ISO27K TOOLKIT

By **ComplyMate**

What does ISO stand for?

- **ISO (the International Organization for Standardization)** and **IEC (the International Electrotechnical Commission)** form the specialized system for worldwide standardization.
- 160 national bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

What is ISO27K?

- ISO27K is the series of international standards that provide the specification for information security in organisation and an Information Security Management System (ISMS).
- An ISMS is a framework of policies and procedure that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

How does an organisation get ISO 27001 certified?

The ISO/IEC 27001 certification process is essentially the same as that for ISO 9001 and other management systems. It is an external audit of the organization's ISMS in three main phases:

- Pre-audit
- Certification audit
- Post-audit

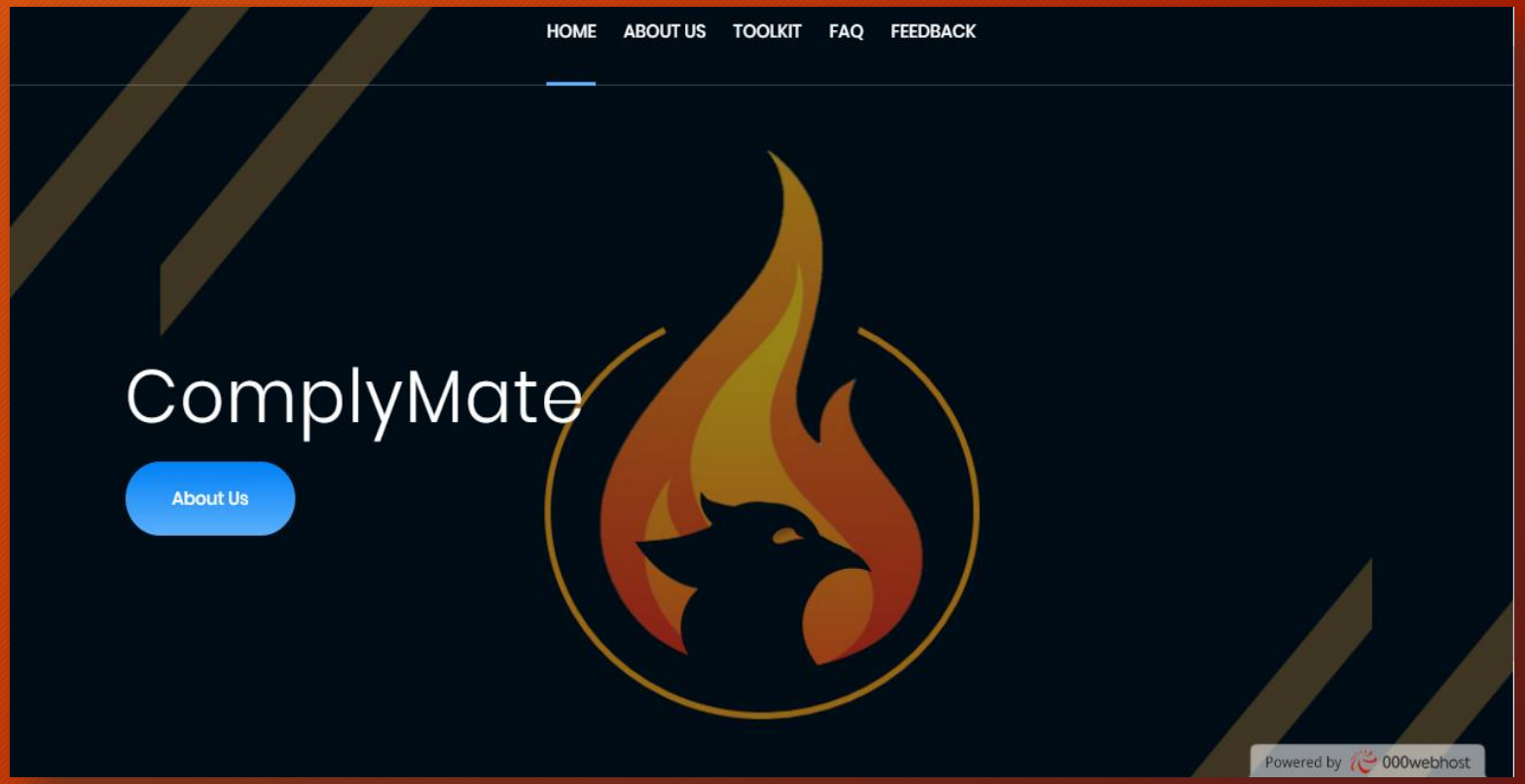
It typically takes anywhere from 3 - 12 months to implement and certify ISO27K requirements for an ISMS and it can cost as low as $6000 to $50000 depending on the scale of the organisation.

THE ISO27K TOOLKIT

- The documentation necessary to create a conformant ISMS, particularly in more complex businesses, can reach up to a thousand pages according to the scale of the organisation.
- The ISO27K Toolkit provides a complete set of easy-to-use, customizable documentation templates along with guidelines and other supporting documents.
- A collection of 90+ documents spanning over 500 pages.
- Aligned with ISO 27001, 27002 and some other ISO27K standards aw well as EU GDPR.
- Open Source project in an effort to give back to the community, the toolkit can be downloaded for free from the ComplyMate website.

Our Website: ComplyMate.xyz

- The website is made under the brand name ComplyMate.
- The toolkit is provided on easily accessible web platform so that anyone can download the toolkit completely free of cost.



