

ISO/IEC 27001

Information Security

Certification Programs

SKILLFRONT



Yeliz Obergfell

Skill Platform For

Professionals

SKILLFRONT

WWW.SKILLFRONT.COM

© COPYRIGHT SKILLFRONT

PROGRAM BOOK

For ISO/IEC 27001 Information Security Certification Programs

The ISO/IEC 27001 Information Security Framework

Dedication

To all of the SkillFront Professionals, thank you for inspiring us, keeping us focused, and making sure we do our best to guide you to execute ideas, grow businesses, and dominate your markets online and offline.

We are proud of seeing you while you serve your clients at your highest levels possible and positively influence their lives that wouldn't happen otherwise.

Without you, your engagement, and your loyal support, SkillFront could not come where it is today.

Table Of Contents

CLICKABLE

Table Of Contents	5
Welcome To The SkillFront	9
Become A Bit Better Than You, Everyday	14
Why Does ISO/IEC 27001 Matter?	20
A Brief History	22
The Structure Of ISO/IEC 27001	23
ISMS Scope and Statement of Applicability (SoA)	26
Mandatory Requirements for Organizational ISO 27001 Certification	28
ISMS Scope (Clause 4.3)	28
Information Security Policy (Clause 5.2)	29
Information Risk Assessment Process (Clause 6.1.2)	29

Information Risk Treatment Process (Clause 6.1.3)	30
Information Security Objectives (Clause 6.2)	31
Evidence Of The Competence Of The People Working In Information Security (Clause 7.2)	32
Other ISMS-related Documents Deemed Necessary By The Organization (Clause 7.5.1b)	32
Operational Planning And Control Documents (Clause 8.1)	33
The Results Of The [Information] Risk Assessments (Clause 8.2)	34
The Decisions Regarding [Information] Risk Treatment (Clause 8.3)	34
Evidence Of The Monitoring And Measurement Of Information Security (Clause 9.1)	35
The ISMS Internal Audit Program And The Results Of Audits Conducted (Clause 9.2)	36
Evidence Of Top Management Reviews Of The ISMS (Clause 9.3)	37
Evidence Of Nonconformities Identified And Corrective Actions Arising (Clause 10.1)	38
Various Others	38
Certification	39
ISO 27001 Audit Programs	41
Success Factors For Practical Implementation	43

ISO 27001 Step-By-Step Implementation Guide	46
Step 1. Obtain Management Support	46
Step 2. Treat It As A Project	46
Step 3. Define The Scope	47
Step 4. Write An Information Security Policy	47
Step 5. Define The Risk Assessment Methodology	47
Step 6. Perform The Risk Assessment & Risk Treatment	48
Step 7. Write The Statement Of Applicability	48
Step 8. Write The Risk Treatment Plan	49
Step 9. Define How To Measure The Effectiveness Of Controls	49
Step 10. Implement The Controls & Mandatory Procedures	50
Step 11. Implement Training And Awareness Programs	50
Step 12. Operate The ISMS	50
Step 13. Monitor The ISMS	51
Step 14. Internal Audit	51

Step 15. Management Review	52
Step 16. Corrective And Preventive Actions	52
ISO 27001 - Roles And Responsibility In Organizations	53
Why Understanding Roles is Critical to the Security Program?	53
Five Typical Roles and Responsibilities	54
1. Security Leadership	54
2. Security Risk Management	56
3. Internal Audit	57
4. Control Owners	57
5. All Employees	58
Next Steps For The Pursuit Of Growth	59
Thanks For Learning With The SkillFront	62

Welcome To The SkillFront

“ As to methods, there may be million and then some, but skills are few. The one who grasps skills can successfully select his or her own methods. The one who tries methods, ignoring skills, is sure to have trouble.”

– Ralph Waldo Emerson, Essayist and Poet

New Year's Eve 2010.

As the rest of the world went about celebrating the dawn of a new year heading into 2011, I lay in my bed, next to my baby, who was born less than four short months ago.

My husband sat next to me, and I can still remember the sound of fireworks set off in the neighborhood.

I could see the colors of fireworks, reflecting off my husband's face. He turned and looked at me, while tears were pouring down my cheeks, and he said, "**You didn't sign up for this. We're going to fix it!**"

I lay down and put my hands back behind my head; closing my eyes, I felt every aspect of my being filled with rage.

My mind raced back to the winter, nearly twelve months before, to me getting promoted to a leadership position at one of Switzerland's largest local banks. As the manager of the busiest branch in the middle of the city of Zurich, I was leading thirty to forty employees, contractors, and agency staff. To this day, I can't help but marvel at the thousands of working hours, the millions of Swiss francs, and the enormously complex processes necessary to make a simple financial investment product shown in our portfolio of products.

And yet, there I was lying, heading into 2011, with the termination letter in my hand. It turned out that my employer didn't want to occupy their demanding positions with mothers of newborn babies. They couldn't wait any longer and quickly sent me my notification at the end of my twelve-weeks of officially deserved maternity leave.

At this moment, you may be wondering why I didn't go

back to my corporate career, although I could have reasonably quickly find another job, given my qualifications and job experiences, even if I had this big "obstacle" of having a few months old baby.

Let me tell you this. The shock of getting fired helped me admit three very important things that I haven't been entirely honest to myself before:

- 1. Large companies move slowly.** Good ideas often died on the vine simply because they had to be approved by too many people.
- 2. Climbing the corporate ladder is an obstacle to doing great work.** I wanted to focus on getting things done and making things better, not constantly positioning myself for promotion. Politics and turf wars are an inescapable part of the daily experience of working for a large company.

3. Frustration leads to burnout. I wanted to enjoy my daily work experience, but instead, I felt like I was running a gauntlet each day. It began to affect my health during my pregnancy, happiness, and relationships with my husband, friends, and family.

The longer I thought of these facts, the more I realized I wanted out. **I desperately wanted to work on my own terms, as an entrepreneur.**

The next ten years took me on a journey, trying to bring up my baby, become a good wife, and transform myself into the practical scientist to unlocking measurable results in every area of my life every day. A scientist I call the SkillFront Entrepreneur.

My name is Yeliz Obergfell.

I am a married woman.

I am a mother.

I am a businesswoman.

And most important:

I am a SkillFront Entrepreneur.

I train entrepreneurs at all levels —from want-to-be entrepreneurs to owners of large enterprises— to execute ideas, grow businesses, and dominate their markets online and offline.

I wasn't trying to become an expert.

In fact, I wasn't even sure what being an expert meant. **I was, and I am still trying to be a student of my own passion; helping and serving other entrepreneurs succeed in business.**

I wanted to set myself free after getting laid off. I had no clue that what would start with a decision to change my life would transform into a global movement thanks to the principles, frameworks, and support of SkillFront, the Skill Platform for Entrepreneurs.

I started the idea of SkillFront in 2011 with zero knowledge of marketing, sales, persuasion, closing, e-commerce, or automated digital marketing systems.

On top of that, I had never delivered a service that was 100 percent created by me, and I had spent most of my career selling other services.

From 2011 to 2014, I struggled to get the message I felt in my heart and soul out to the world. Although we were having some mild success, I was paralyzed trying to figure out not only the psychology of being a female leader with my message, but also the science and technology to sustain and scale my business.

I have always been an avid learner, but before I decided to learn everything I could about how I can succeed as an entrepreneur, most of what I read was fiction. If there is one thing I am good at it, it is taking in a huge amount of information and distilling it into essentials. I am a

synthesist by nature, and my travels through the business literature quickly became an exercise in separating the diamonds from the rough.

The more I learned, the more helpless I felt. For every great resource I found, I had to process ten other resources to figure out how to apply that resource in practice to excel on my own entrepreneurship journey.

I started to wonder: how much of what's out there—and there is a lot out there—I really needed to know. How could I separate practical business and entrepreneurship skills from the dry theory and technobabble? I only had so much time and energy, so I started searching for a filter: something that would direct me to the useful skills and keep me away from the chaff. **The more I searched, the more I realized it didn't exist — so I decided to create the SkillFront.**

As of this moment, 143,487 SkillFront Entrepreneurs are actively using the SkillFront Platform to quickly get their ideas, products, and services out to the world!

I don't share that with you to impress you. To some of you hearing this, that is a big thing, and to others, it's nothing. I share it to demonstrate what is possible when you learn, live, and leverage the practical science and art of being an entrepreneur while combining those skills with lessons you are going to earn in real practice.

So take a deep breath. It's time for you to unlock the blueprint of success as an entrepreneur and get to work.

Welcome to the SkillFront.

Yeliz Obergfell, SkillFront
Cofounder, Vice President – Entrepreneur Experience

Francis Bremping
IA Analyst w/ focus on AI/ML & Cyber-ecosystem Impact | Resume Reviewer | U.S. Navy Medical (w/ Secret Clearance)
June 6, 2020, Francis was a client of Yeliz's
Myself and my team relied on Yeliz. She promptly sent us great materials, and still updates my team on methodology trends. Yeliz is totally in, and committed to the program.

