

Understanding the organisational context is essential for establishing an effective information security management system. It ensure that information security objectives and controls are relevant, proportionate, and aligned with organisational needs.

It can be useful to include a list of items in the description of the context [91]. These items are divided into *internal* and *external issues*. Among the internal issues are:

- current and future strategies and priorities;
- the current and expected level of innovation;
- characteristics of the organization's main activities in terms of services and products and planned changes to the portfolio of products and services;

- organizational structure, including the main suppliers and outsourced processes;
- characteristics of the sites where the activities are performed;
- the types of information handled by the organization;
- the main features of the information system, including:
  - the main ICT services and related infrastructure technologies and applications;
  - the type of portable devices in use, if any, including mobile phones, smartphones and tablets;
  - information archives, in digital and non-digital (e.g. paper) supports;
  - sites of the information systems and archives, including those operated by suppliers;
  - a list of ICT systems shared with other entities (customers, suppliers, partners and other third parties) and their owner (an organization can use some system owned by customers, suppliers or partners);
- the relationships between internal staff (regardless of the type of contract between the parties) and their competence;
- the expectations of the interested internal parties (see 5.2).

Some of the external issues that could have an impact on information security are:

- competitors and potential competitors;
- applicable regulations, including their expected changes;
- the current and expected economic situation in regions where the organization operates;
- the socio-political situation in the regions where the organization operates;
- market availability and costs of resources incurred by the organization;
- market strategies of current and potential suppliers, customers and partners;
- expectations of interested external parties (see 5.2).

When describing the context, all the previous points don't have to be included, but only the relevant ones for the information security.

Example 5.1.1. Here is a possible description of the context in a dairy farm.

Characteristics of the services and products. The company deals with the production and sale of dairy products. It has annual sales of around 10 million EUR.

Organizational structure. The company structure is depicted in the organizational chart (Figure 5.1.1). Other suppliers, apart from the

accountant and sales agents, are the CRM developer, a telecommunications operator, a security company and a cleaning company.

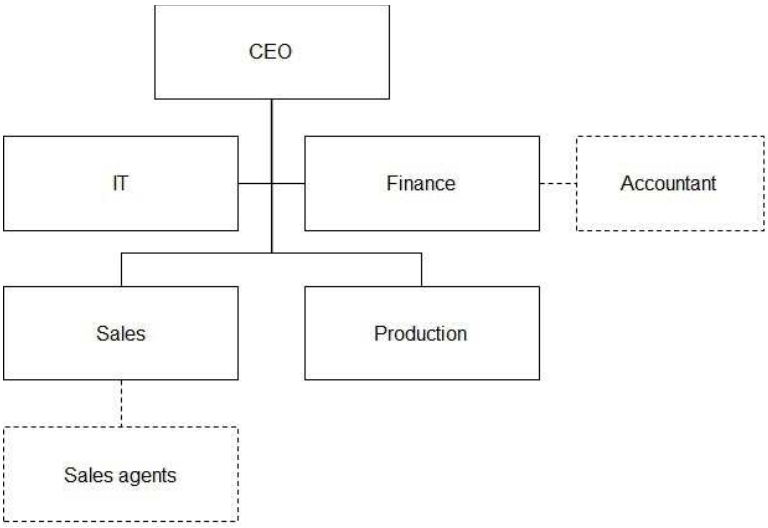

Figure 5.1.1: Example of an organizational chart

Physical locations. The company is located in a wholly-owned (not shared with other organizations) farm in the municipality of Basilio near Milan, Italy.

Information handled. The information handled relates to customers, suppliers, partners, personnel, and products (recipes and quality audits). Given the competition, it is very important to ensure the confidentiality of client', suppliers' and partners' information. Handling personal data correctly is important to comply with current data protection regulations, and ensuring the confidentiality and integrity of receipt s and audit reports will allow the company to safeguard corporate knowledge.

ICT system. From an infrastructure point of view, the architecture is based on Microsoft Windows systems for servers and personal computers. The most important applications and services are email, a file server, a CRM (customer relationship management) system, and a system internally developed specifically for warehouse and production control. Sales agents can access the CRM, the list of customers, and orders with a web browser.

Hardcopy documentation. All data can also be on hard copies, stored in archives, or, exclusively for accounting and administrative data, in the accountant's office.