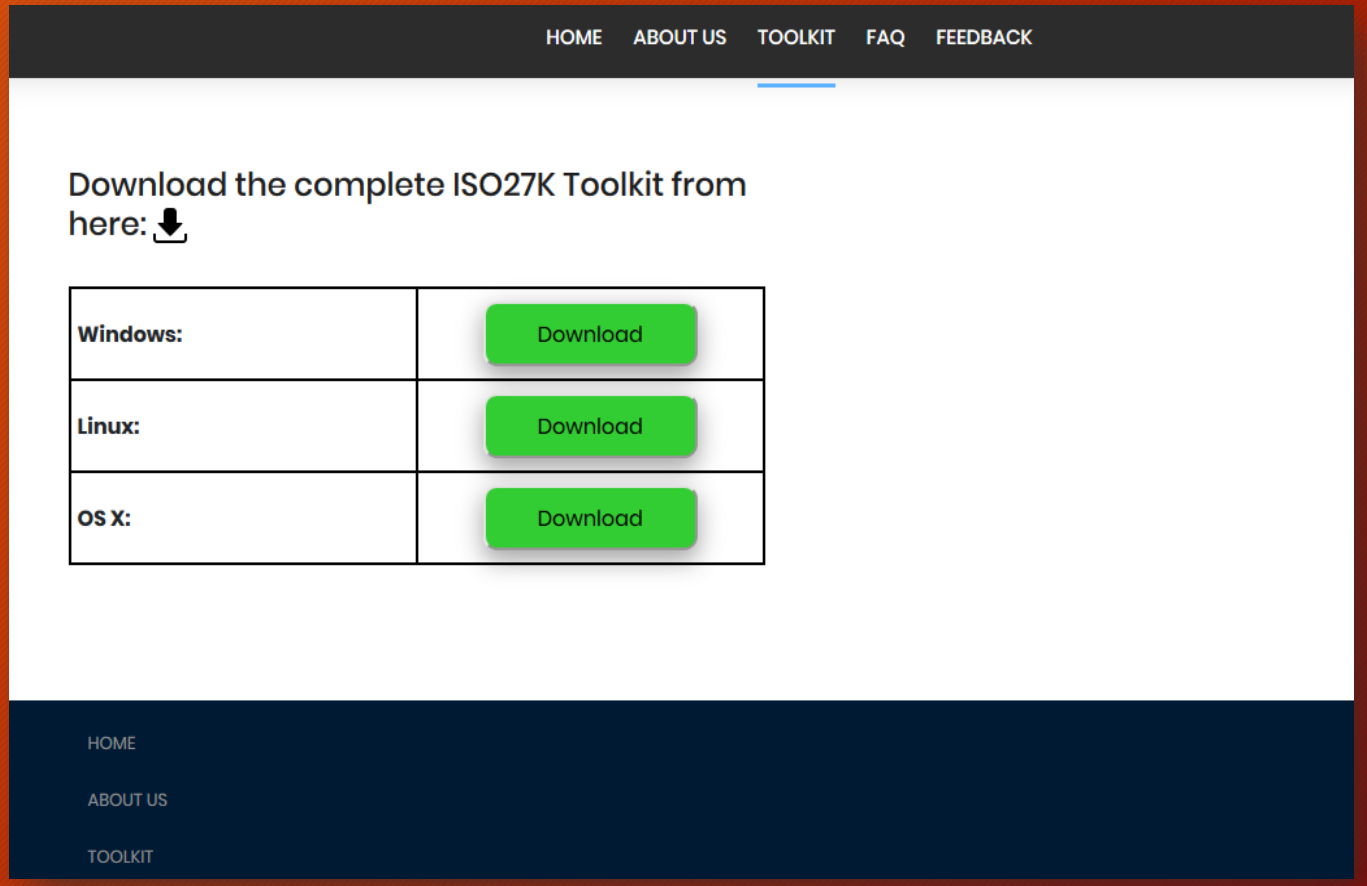
Website Development

- **HTML:** is used for frontend development.
- **CSS:** to format the layout of Web pages.
- **JavaScript:** to add dynamic and special effect on pages.
- **PHP:** for backend development of the website.

Download Page

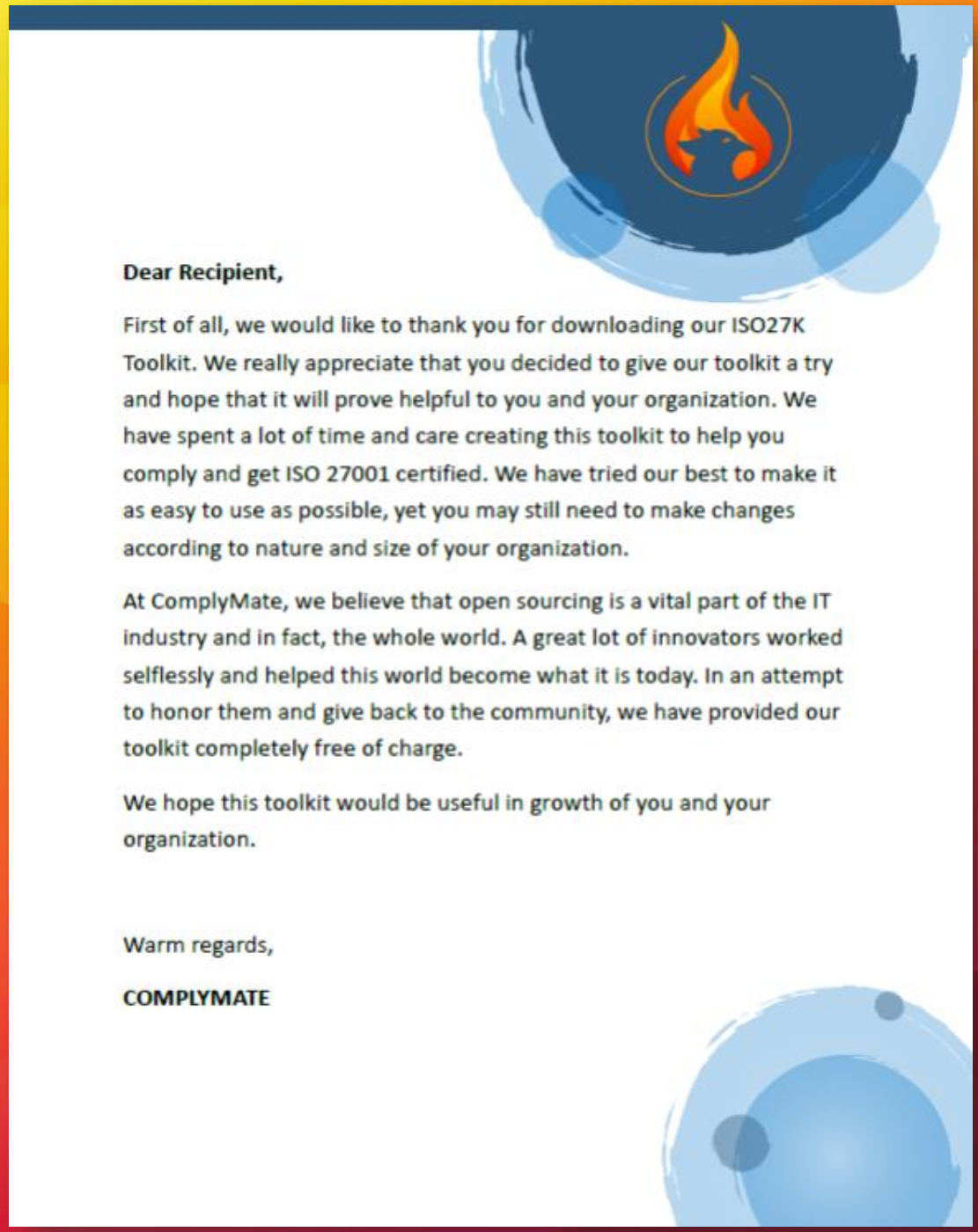
- The website's download page provides three different archive formats of the toolkit specific to the following platforms:

1. Windows
2. Linux
3. OS X



A Happy Beginning

This toolkit is our ongoing endeavour to serve the people or organisations and it's only befitting that we begin this toolkit by showing our gratitude to every user who downloads our product and welcome them to the ComplyMate family.