William (Ray) Woods
★Project Management
★Mechanical Engineer
★Content Creator ★
Business/Data Analyst
March 29, 2020, Yeliz worked with William (Ray) in the same group
I highly recommend working with Yeliz. She is an awesome individual who is always willing to help you and provide you with the highest quality resources to excel further in your career. She has helped me bring more value to my clients in a highly competitive engineering industry through business and entrepreneurship training. Thanks a ton.

Ilya Kharitonov
VP & CRO at the bank |
Areas of interest: FinTech, Risks & CyberTech, Longevity, Venture investments
March 9, 2020, Ilya was a client of Yeliz's
Very smartly organized online course and certification programs for entrepreneurs! Very good structured educational books! Very responsively built feedback loops helped us form and excel in our business operations and practices.

Vanya Pashova • 1st
Turning people into teams, obstacles into opportunities and ideas into r...
1d • 🗨️

The best thing you can do in a lockdown is to invest in your skills and knowledge. "I hate studying. I like learning, learning is beautiful!", a wise lady once said and she was absolutely right. :)
Thank you **Yeliz Obergfell** 🌟 and **SkillFront** for your continuous support and inspiration! Already looking forward to the next chapter!

👍 🌱 82 • 8 Comments

Reactions

+74

Become A Bit Better Than You, Everyday

“ Before you can be great, you must be good. Before you can be good, you must be bad. Before you can be bad, you must try.”

– Jim Edwards, Copywriter and Digital marketer

The Key To Success: Model The Best

During one of the seminars I attended more than a decade ago in Nashville, Tennessee, I had one of the most significant aha moments in my personal and entrepreneurial growth journey, which impacted my business more than everything else I learned until today.

That was the discovery of thoughtful modeling to build my own skills and career. Children use modeling all the time to learn how to speak, use tools, or tie their shoes.

If you look at it carefully, modeling is not only essential to build new skills, but also it's necessary for the continuity of skills, lessons, know-how, and the world's intellectual and cultural legacy from one generation to another.

One caveat here: I have seen and met many people who mix modeling with copying someone else's materials, patents, works, ideas as they're, and use them for their own goals. Don't do this. That is illegal and unethical.

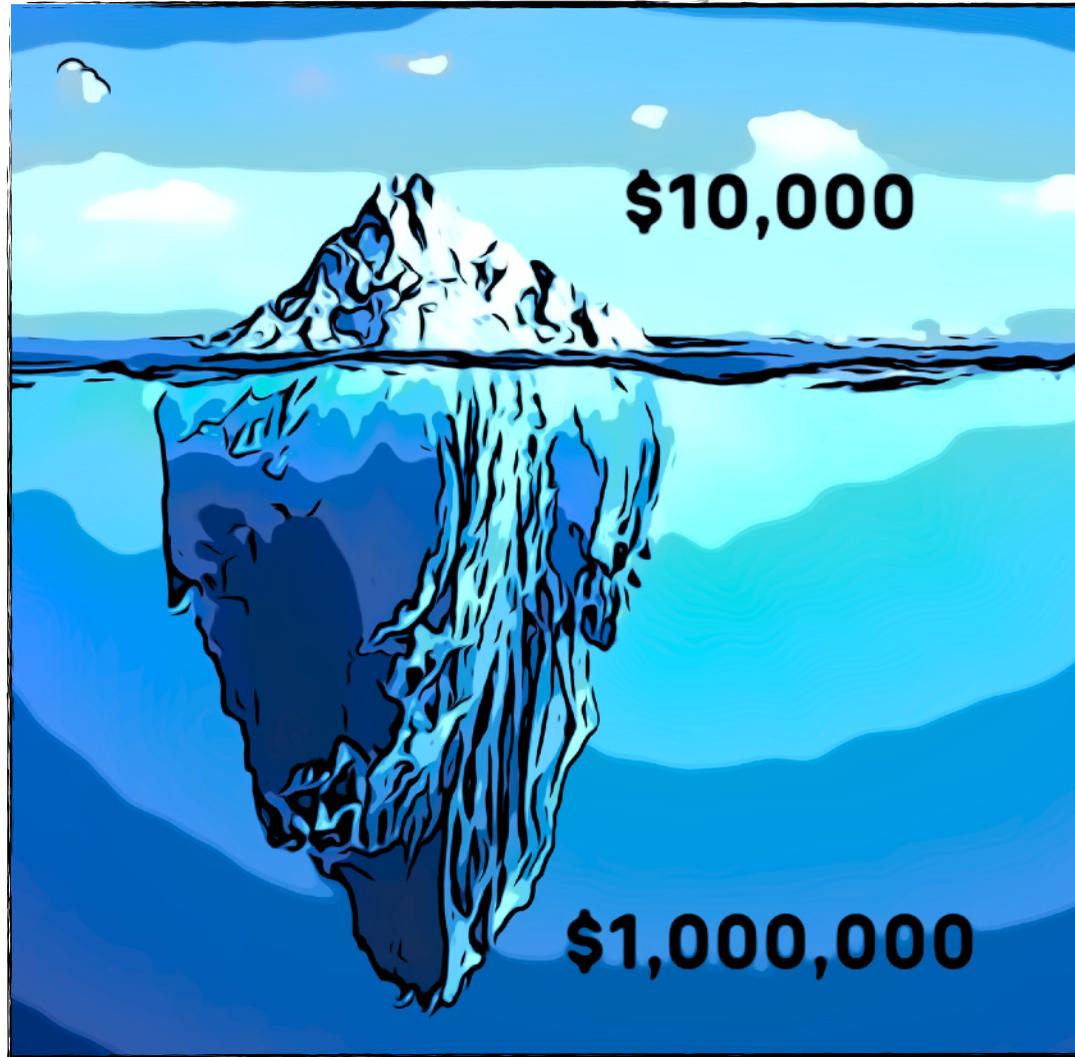
What I mean with thoughtful modeling is:

1. **Look for a business that is already successful** in your chosen field or a leader who has created the kind of life you want to live.
2. As Tony Robbins rightly put out there: **Success leaves clues. Find them.** There's no need to reinvent the wheel. Those who have succeeded before you have done so, followed a plan, and you can do the same thing. Look into their history and their rise to the top. How did they get to where they are today? What kind of obstacles and setbacks did they face, and how did they overcome them? What are their philosophies about their work and their life?

3. **Use this information to build the path of your success** that mirrors theirs. Your strategy may be similar to the business or leader you're modeling, or you adjust it for your present circumstances.

So, I started looking at other businesses, studying how they came to where they're today. After all, their techniques worked for them, they could work for me. But for some reason, my efforts made very little (if any) success and income. I was frustrated because I could see others making money successfully. What was I doing wrong?

It took me almost four years of studying, researching, and interviewing successful business people before I realized that what I was seeing on the surface wasn't their full arsenal of skills and strategies. The entrepreneurs who were making decent money were doing it through steps and processes invisible to the naked eye.



I was modeling what I could see happening on the surface of successful businesses, but they made the real money in ways I couldn't see.

While I had learned and modeled the part of their businesses that I could see, multiple things were happening behind the scenes that made the magic work.

I found that the difference between a \$10,000 and \$1,000,000 business was all the things happening after a buyer initially contacted those businesses.

It took me years to discover and master these hidden skills below the surface of the iceberg, but when I did it, the results spoke for themselves. I wanted to launch SkillFront because I know there are entrepreneurs like me who have been trying to be successful, yet are not having much success.

This and other SkillFront programs are the culmination of a decade spent analyzing thousands of companies and their success models. I have built a number of successful companies of my own, and I have worked with

tens of thousands of students and clients to guide them to build businesses in every industry you can dream of - both online and offline.

This and other programs in the SkillFront platform will unlock the practical skills and frameworks that are mastered and continuously used by champion businesses and leaders in their industries.

I hope that while you're learning those skills, you will realize your dreams of success are a lot closer than you think. You will soon see that by providing a ton of value, communicating effectively with your audience, and building out your sales processes and flows in a very strategic way, you can get your product, service, and message out to the world. And you can get paid what you're worth while doing it.

All Skills You're Going To Learn Are Evergreen

If you've tried to learn how to build and grow your company in the past, you've probably purchased courses and courses that teach systems that worked when they were created but became outdated. Often, before they even reached a wider audience and found their way to you.

SkillFront programs, on the other hand, are playcourses for creating and scaling successful businesses that will exponentially increase your sales and income. SkillFront teaches evergreen skills, frameworks, and strategies that will be just as useful 20 years from now as they are today. **It's the mission of the SkillFront to focus on principles and methods that are timelines, even if technologies and tools change.**

We don't just teach this stuff; We actually do it.

There are many people teaching business and entrepreneurship from one or another angle, and the vast majority of them are making money by teaching other people's business strategies. Russell Brunson calls those people "shovel sellers" because during the gold rush, the people who made the most money were the ones selling the shovels. Today's modern shovel sellers are selling you those strategies without actually using any of the techniques themselves.

The difference between SkillFront and most others is that we actually do this for real. That's right. The skills we're going to reveal to you have been learned and then verified by our own real-world practices, or we have earned them after thousands of tests, sleepless nights, mistakes, trials, errors, successes, as well as failures.