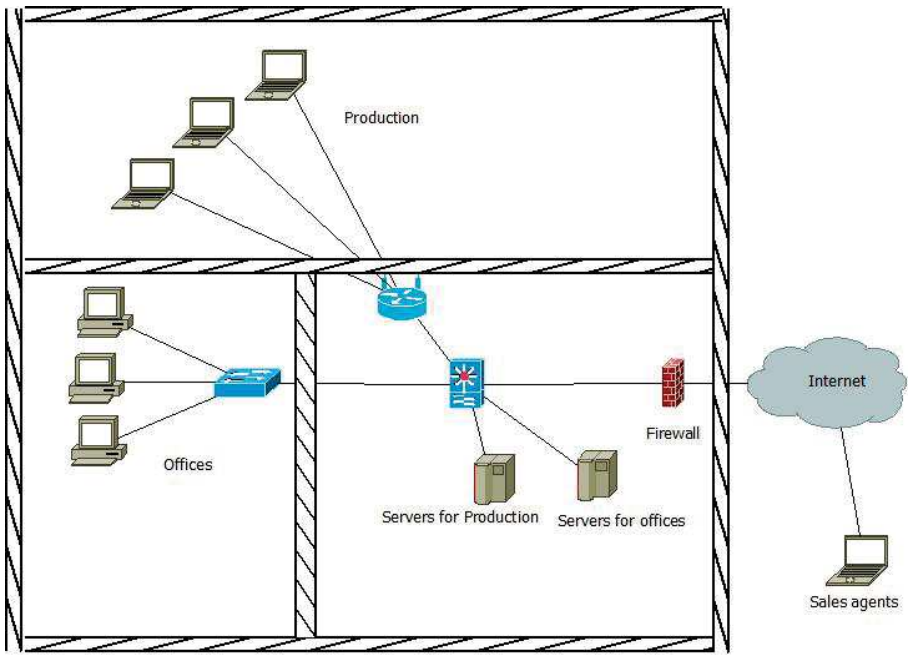

Figure 5.1.2: Example of ICT network

Current regulations. The legislation requires extreme care in maintaining information on products placed on the market and for this it is vital to ensure the integrity of data on the production. There are no foreseen legislation major changes in the future, but there is the need to monitor it.

Level of innovation. Innovations are necessary to maintain market competitiveness (computerization of warehouse, communication with suppliers via digital means, etc.).

5.2 The interested parties

The definition of *interested party* from ISO/IEC 27000:2015 is the following.

> *Interested party* or *stakeholder*: person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.

The interest parties have requirements, or expectations, relevant to the information security management system. The organization should consider them.

The *interested internal parties*are staff and shareholders. Their expectations include the respect for contracts and agreements and the good quality of the working environment.

The *interested external parties* include current and potential customers, suppliers and partners, regulators, control agencies. Their expectations include the respect of contracts and agreements, intra-group agreements, and regulations.

Example 5.2.1. Here is a possible description of the interest parties of the dairy farm above.

Competitors. The competition is very strongly felt in the area, but industrial espionage activities are not significant enough to cause concern.

Customers. Customers ask for compliance regarding deadlines and product quality, in accordance with contracts and regulations.

Suppliers. In addition to sales agents, major suppliers provide raw materials and packages, expect their efforts to meet the needs of an organization to be appreciated, and expect to be paid according to agreed deadlines.

Internal staff. Comprised of thirteen people, both blue- and white-collar, with little education and training and with no specific skills on the use of computer systems, except the two employees that develop and maintain IT systems. Staff expect to work in a good workplace, respectful of safety, privacy and all existing legislation and of the schedule of payments. The business climate is good and there were no major disputes over the last twenty years.

The organization does not necessarily have to address all the requirements of the interested parties, but it must identify them and determine which the information security management system intends to address.

Example 5.2.2. Customers of a cloud infrastructure service (IaaS) may require the backup service. This could be offered as an optional service or automatically included in the infrastructure service. The same customers may want, in the event of an incident, maximum service interruption times, while the supplier may ensure different ones.

From a management perspective, customers may want the supplier to comply with certain regulations or standards that are not mandatory in the Country where the supplier operates (e.g., U.S. HIPAA). The supplier may or may not address these requirements.

The compliance with the applicable legislation and accepted agreement with employees, suppliers and customers should always be ensured.

5.3 The scope

After the context is understood, it is possible to set the *scope* of the information security risk assessment, i. e. its boundaries and applicability. It may include all or part of the organization.

Organizations often only consider their customers' perception and limit the scope to the services they offer.

Example 5.3.1. The dairy farm might decide to assess the information security risk throughout the whole organization because each area has impacts on customer relations, product quality, and employee satisfaction.

The same company could limit the scope to production, both because of the impacts on customers and because this is required by food industry regulations.

The scope could be widened to include suppliers in cases where they process the company's data or provide critical products.

Some processes cannot be completely excluded from the scope, especially when the purpose of the risk assessment is the certification of the information security management system.

Example 5.3.2. If the dairy farm decides to assess information security risks within the scope of production, it should still consider some seemingly external processes. For example, personnel management is external to production but very important to information security (section 12.4). This must, at least partially, be included in the scope.

If the dairy farm uses a provider for IT services, it also should be included.

When the scope has been established, its boundaries must be analyzed.

Example 5.3.3. When the scope of the dairy farm is considered, it must be noted that its IT systems are connected to the Internet, the CRM is accessible via the web from any PC and some data is accessible to external agents.

The scope should be described in terms of:

- the types of information that the organization wants to protect;
- the characteristics of the products and services provided by the organization and relevant for the information to be protected;
- the organizational structure involved in the activities included in the scope and its relations with the organization structure excluded from the scope;
- the technology used, a scheme of IT network and a description of its interfaces with other systems in the organization or suppliers;
- the sites where the relevant information is processed (archives and data centers), including sites of the relevant suppliers or other external parties;
- the most important suppliers involved in information security, including those who develop or operate the IT systems of the organization.