Dear Recipient,

First of all, we would like to thank you for downloading our ISO27K Toolkit. We really appreciate that you decided to give our toolkit a try and hope that it will prove helpful to you and your organization. We have spent a lot of time and care creating this toolkit to help you comply and get ISO 27001 certified. We have tried our best to make it as easy to use as possible, yet you may still need to make changes according to nature and size of your organization.

At ComplyMate, we believe that open sourcing is a vital part of the IT industry and in fact, the whole world. A great lot of innovators worked selflessly and helped this world become what it is today. In an attempt to honor them and give back to the community, we have provided our toolkit completely free of charge.

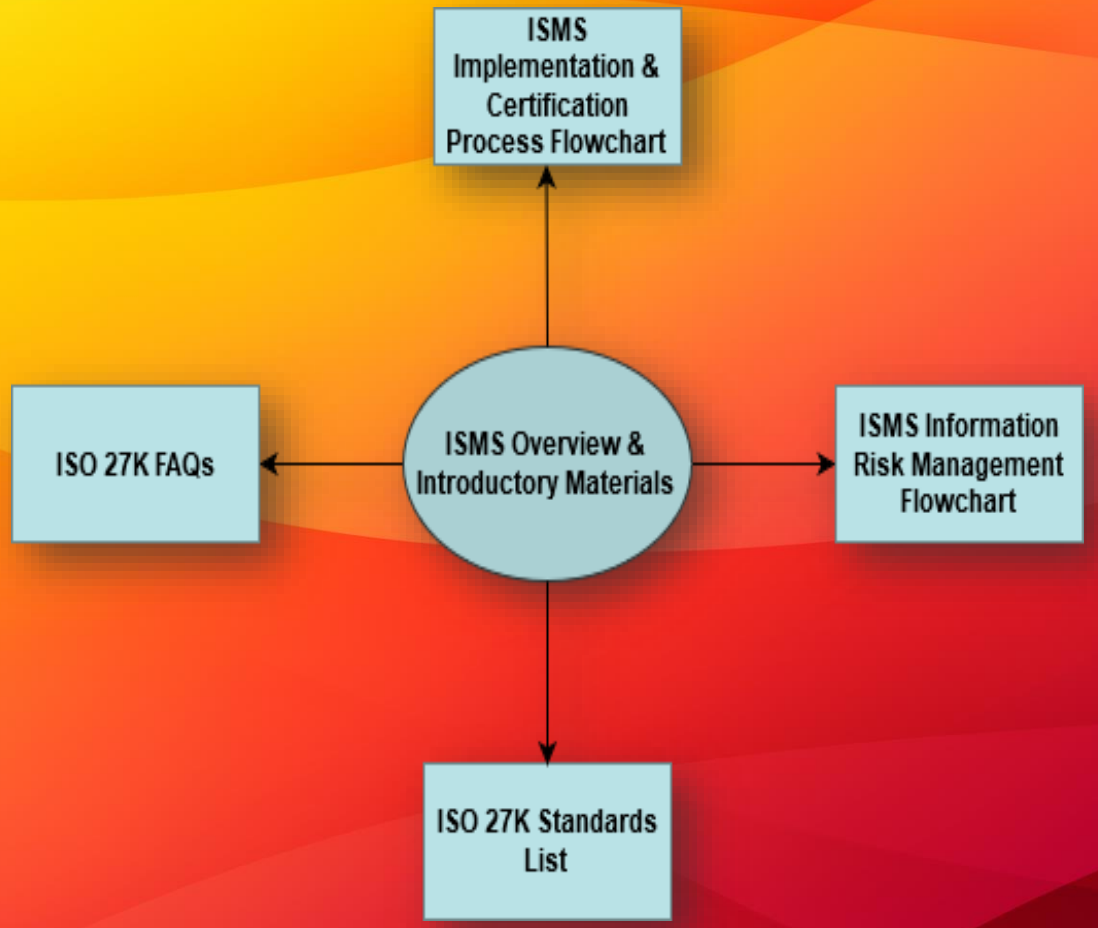
We hope this toolkit would be useful in growth of you and your organization.

Warm regards,

COMPLYMATE

ISMS OVERVIEW & INTRODUCTORY MATERIALS

- This module provides the organisations with a basic overview of the ISMS, its implementation and risk management processes.
- These processes are explained with the help of flowcharts, presentations and road maps as well.
- This module also has a list of FAQs and a list of all current and future ISO27K standards that will clear all the doubts of any organisation related to the ISMS.