One of our amazing partners MicroTrain from Chicago, the United States of America, and their valuable trainees for their successful course and certification programs.

We have tried these skills in countless different industries, from law practices to multinational e-commerce giants, from coaching services to software-as-a-service providers, from physical product retailers online and offline to real estate brokers, from healthcare, fitness, wellness and leisure providers to sports clubs and educational institutions, and everything else you ever imagine in between.

We also directly work with hundreds of other businesses, advising them and increasing their profitability in almost every niche and industry you can dream of.

I am excited for you to dive in and have some fun with this. So, let's get started!

Why Does ISO/IEC 27001 Matter?

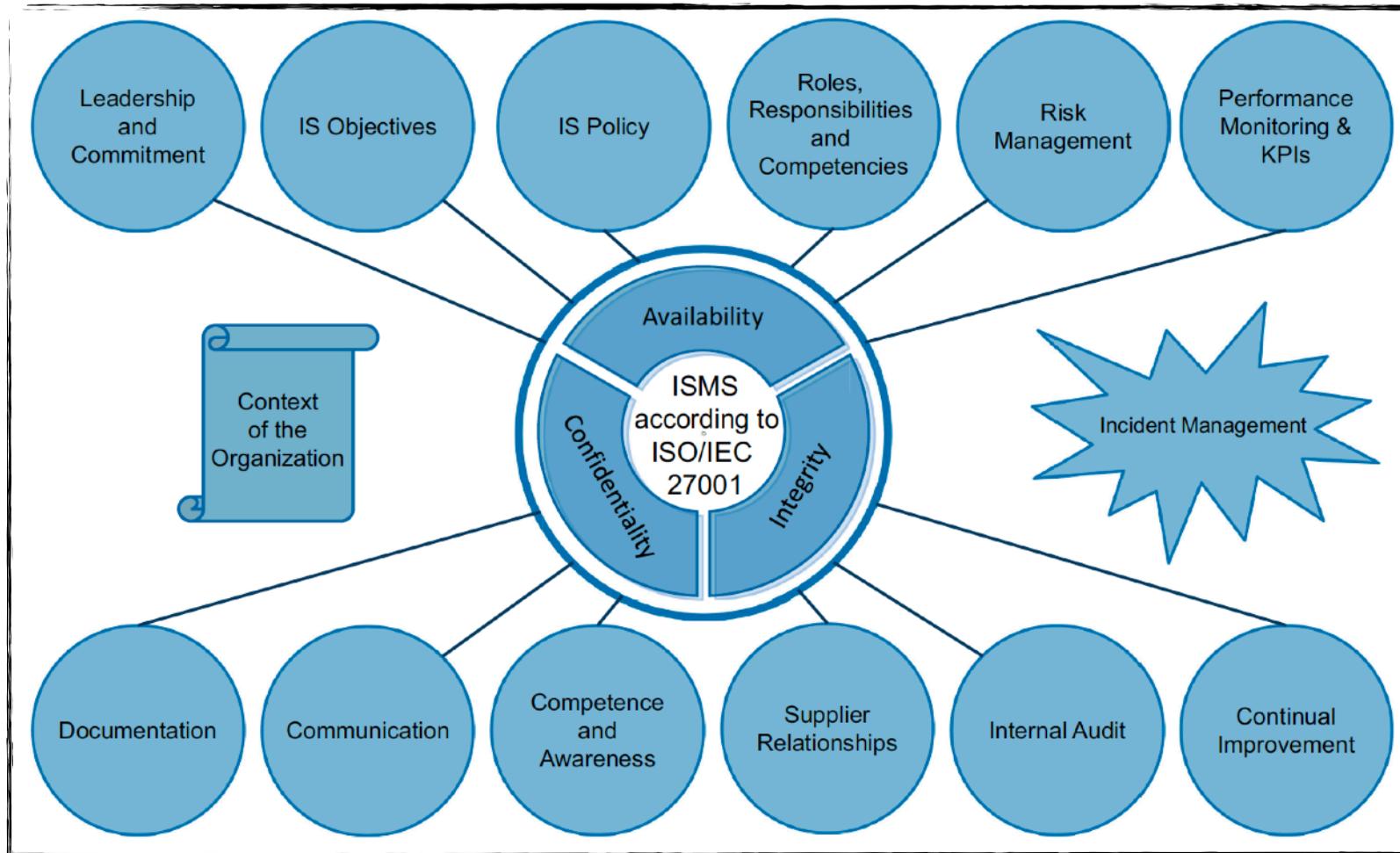
ISO/IEC 27001 formally specifies an **Information Security Management System (ISMS)**, a governance arrangement comprising a structured suite of activities with which to manage information risks (called 'information security risks' in the standard).

The ISMS is an overarching framework through which management identifies, evaluates and treats (addresses) the organisation's information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profits) of all sizes (from micro-businesses to huge multinationals) in all industries (e.g. retail, banking, defense, healthcare, education and government). This is clearly a very wide brief.

ISO/IEC 27001 does not formally mandate specific information security controls since the controls that are required vary markedly across the wide range of organizations adopting the standard.

The information security controls from ISO/IEC 27002 are summarised in annex A to ISO/IEC 27001, rather like a menu. Organizations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information risks, drawing on those listed in the menu and potentially supplementing them with other a la carte options (sometimes known as extended control sets).



Components of an ISMS in accordance with ISO/IEC 27001

As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organization's information risks, which is one vital part of the ISMS.

Furthermore, management may elect to avoid, share or accept information risks rather than mitigate them through controls - a risk treatment decision within the risk management process.

A Brief History

ISO/IEC 27001 is derived from BS 7799 Part 2, first published as such by the British Standards Institute in 1999.

BS 7799 Part 2 was revised in 2002, explicitly incorporating the Deming-style Plan-Do-Check-Act

cycle.

BS 7799 part 2 was adopted as the first edition of ISO/IEC 27001 in 2005 with various changes to reflect its new custodians.

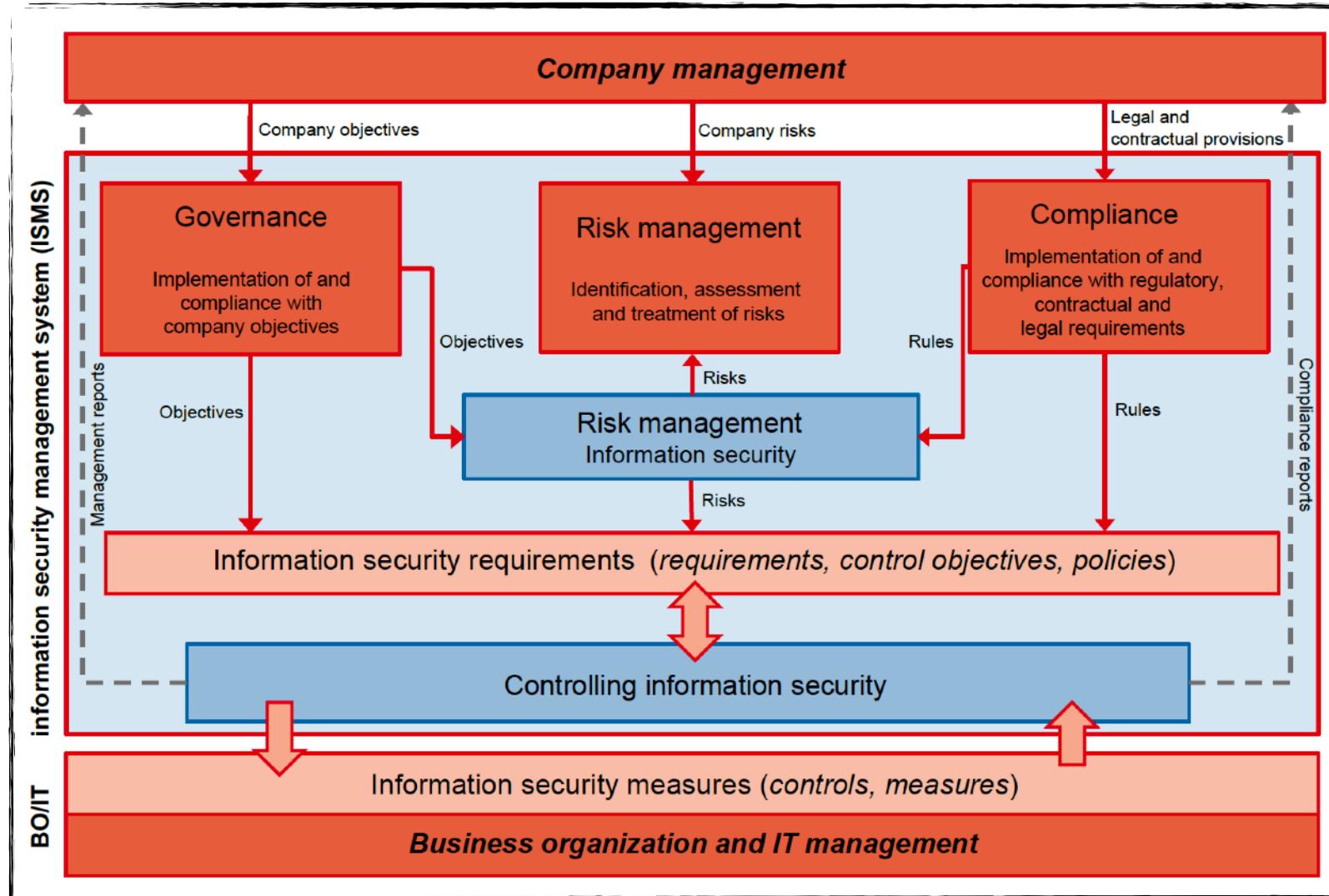
The second edition of ISO/IEC 27001 was published in 2013, having been extensively revised to align with the other ISO management systems standards. PDCA is no longer explicit, but the concept of continuous refinement and systematic improvement remains, for sure.