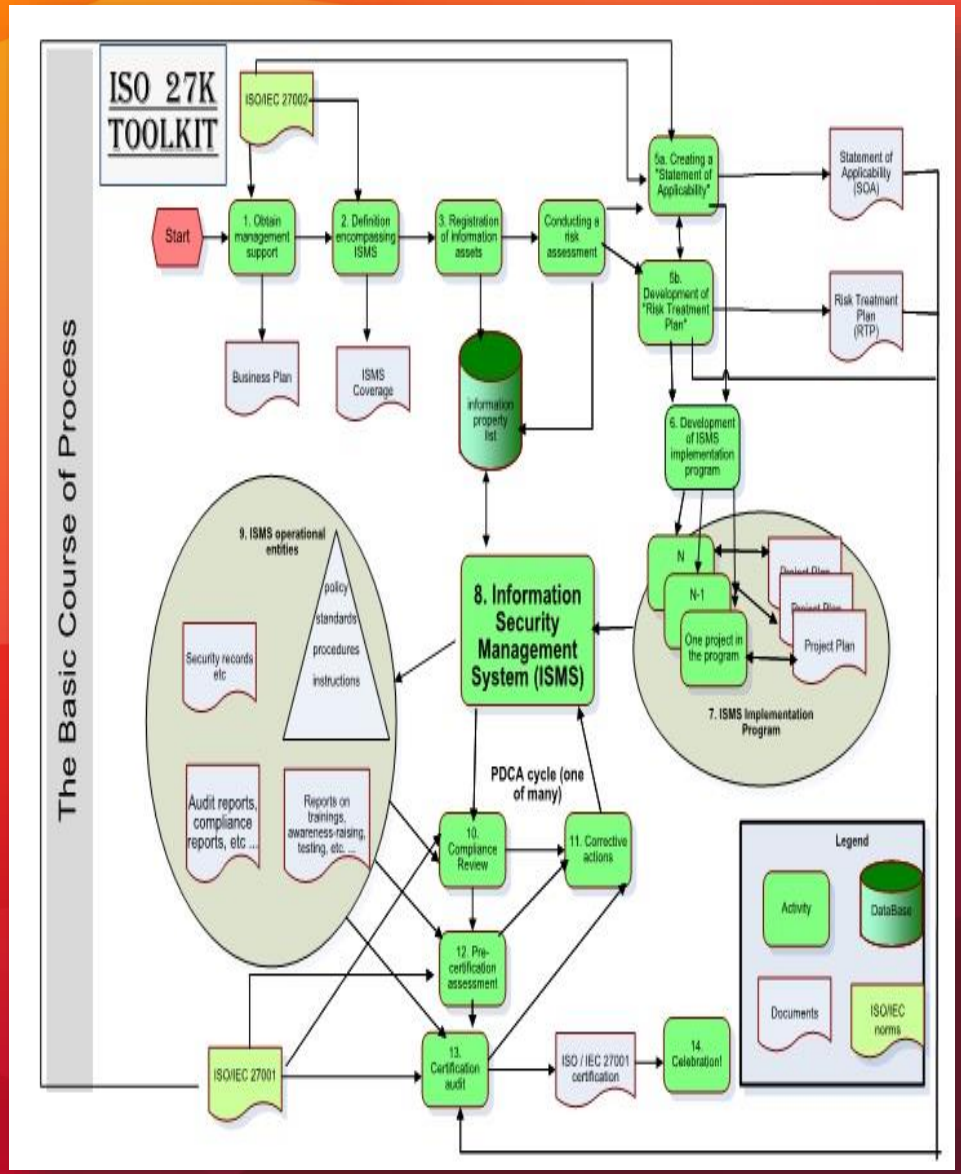


ISMS Implementation & Certification Process

- The whole process of implementing the ISMS and achieving certification has been explained through flowcharts in different languages as an effort to cross the language barrier.
- The flow chart gives a high level view of the major steps in the process.
- The process is also explained theoretically through a PowerPoint presentation in order to further simplify the process.

This is a generic summary - the details will vary from situation to situation. The main activities are as follows:

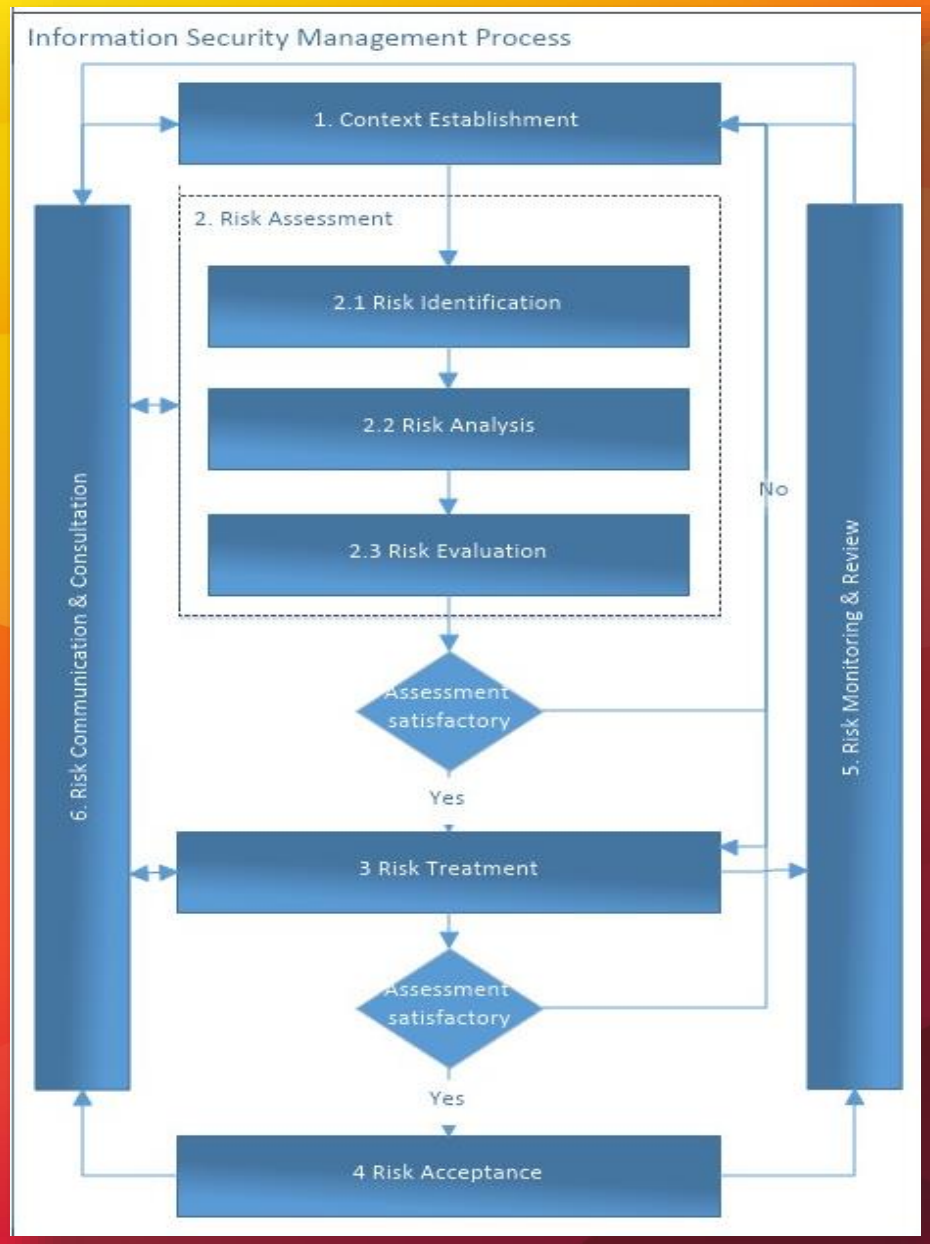
i. **Get management support**
ii. **Define ISMS scope**
iii. **Inventory your information assets**
iv. **Inventory your information assets**
v. **Prepare a S**tatement **o**f **A**pplicability
vi. **Prepare a R**isk **T**reatment **P**lan
vii. **Develop ISMS implementation program**
viii. **Run the ISMS implementation program**
ix. **Operate the ISMS**
x. **Collect ISMS operational artefacts**
xi. **Audit the ISMS**
xii. **Review compliance**
xiii. **Undertake corrective actions**
xiv. **Conduct a pre-certification assessment**
xv. **Certification audit**
xvi. **Celebration!**
xvii. **Operate the ISMS**



ISMS Risk Management Process

- Flow charts are provided that provide guidance on preparing a risk management process, emphasising on following points :

1. Establish the context of Risk.
2. Assess the Risk.
3. Apply Risk Treatment Plan.
4. Accept the Risk.
5. Monitor & Review the risk.
6. Communicate and consult about the risk.



ISMS GOVERNANCE, MANAGEMENT & IMPLEMENTATION GUIDANCE

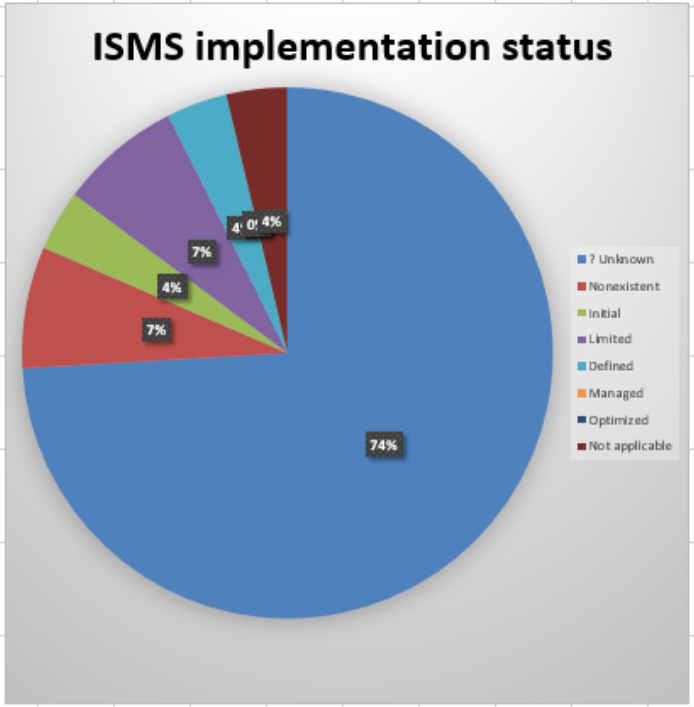
This module provides number of documents on effective governance, management and implementation of ISMS covering the following areas:

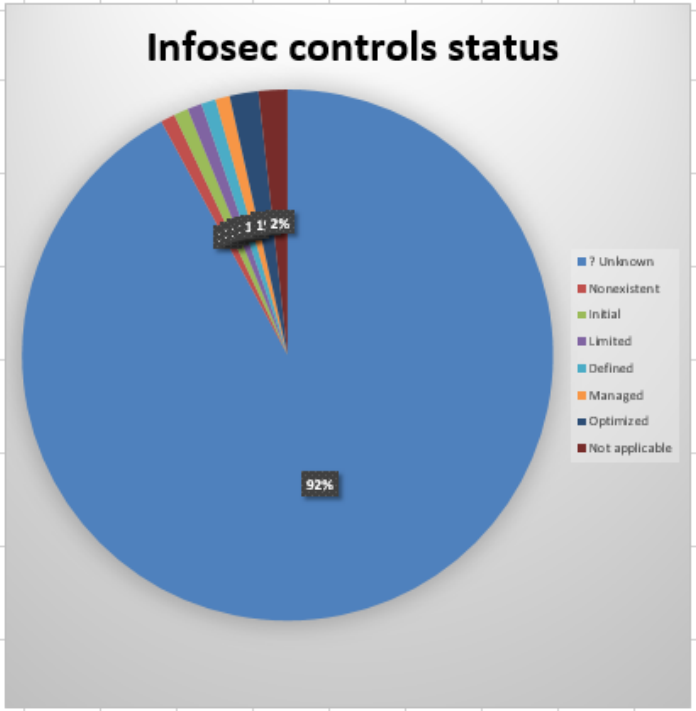
- **Benefits and costs of ISMS, standardization, structured approach, certification, compliance:**
  - **Information security risk reduction**
  - **Cost saving**
  - **Standardization**
  - **brand value**
- ***Direct benefits (*profits, cost-effective, compliance *)***
- ***Indirect benefits (h*uman relations, risk management, customer confidence*)***

Information Security Program Assessment covers following documentation:

- Controls(IS Policies, HR Security, Asset Management, Cryptography)
- ISMS *Management Review* Meeting: Purpose , Agenda , Recap
- ISMS Documentation Checklist

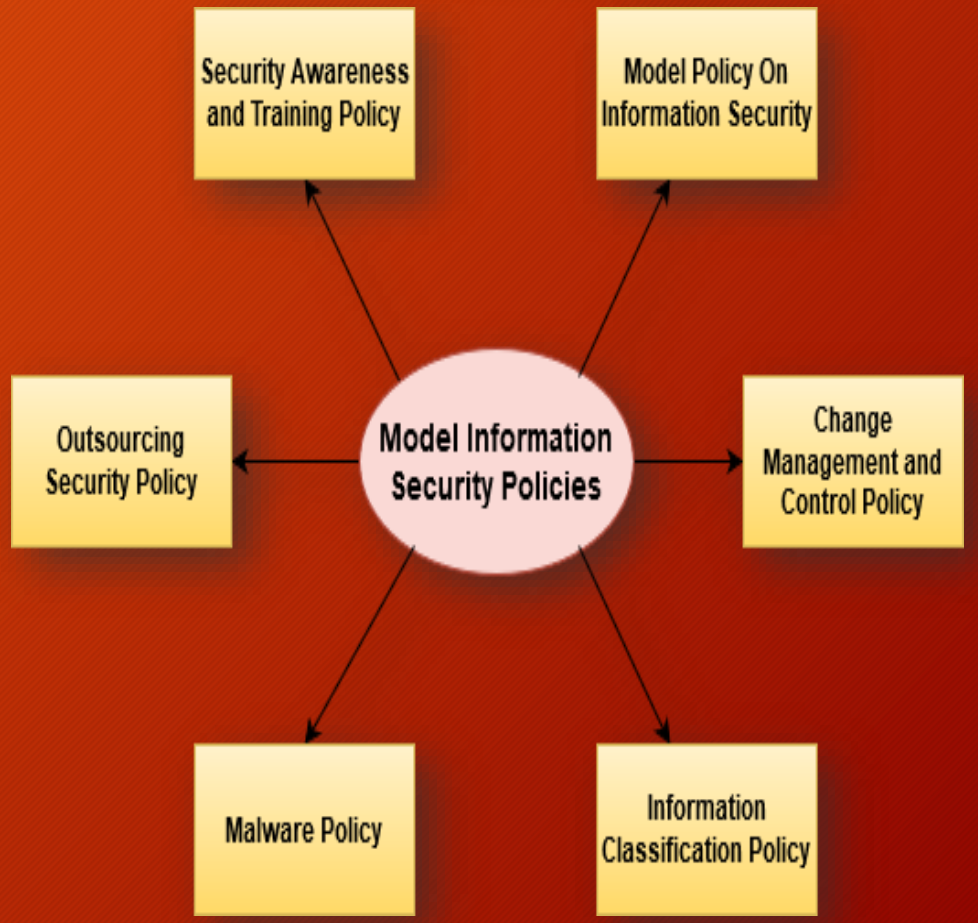
Status	Meaning	Proportion of ISMS requirements	Proportion of information security controls
? Unknown	Has not even been checked yet	74%	92%
Nonexistent	Complete lack of recognizable policy, procedure, control *etc*	7%	1%
Initial	Development has barely started and will require significant work to fulfill the requirements	4%	1%
Limited	Progressing nicely but not yet complete	7%	1%
Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	4%	1%
Managed	Development is complete, the process/control has been implemented and recently started operating	0%	1%
Optimized	The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors	0%	2%
	ALL requirements in the main body of ISO/IEC 27001 are mandatory IF your ISMS is to be	4%	2%