The Structure Of ISO/IEC 27001

ISO/IEC 27001 has the following sections:

- **Introduction:** the standard describes a process for systematically managing information risks.
- **Scope:** it specifies generic ISMS requirements suitable for organizations of any type, size or nature.
- **Normative references:** only ISO/IEC 27000 is considered absolutely essential to users of '27001: the remaining ISO27k standards are optional.
- Terms and definitions
- **Context of the organization:** understanding the organizational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" the ISMS.
- **Leadership:** top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.
- **Planning:** outlines the process to identify, analyze and plan to treat information risks, and clarify the objectives of information security.
- **Support:** adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
- **Operation:** a bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).
- **Performance evaluation:** monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.

- **Improvement:** address the findings of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS.
- **Annex A Reference control objectives and controls:** little more in fact than a list of titles of the control sections in ISO/IEC 27002. The annex is 'normative', implying that certified organizations are expected to use it, but the main body says they are free to deviate from or supplement it in order to address their particular information risks. Annex A alone is hard to interpret. Please refer to ISO/IEC 27002 for more useful detail on the controls, including implementation guidance.
- **Bibliography:** points readers to five related standards, plus part 1 of the ISO/IEC directives, for more information. In addition, ISO/IEC 27000 is identified in the body of the standard as a normative (i.e. essential) standard and there are several references to ISO 31000 on risk management.



Incorporating the ISMS into corporate control processes

ISMS Scope and Statement of Applicability (SoA)

Whereas the standard is intended to drive the implementation of an enterprise-wide ISMS, ensuring that all parts of the organization benefit by addressing their information risks in an appropriate and systematically-managed manner, organizations can scope their ISMS as broadly or as narrowly as they wish - indeed scoping is a crucial decision for senior management. A documented ISMS scope is one of the mandatory requirements for certification.

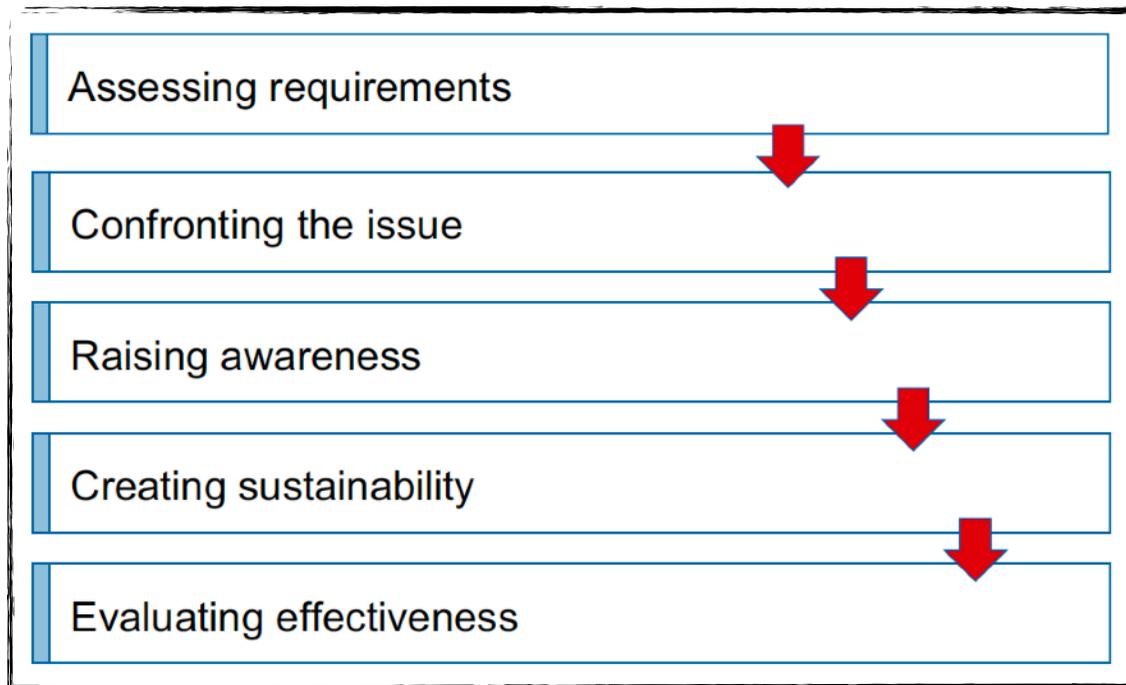
And yet, although the Statement of Applicability is not explicitly defined, it is a mandatory requirement.

SoA refers to the output from the information risk assessments and, in particular, the decisions around treating those risks. The SoA may, for instance, take the form of a matrix identifying various types of information risks on one axis and risk treatment options on the other, showing how the risks are to be treated in the body, and perhaps who is accountable for them.

The ISMS scope and SoA are crucial if a third party intends to attach any reliance to an organization's ISO/IEC 27001 compliance certificate. If an organization's ISO/IEC 27001 scope only includes "Acme Ltd. Department X", for example, the associated certificate says absolutely nothing about the state of information security in "Acme Ltd. Department Y" or indeed "Acme Ltd." as a whole.

Similarly, if for some reason management decides to accept malware risks without implementing conventional antivirus controls, the certification auditors may well

challenge such a bold assertion but, provided the associated analyses and decisions were sound, that alone would not be justification to refuse to certify the organization since antivirus controls are not in fact mandatory.



**Phase Model For ISMS Scope Definition and SoA
Awareness Campaigns**

Mandatory Requirements for Organizational ISO 27001 Certification

ISO/IEC 27001 is a formalized specification for an ISMS with two distinct purposes:

1. It lays out the design for an ISMS, describing the important parts at a fairly high level;
2. It can (optionally) be used as the basis for formal compliance assessment by certification auditors in order to certify an organization compliant.

The following mandatory documentation is explicitly

required for certification:

ISMS Scope (Clause 4.3)

Determining the scope of the information security management system: The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

- the external and internal issues;
- the requirements;
- interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

Information Security Policy (Clause 5.2)

Policy: Top management shall establish an information security policy that:

- is appropriate to the purpose of the organization,
- includes information security objectives or provides the framework for setting information security objectives,
- includes a commitment to satisfy applicable requirements related to information security and
- includes a commitment to continual improvement of the information security management system.

The information security policy shall:

- be available as documented information;
- be available to interested parties, as appropriate.

Information Risk Assessment Process (Clause 6.1.2)

Information security risk assessment: The organization shall define and apply an information security risk assessment process that:

- establishes and maintains information security risk criteria that include:
 - the risk acceptance criteria; and
 - criteria for performing information security risk assessments;
- ensures that repeated information security risk assessments produce consistent, valid and comparable results;
- identifies the information security risks:
 - apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for

information within the scope of the information security management system; and

- identify the risk owners;
- analyses the information security risks:
 - assess the potential consequences that would result if the risks identified;
 - assess the realistic likelihood of the occurrence of the risks identified in and
 - determine the levels of risk;
- evaluates the information security risks:
 - compare the results of risk analysis with the risk criteria established; and
 - prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

Information Risk Treatment Process (Clause 6.1.3)

Information security risk treatment: The organization shall define and apply an information security risk treatment process to:

- select appropriate information security risk treatment options, taking account of the risk assessment results;
- determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
- compare the controls determined.
- produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
- formulate an information security risk treatment plan; and

- obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.
- The organization shall retain documented information about the information security risk treatment process.

Information Security Objectives (Clause 6.2)

Information security objectives and planning to achieve them: The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

- be consistent with the information security policy;
- be measurable (if practicable);
- take into account applicable information security

requirements, and results from risk assessment and risk treatment;

- be communicated; and
- be updated as appropriate.

The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed; and
- how the results will be evaluated.

Evidence Of The Competence Of The People Working In Information Security (Clause 7.2)

The organization shall:

- determine the necessary competence of person(s) doing work under its control that affects its information security performance;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- retain appropriate documented information as evidence of competence.

Other ISMS-related Documents Deemed Necessary By The Organization (Clause 7.5.1b)

The organization's information security management system shall include: documented information determined by the organization as being necessary for the effectiveness of the information security management system.