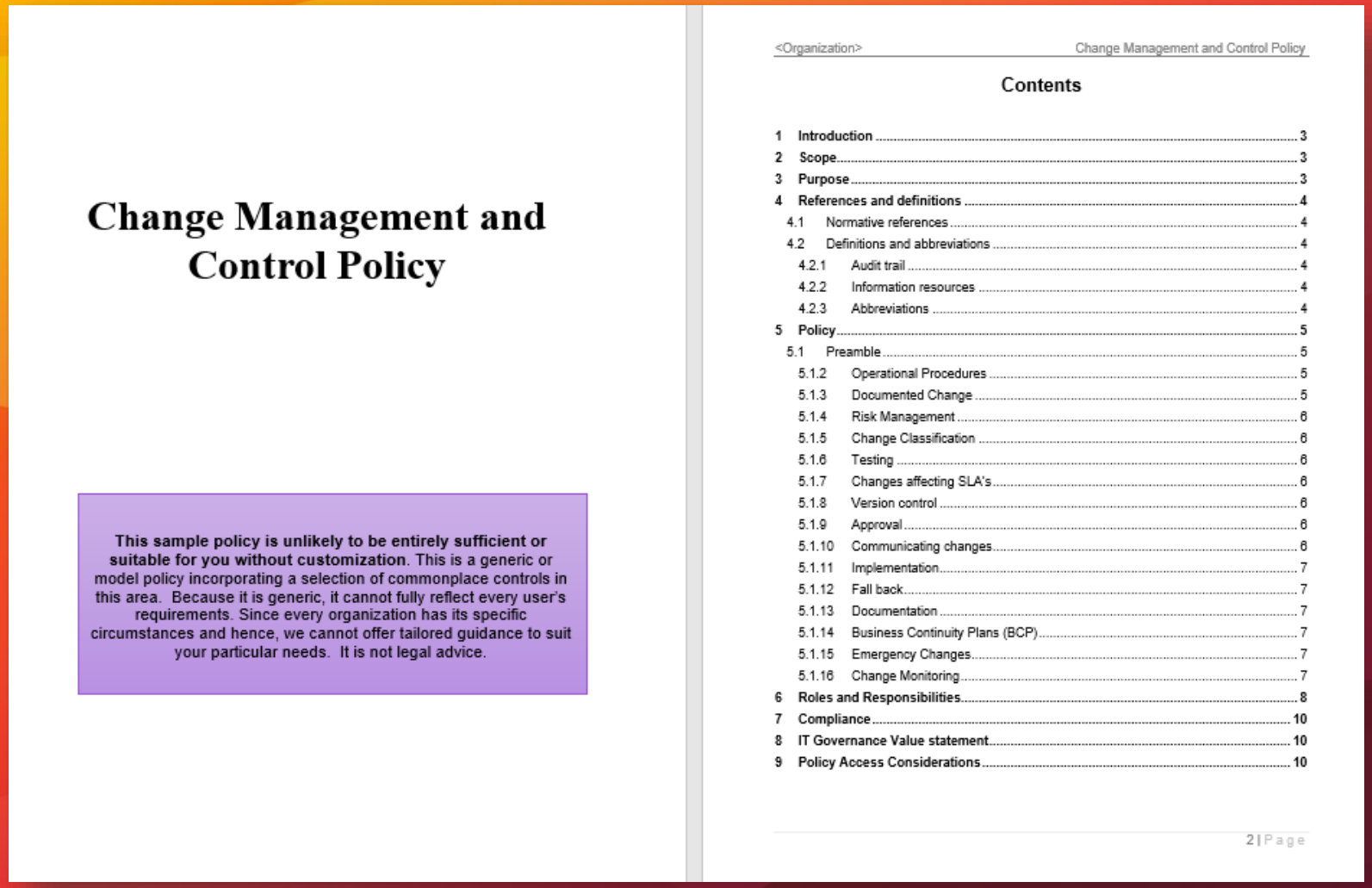
MODEL INFORMATION SECURITY POLICIES

- As a part of ISO 27001 project, the organisations must develop and document information security policies according to ISO 27001 requirements.
- These policies sets out the ISMS requirements of an organisation.
- It defines management direction for information security in accordance with business requirements and relevant laws and regulations.
- This toolkit will help the organisations in framing their policies and the organisations can customise these policies according to their requirements.



Following are the sample policies provided in the ISO27K Toolkit:

- **Modern Policy on Change Management and Control**
- **Model Policy on Information Classification**
- **Model Policy on Information Security**
- **Model Policy on Malware**
- **Model Policy on Outsourcing**
- **Model Policy on Security Awareness and Training**



Change Management and Control Policy

This sample policy is unlikely to be entirely sufficient or suitable for you without customization. This is a generic or model policy incorporating a selection of commonplace controls in this area. Because it is generic, it cannot fully reflect every user's requirements. Since every organization has its specific circumstances and hence, we cannot offer tailored guidance to suit your particular needs. It is not legal advice.

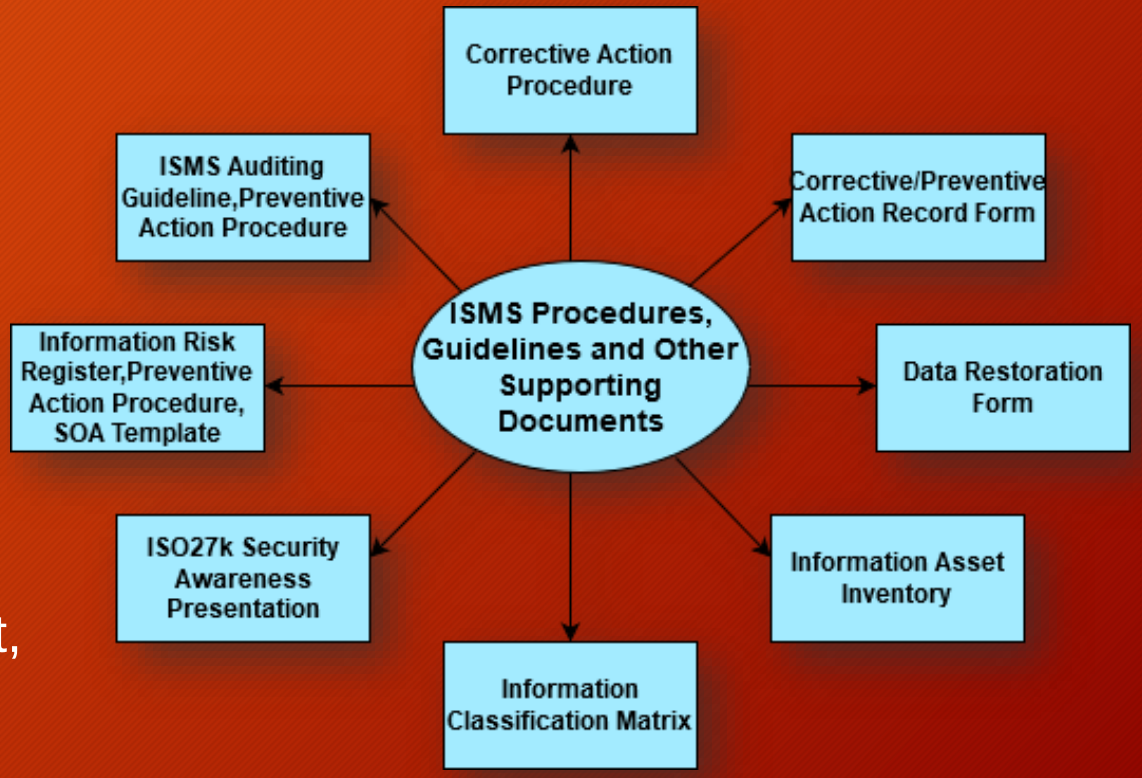
<Organization> Change Management and Control Policy

Contents

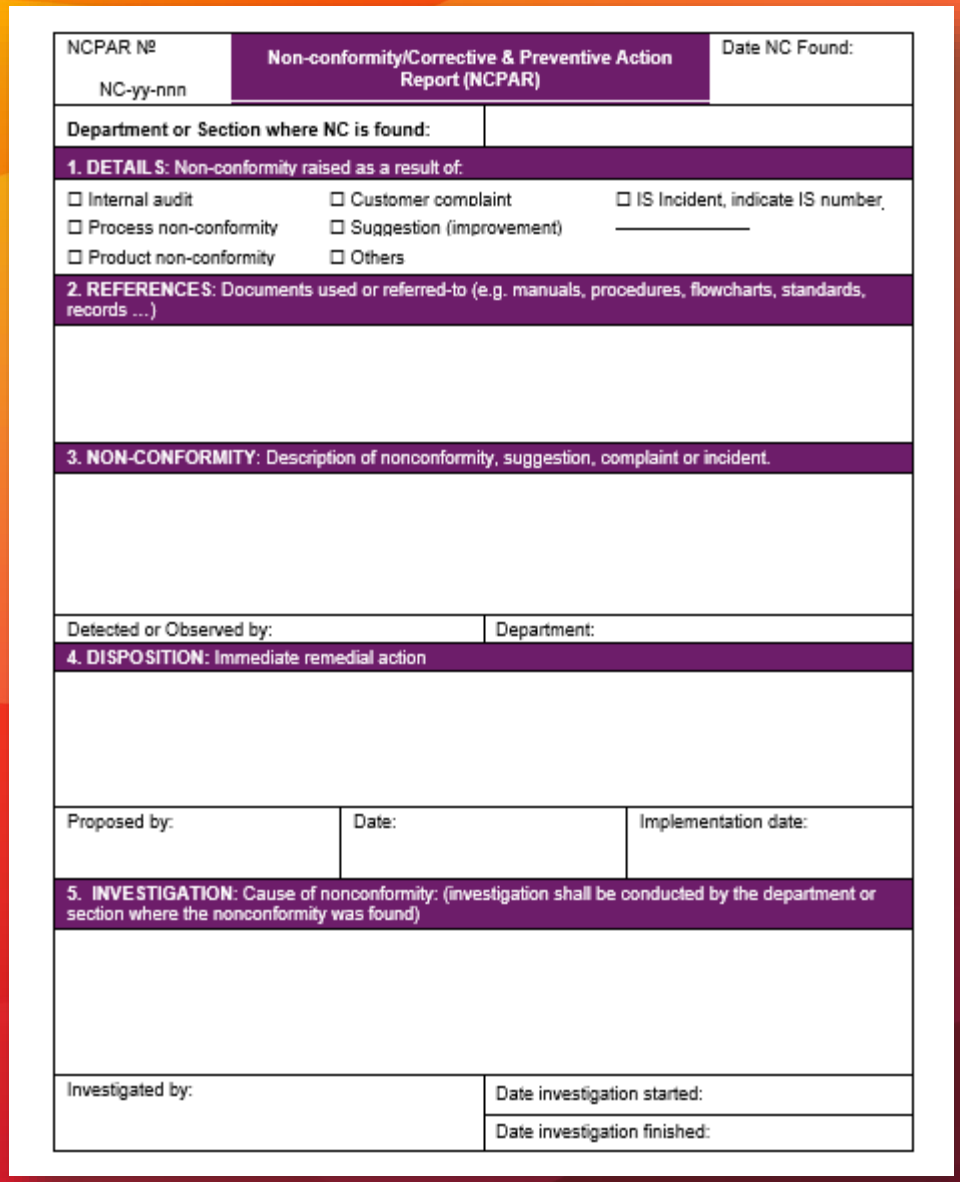
ISMS PROCEDURES, GUIDELINES AND OTHER SUPPORTING DOCUMENTS

This module provides documentations that include forms, checklists, guidelines and procedures covering a vast area of ISO 27001 requirements.