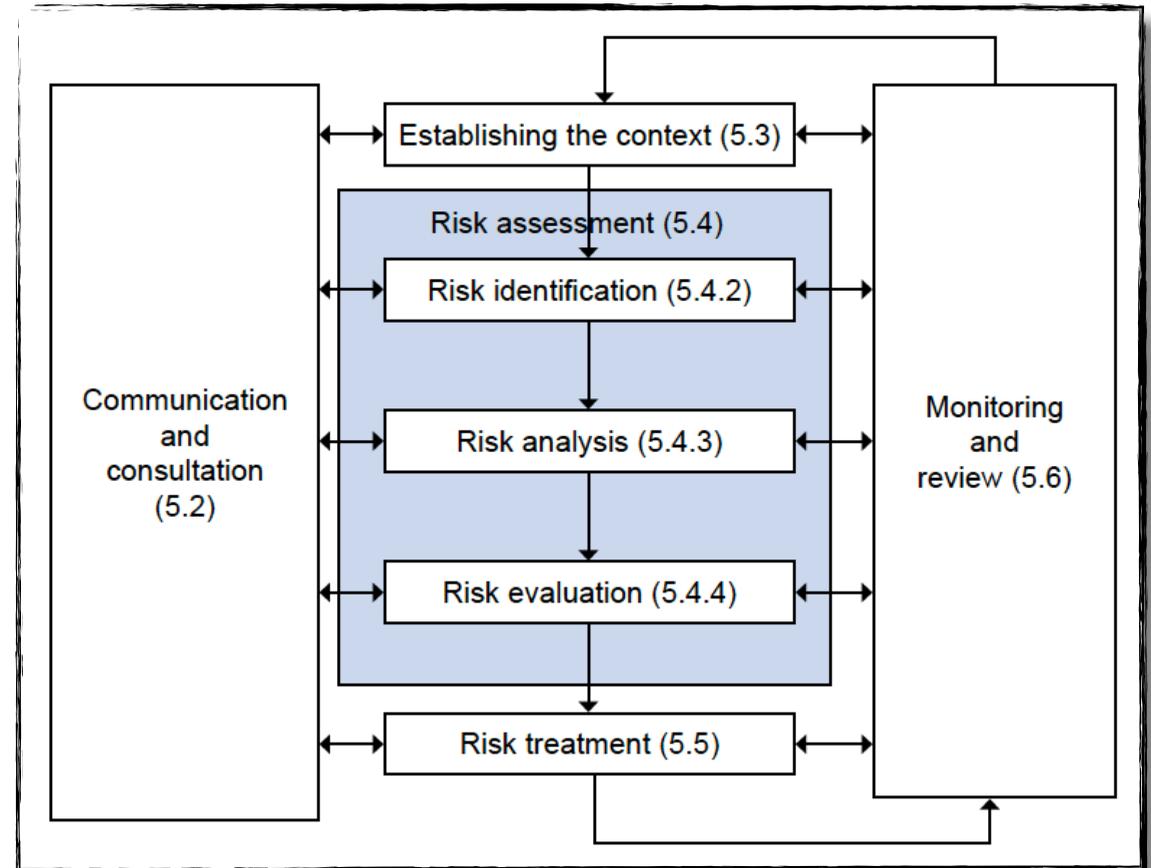
Operational Planning And Control Documents (Clause 8.1)

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined. The organization shall also implement plans to achieve information security objectives determined.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.



Risk Management Process Based On ISO 31000

The Results Of The [Information] Risk Assessments (Clause 8.2)

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established.

The organization shall retain documented information of the results of the information security risk assessments.

The Decisions Regarding [Information] Risk Treatment (Clause 8.3)

The organization shall implement the information security risk treatment plan.

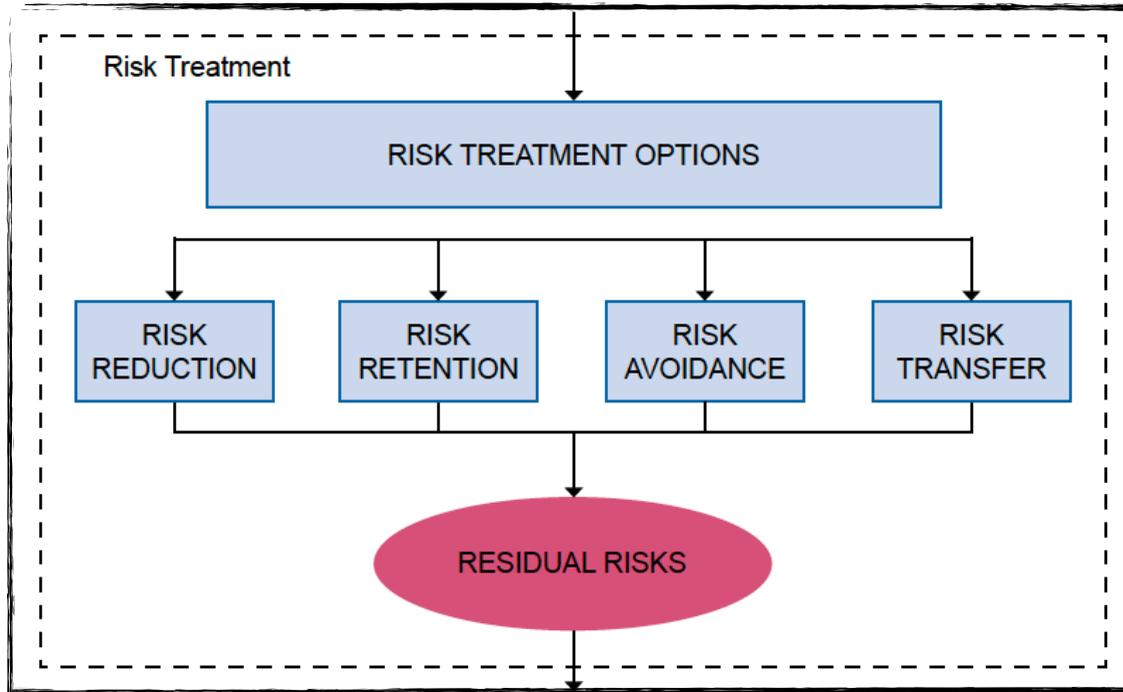
The organization shall retain documented information of the results of the information security risk treatment.

Evidence Of The Monitoring And Measurement Of Information Security (Clause 9.1)

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

- what needs to be monitored and measured, including information security processes and controls;
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- when the monitoring and measuring shall be performed;
- who shall monitor and measure;
- when the results from monitoring and measurement



Risk Treatment Options Based On ISO/IEC 27005

- shall be analysed and evaluated; and
- who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

The ISMS Internal Audit Program And The Results Of Audits Conducted (Clause 9.2)

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

- conforms to

- the organization's own requirements for its information security management system; and
- the requirements of this International Standard;
- is effectively implemented and maintained. The organization shall:
- plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
- define the audit criteria and scope for each audit;
- select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- ensure that the results of the audits are reported to relevant management; and
- retain documented information as evidence of the audit programme(s) and the audit results.

Evidence Of Top Management Reviews Of The ISMS (Clause 9.3)

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

- the status of actions from previous management reviews;
- changes in external and internal issues that are relevant to the information security management system;
- feedback on the information security performance, including trends in:

- nonconformities and corrective actions;
- monitoring and measurement results;
- audit results; and
- fulfilment of information security objectives;
- feedback from interested parties;
- results of risk assessment and status of risk treatment plan; and
- opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

Evidence Of Nonconformities Identified And Corrective Actions Arising (Clause 10.1)

When a nonconformity occurs, the organization shall:

- react to the nonconformity, and as applicable:
 - take action to control and correct it; and
 - deal with the consequences;
- evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
 - reviewing the nonconformity;
 - determining the causes of the nonconformity; and
 - determining if similar nonconformities exist, or could potentially occur;
- implement any action needed;
- review the effectiveness of any corrective action

taken; and

- make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:
 - the nature of the nonconformities and any subsequent actions taken, and
 - the results of any corrective action.

Various Others

Annex A mentions but does not fully specify further documentation including the rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, information security

incident response procedures, relevant laws, regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

However, despite Annex A being normative, organizations are not formally required to adopt and comply with Annex A: they can use other structures and approaches to treat their information risks.

Certification auditors will almost certainly check that these fifteen types of documentation are (a) present, and (b) fit for purpose.

The standard does not specify precisely what form the documentation should take, but section 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a fairly formal ISO 9000-style approach.

Electronic documentation (such as intranet pages) are just as good as paper documents, in fact better in the sense that they are easier to control and update.

Certification

Certified compliance with ISO/IEC 27001 by a respected certification body is entirely optional but is increasingly being demanded from suppliers and business partners by organizations that are (quite rightly!) concerned about the security of their information, and about information risks throughout the supply chain/supply network.

Certification brings a number of benefits above and beyond mere compliance, in much the same way that an ISO 9000-series certificate says more than just “We are a quality organization”.

Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires senior management approval (which is an advantage in security awareness terms, at least!).

The certificate has marketing potential and brand value, demonstrating that the organization takes information security management seriously.

ISO 27001 Audit Programs

The primary objectives of internal ISMS audits include monitoring the extent to which the ISMS meets the requirements of the organization, and the requirements of ISO/ IEC 27001 (conformity control), and monitoring the implementation and effectiveness of the measures taken (implementation and effectiveness control).

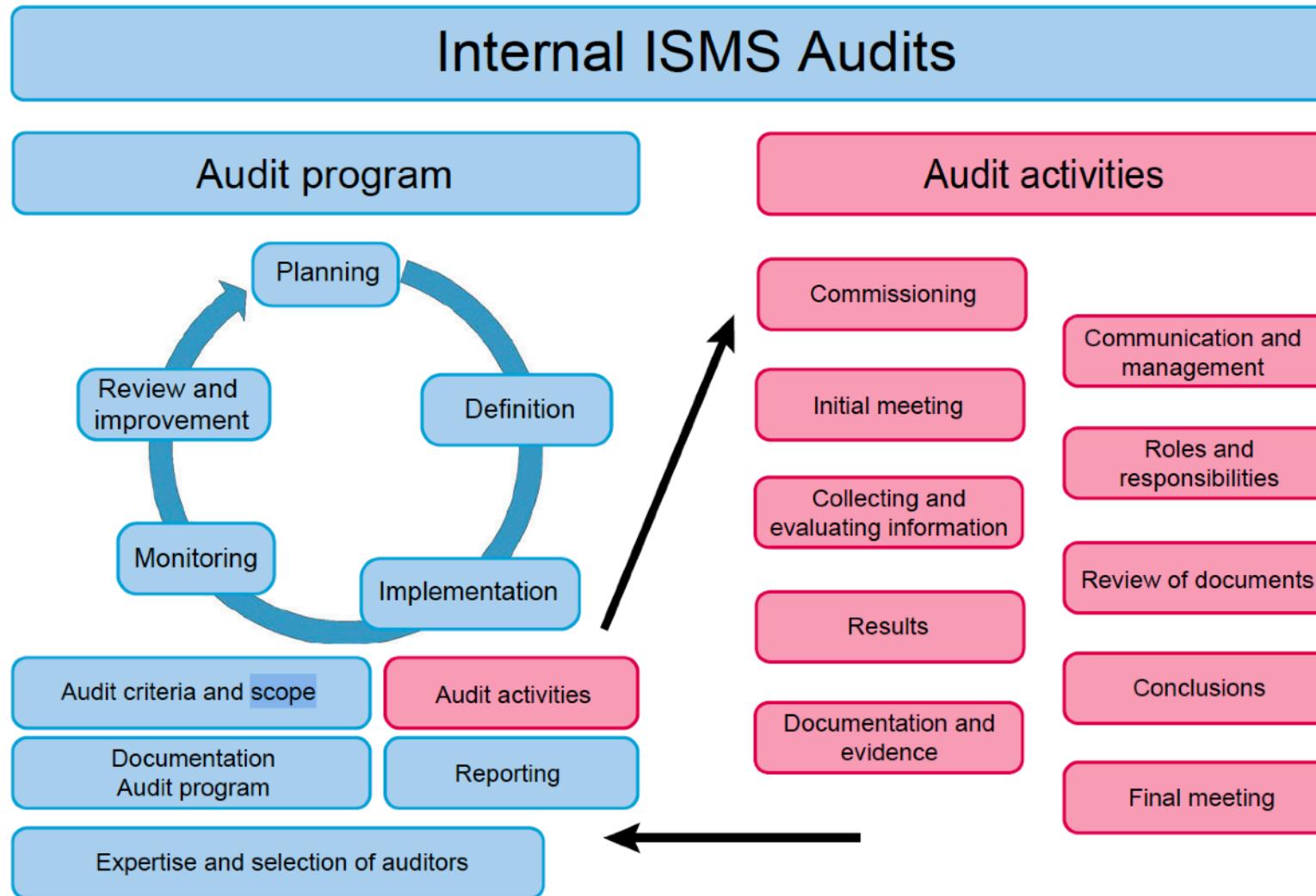
To that end, an audit program must be planned and implemented; it should govern aspects such as frequency, procedure, roles and responsibilities, planning requirements, traceability, and reporting. In addition, a method for dealing with corrective and preventive actions (the measures derived directly from the audits) must be defined, and it must be determined

who will follow up to ensure that the measures are implemented.

The audit program is intended to ensure that all the business processes covered by the ISMS (in accordance with the scope) are audited at least once every three years in terms of the applicable provisions and guidelines on information security and in terms of conformity with the ISMS. Evidence of the audit must be provided.

For purposes of the standard, the term ‘internal audits’ does not refer to internal audits in the narrow sense, although this department may be the one to actually conduct internal audits.

In practice, the internal ISMS audits are a primary task of the ISMS officer/CISO, who – in cooperation with an internal audit team or external support, if necessary – plans and manages audits.



Structure For Internal ISMS Audits (Audit Program vs. Audit Activities)

Success Factors For Practical Implementation

A distinction can be drawn between two areas when implementing internal audits:

1. The 'audit program'/'audit framework,' which serves as an organizational scaffolding for controlling and monitoring all activities in the context of internal audits and as an interface to other processes in the ISMS.
2. The actual 'audit activities' that include the planning and practical execution of individual internal audits.
 - The purpose of the audit activities is to implement the audit program within the company.
 - It is a good idea to coordinate with the internal auditing department.
 - In larger organizations, it is often recommendable to

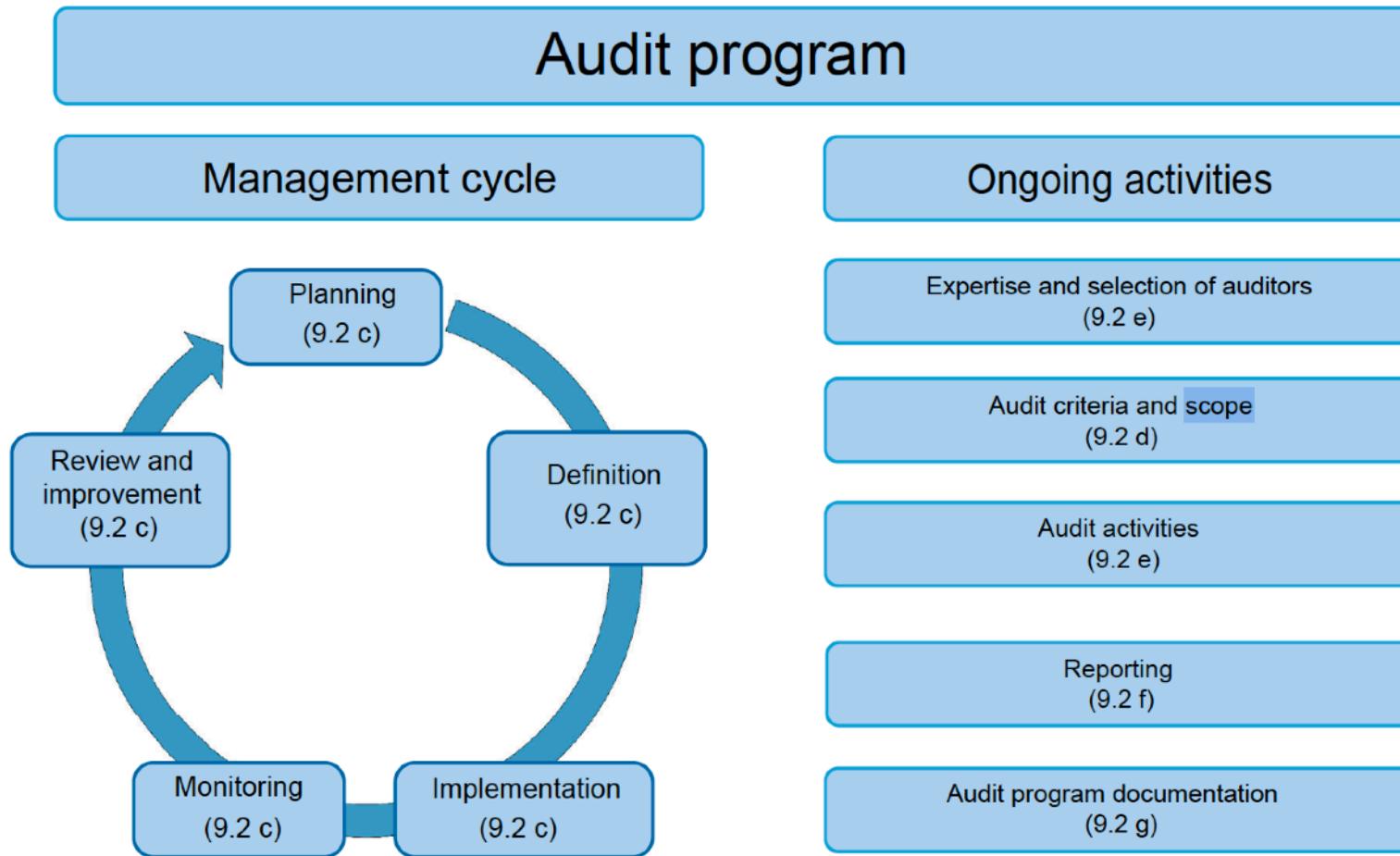
separate these two departments; an audit team leader is then responsible for the audit program, while a team of auditors carries out the internal audits.

- It must be ensured that the overall design and operational management of the audit program are optimally tailored toward achieving the IS objectives. In this way, the organization will achieve the best possible return on investment for the resources it puts toward auditing.

The audit program The audit program is a cyclical process, which includes the sub-processes planning, definition, implementation, monitoring, and review and improvement of the audit program itself.

- the importance of the affected processes (core processes, damage effects, business criticality) and IT systems and the results of previous audits must be considered in the audit program and in risk-based planning of specific audit activities.

- general audit criteria must be defined in the audit program. Depending on the size of the organization, the number of audits conducted, and the desired degree of detail in the audit program, the specific scope of individual audits can also be directly defined here.
- completed audits must be documented and associated information (such as audit reports) must be provided as evidence that the audit program has been implemented.
- management reports with information about the audit program's performance and about the audit activities and their results must be regularly generated.



Audit Program Requirements

ISO 27001 Step-By-Step Implementation Guide

If you are starting to implement ISO 27001, you are probably looking for an easy way to implement it. From getting buy-in from top management, to going through activities for implementation, monitoring, and improvement, in this ISO 27001 checklist you have the main steps your organization needs to go through if you want to achieve ISO 27001 certification.

Step 1. Obtain Management Support

This one may seem rather obvious, and it is usually not taken seriously enough. But this is the main reason why most of ISO 27001 certification projects fail – management is either not providing enough people to work on the project, or not enough money.

Step 2. Treat It As A Project

The implementation of an Information Security Management System (ISMS) based on ISO 27001 is a comprehensive project, involving various activities and lots of people, lasting several months (or more than a year). If you do not clearly define what is to be done, who is going to do it, and in what time frame (i.e., apply

project management), you might as well never finish the job.

Step 3. Define The Scope

If you are a larger organization, it probably makes sense to implement ISO 27001 only in one part of your organization, thus significantly lowering your project risk; however, if your company is smaller than 50 employees, it will be probably easier for you to include your whole company in the scope.

Step 4. Write An Information Security Policy

The Information Security Policy (or ISMS Policy) is the

highest-level internal document in your ISMS – it shouldn't be very detailed, but it should define some basic requirements for information security in your organization. But what is its purpose if it is not detailed?

The purpose is for management to define what it wants to achieve, and how to control it.

Step 5. Define The Risk Assessment Methodology

Risk assessment is the most complex task in the ISO 27001 project – the point is to define the rules for identifying the risks, impacts, and likelihood, and to define the acceptable level of risk. If those rules were not clearly defined, you might find yourself in a situation where you get unusable results.

Step 6. Perform The Risk Assessment & Risk Treatment

Here you have to implement the risk assessment you defined in the previous step – it might take several months for larger organizations, so you should coordinate such an effort with great care. The point is to get a comprehensive picture of the internal and external dangers to your organization’s information.

The purpose of the risk treatment process is to decrease the risks that are not acceptable – this is usually done by planning to use the controls from Annex A.

In this step, a Risk Assessment Report has to be written, which documents all the steps taken during the risk

assessment and risk treatment process. Also, an approval of residual risks must be obtained – either as a separate document, or as part of the Statement of Applicability.

Step 7. Write The Statement Of Applicability

Once you have finished your risk treatment process, you will know exactly which controls from Annex A you need (there are a total of 114 controls, but you probably won’t need them all). The purpose of this document (frequently referred to as the SoA) is to list all controls and to define which are applicable and which are not, and the reasons for such a decision; the objectives to be achieved with the controls; and a description of how they are implemented in the organization.

The Statement of Applicability is also the most suitable document to obtain management authorization for the

implementation of the ISMS.

Step 8. Write The Risk Treatment Plan

Just when you thought you had resolved all of the risk-related documents, here comes another one – the purpose of the Risk Treatment Plan is to define exactly how the controls from the SoA are to be implemented – who is going to do it, when, with what budget, etc. This document is actually an implementation plan focused on your controls, without which you wouldn't be able to coordinate further steps in the project.

Step 9. Define How To Measure The Effectiveness Of Controls

This is another task that is usually underestimated in a management system. The point here is – if you can't measure what you've done, how can you be sure you have fulfilled the purpose? Therefore, be sure to define how you are going to measure the fulfillment of objectives you have set both for the whole ISMS, and for security processes and/or controls.

Step 10. Implement The Controls & Mandatory Procedures

This might be easier said than done. This is where you have to implement the documents and records required by clauses 4 to 10 of the standard, and the applicable controls from Annex A. For more about ISO 27001-required documents and records, read the article [List of mandatory documents required by ISO 27001](#). For more about Annex A, read the article [How to structure the documents for ISO 27001 Annex A controls](#)

This is usually the riskiest task in your project because it means enforcing new behavior in your organization.

Often, new policies and procedures are needed (meaning that change is needed), and people usually

resist change – this is why the next task (training and awareness) is crucial for avoiding that risk.

Step 11. Implement Training And Awareness Programs

If you want your personnel to implement all of the new policies and procedures, first you have to explain to them why they are necessary, and train your people to be able to perform as expected. The absence of these activities in a management system is the second most common reason for ISO 27001 project failure.

Step 12. Operate The ISMS

This is the part where ISO 27001 becomes an everyday

routine in your organization. The crucial word here is: “records.” ISO 27001 certification auditors love records – without records, you will find it very hard to prove that some activity has really been done. But records should help you in the first place – by using them, you can monitor what is happening – you will actually know with certainty whether your employees (and suppliers) are performing their tasks as required.

Step 13. Monitor The ISMS

What is happening in your ISMS? How many incidents do you have, and of what type? Are all the procedures carried out properly?

This is where the objectives for your controls and measurement methodology come together – you have to check whether the results you obtain are achieving

what you have set in your objectives. If not, you know something is wrong – you have to perform corrective and/or preventive actions.

Step 14. Internal Audit

Very often, people are not aware that they are doing something wrong (on the other hand, they sometimes are, but they don’t want anyone to find out about it). But being unaware of existing or potential problems can hurt your organization – you have to perform an internal audit in order to find out such things. The point here is not to initiate disciplinary actions, but to take corrective and/or preventive actions.

Step 15. Management Review

Management does not have to configure your firewall, but they must know what is going on in the ISMS, i.e., if everyone performed their duties, and if the ISMS is achieving the desired results, fulfilling the defined requirements, etc. Based on that, the management must make some crucial decisions.

Step 16. Corrective And Preventive Actions

The purpose of the management system is to ensure that everything that is wrong (so-called “non-conformities”) is corrected, or hopefully prevented. Therefore, ISO 27001 requires that corrective and preventive actions are done systematically, which means

that the root cause of a non-conformity must be identified, and then resolved and verified. (Read the article Practical use of corrective actions for ISO 27001 and ISO 22301).

This ISO 27001 step-by-step guide has clarified what needs to be done – although ISO 27001 is not an easy task, it is not necessarily a complicated one. You just have to plan each step carefully.

ISO 27001 - Roles And Responsibility In Organizations

Understanding security roles and responsibilities, and why they are vital to the success of your security program is very crucial.

When building your Information Security Management System (ISMS) as part of ISO 27001 program implementation, one of the most important elements of the system of management for your security program is ensuring all stakeholders understand their roles and responsibilities.

Why Understanding Roles is Critical to the Security Program?

Implementing an information security program is truly an organization wide initiative. It takes security, department level, and organization wide leadership to support, adopt, drive, and socialize information security concepts. A siloed security program will never be able to rise above the level of compliance check-the-box.

The good news is that most leaders across the organization understand the importance of information security and are typically willing to support a right-sized and well thought-out security program. If you are charged with implementing the security program, it is your job to to communicate the “why” and the “what” behind the security program. If you are seeking to align

with ISO 27001 – defining and communicating roles and responsibilities is also required to achieve certification.

Five Typical Roles and Responsibilities

While the specific naming and place on the organizational chart may vary – all security programs have at least five “role types”. These role types are a minimum requirement for any security program and a requirement to fulfill the requirements outlined in clauses 4-10 of ISO 27001.

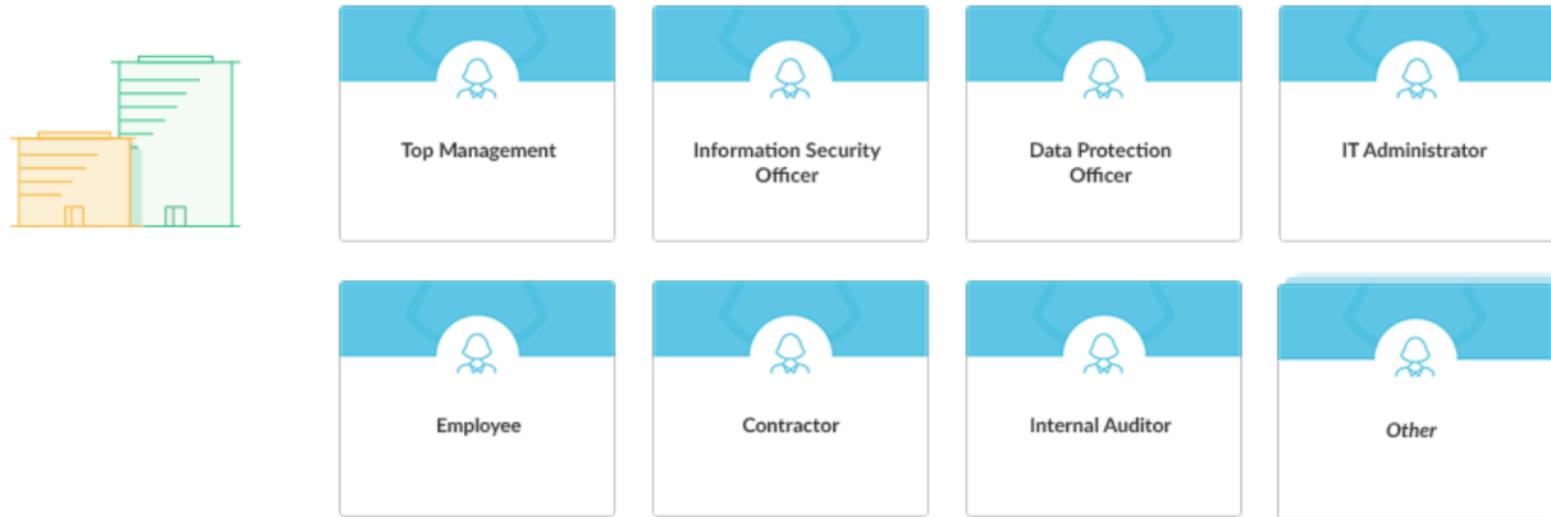
1. Security Leadership

The defined leader of an information security program varies widely dependent upon organization shape and

size. In some small organizations security leadership may be shared with members of other departments such as information technology, engineering, or legal. In more mature organizations the security leader may be a Chief Information Security Officer (CISO), VP, or Director level security practitioner. In either case, security leadership must own the information security program (including formalized responsibility and authority).

Typical duties include:

- Defining the context of the security program including aligning the program to business objectives and ensuring appropriate stakeholders have been considered
- Setting the strategic objective, building the security program road-map, allocating budget and human resources
- Developing, tracking, and reporting security KPIs to relevant stakeholders (e.g., Customers, Leadership, the Board of Directors)



ISO/IEC 27001 Main roles in Information Security Management System

2. Security Risk Management

Security risk management is often one or many committees and sub-committees charged with overall risk management activities as related to information security. Sometimes called an Information Risk Council (IRC), Security Risk Council (SRC), or similar these functions must oversee and own policy and risk management activities.

These organizations are also design to be cross functional in nature, not siloed to information security or technology practitioners. Often department heads from finance, HR, sales, legal, and others are representatives. Cross functional representation helps drive organizational change and socialization of information security initiatives.

Typical duties include:

- Attendance to Quarterly Risk Management meetings

(Quarterly is usually a good cadence that is no overly burdensome on members)

- Defining the risk management process including risk analysis, risk measurement, and risk treatment
- Overseeing the annual risk assessment including periodically reviewing the risk register
- Reviewing, approving, socializing, and enforcing policy decisions across the organization
- Reviewing results of security assessments and other security related activities
- Charged with Incident Management and Incident Response (often this is a sub-committee or separate team under the risk management function)

3. Internal Audit

A key philosophical principle of ISO 27001 is Management's commitment to continuous improvement. Internal audit is a key part of monitoring and driving continuous improvement of your security program. Because internal audit must be both qualified and independent of the ISMS, many organizations choose to leverage third parties to perform security assessments.

Typical duties include:

- Internal audit must be qualified (e.g., an ISO 27001 Lead Auditor, or similar) to perform a security assessment
- Independent from the ISMS (e.g., No conflict of interest such as operating controls or governing the ISMS).
- Creating an annual audit plan
- Executing against the audit plan (e.g., Performing

audits of the ISMS and 114 ISO 27001 Annex A controls)

- Reporting results to management

4. Control Owners

Control owners are the individuals responsible for operation of the various tasks and duties that make up the security program. Many of these duties are defined by the 114 controls outlined in ISO 27001 annex A. These roles will vary widely from organization to organization, but it is critical that an organization take the time to define these duties and periodically measure their performance.

Typical duties include:

- Secure engineering, development, and operations (devops)

- Security operations such as vulnerability management, intrusion monitoring, and active defense
- Network Engineering and perimeter support
- Availability of systems including back-up and restoration

5. All Employees

It must be emphasized that all employees play a critical role when it comes to information security. (It is of note that countless studies site end users as the most common origin of security incidents.)

Typical duties include:

- Basic end-user security awareness training (e.g., Email Phishing, Internet Browsing)
- Training on the do's and don'ts based on their role (for example, a person in finance should understand never

- to change the routing number of a client's bank account based on an email request)
- Training based on regulatory or contractual requirements such as GDPR or Sarbanes Oxley

Next Steps For The Pursuit Of Growth

“ The Life You Want, The Marriage You Want... The Family That You Want, Is Going To Be Fueled By The Business You Build.”

– Russell Brunson, Author and CEO of ClickFunnels

How to Guarantee Your Position As A Successful Entrepreneur

I feel that it's now my job to inspire you to actually implement and execute what you have learned from this program.

Let's face it: The big, vast economy is not going to accommodate you with more opportunities and more business without you taking some serious initial steps.

The economy most likely doesn't even know you exist; up until now, you only operated as a small part of it, or you're just getting started.

The government is not going to bail you out on your difficult days, and they certainly are not going to help you to advance and conquer on your entrepreneurship journey while you are setting yourself free.

Something tells me that you didn't pick up this program because you are comfortable or satisfied with where

you're in your career and business. Chances are you want to change or improve your career, build a side hustle, increase your level of flexibility and independence, or you want to simply have much security and more available options in life and business. Otherwise, you wouldn't have finished this program.

Taking the time to pick up this program and study it suggests that you truly do want to do something different. For this, I acknowledge and congratulate you.

Well done to you on getting this program. I applaud you for starting it and even more for finishing it. Now, if you want the world to give you a standing ovation, put lessons in it to work.

Interestingly, one of the most effective ways of perfecting these disciplines is to help others attain success and implement these actions themselves. When people with common goals and motivations come

together, they tend to learn faster and become a support system for one another. So gather a group of like-minded and highly driven people who refuse to live by the norms of the mediocre. Assemble a group to discuss this program and brainstorm it with you. Ask your family, friends, and other like-minded entrepreneurs to make this program as a team.

Then help one another apply and commit to using the actions, hold one another accountable to these commitments. **This is the game, and it's the most fun game that I've ever played. You now started getting the skills you need to start building your empire or make it bigger.**

During this journey that we've been on together through this program, we've covered a lot of things, but there are still a lot I am going to provide you. Everything you've learned in this program is literally the same thing we would discuss and do with you if one of my SkillFront

advisors or I had a chance to fly to you and sit in your office. You now have access to the skills that will unlock the path of success in your business and ultimately in your life.

You've just learned what took me a decade to discover and master

Tony Robbins often talks about how reading a course is like taking a decade of someone's life and compressing it down to a day.

My entrepreneurial journey hasn't been all sunshine and roses. There have been many ups and downs, and I fought hard to learn all these skills in this program you have in your hands, and all other programs we have released, and we're going to release. It is my honor and privilege to be able to share them with you.

I still remember the excitement as I learned each of these skills and used them for the business for the first time. Whenever I meet someone talking about our programs and skills they are learning from SkillFront, I get slightly jealous about how much fun it would be to rediscover all these skills.

At this moment, you just officially became our latest SkillFront Entrepreneur. I hope that you had as much fun learning as I did when I started my own journey.

We will end this program now, and we will be happy to serve you again with another program.

If you want to get up-to-the-minute ideas, keep yourself informed about other SkillFront Programs like this one, follow our pages on [LinkedIn](#), [Facecourse](#), [Twitter](#), and [Instagram](#).

P.S. Don't forget, you're just one skill away...



Thanks For Learning With The SkillFront

I want to thank you for taking the time with our program. We hope you enjoyed studying this lecture as much as we had enjoyed while we were creating it. It would be our greatest pleasure if we managed to help you to learn a thing or two, which will guide you on your own exciting entrepreneurship journey.

This program is a playcourse. Don't just study it once and go on with business as usual. Keep it handy and refer to it often. Having these tactics and using them hand in hand will give you strategies to grow your business and career geometrically.

And with that ... Thank you so much once again, and I wish you all the success you can dream of.

— Yeliz Obergfell, SkillFront

What's Coming Next?

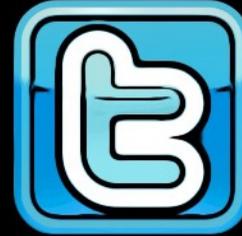
If you want to get up-to-the-minute ideas, keep yourself informed about SkillFront Programs like this one, follow our pages on



[LinkedIn](#)



[Facebook](#)



[Twitter](#)



[Instagram](#)

SKILLFRONT