- **Asset Inventory** (Types [Availability, data classification, protection level])
- **Asset Register** (Digital, DB, software, people, network devices, computer)
- **Controls Checklist** (Obj [C,I,A], Type [detect, react, prevent, recover])



- Corrective Action Procedure (to eliminate the cause of non-conformities on the established ISMS)
- Data Restoration Form
- Failure Modes and Effects Analysis (FMEA) techniques [Risk Assessment (RA), controls, severity, portability]
- Information Asset Valuation (classification , owner ,CIA ,)
- Information Classification and Handling
- Non-conformity/Corrective & Preventive Action Report



NCPAR № NC-yy-nnn	**Non-conformity/Corrective & Preventive Action Report (NCPAR)**	Date NC Found:
Department or Section where NC is found:		

1. DETAILS: Non-conformity raised as a result of:

☐ Internal audit ☐ Customer complaint ☐ IS Incident, indicate IS number_____
☐ Process non-conformity ☐ Suggestion (improvement)
☐ Product non-conformity ☐ Others

2. REFERENCES: Documents used or referred-to (e.g. manuals, procedures, flowcharts, standards, records …)

3. NON-CONFORMITY: Description of nonconformity, suggestion, complaint or incident.

Detected or Observed by:	Department:

4. DISPOSITION: Immediate remedial action

Proposed by:	Date:	Implementation date:

5. INVESTIGATION: Cause of nonconformity: (investigation shall be conducted by the department or section where the nonconformity was found)

Investigated by:	Date investigation started:
	Date investigation finished:

Mapping between EU GDPR (European Union General Data Protection Regulation) and ISO27K Standards for organisations based in EU nations so that organisations that currently have an ISO27K ISMS in place already can easily align it with GDPR requirements but may need to make some adjustments and same is true vice versa.

Mapping between GDPR (the EU General Data Protection Regulation) and ISO27K Standards

Executive summary

The European Union (EU) General Data Protection Regulation (GDPR) - currently being introduced across Europe and beyond ahead of the May 2018 final implementation deadline - mandates numerous privacy arrangements and controls designed to protect personal data, many of which are also recommended by ISO/IEC 27001:2013, ISO/IEC 27002:2013 and other "ISO27K" standards. Organizations that currently have an ISO27K ISMS (Information Security Management System) are therefore likely to have many of the GDPR requirements in place already but may need to make some adjustments. Others may choose to implement an ISO27K ISMS as an overarching framework to manage privacy and personal information as part of the broader management of information risks, information security and related compliance, incident management and business continuity issues.

This document maps between the GDPR and ISO27K in the particular context of private/non-governmental organizations subject to GDPR.

ComplyMate and the ISO27K Toolkit

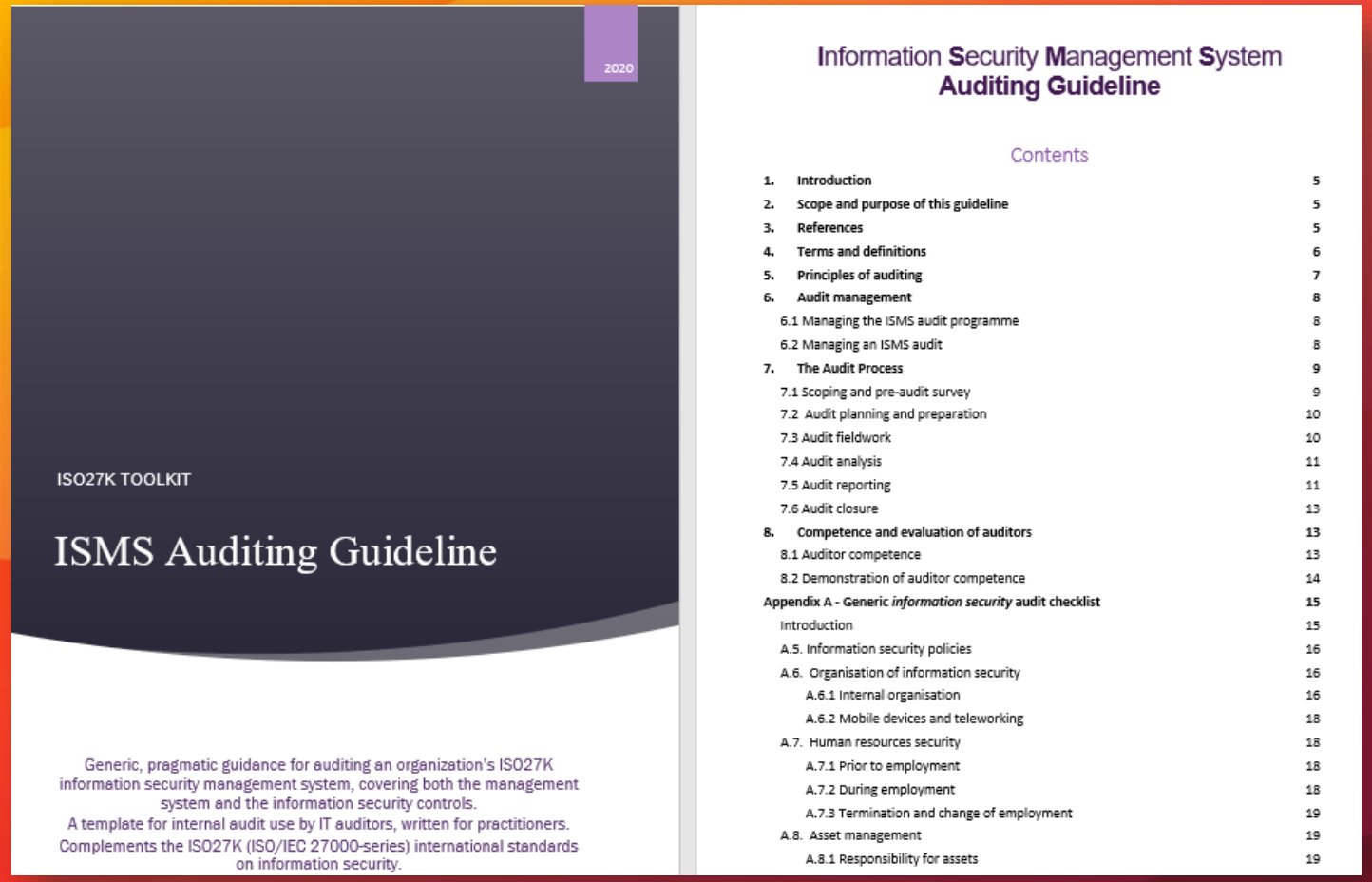
The complymate.xyz website has been running since April 2020 as a free public information resource concerning the ISO/IEC 27000-series information risk and security management standards ("ISO27K"). It is not an official ISO/IEC site, but an unofficial community project supporting users of the ISO27K standards.

The ISO27K Toolkit is a free collection of materials donated or created to guide and support users in implementing the ISO27K standards in their organisation. This mapping document demonstrates the power of crowdsourcing.

GDPR		ISO27K	
Article	Outline/summary	Control	Notes
	and networks) and in a business or corporate/organizational context (private home uses are not in scope).		built around a 'management system'. ISO27K systematically addresses information risks and controls throughout the organization as a whole, including but going beyond the privacy and compliance aspects.
3	GDPR concerns personal data for people in the European Union whether is it processed in the EU or elsewhere	A.18.1.4 *etc.*	ISO27K is global in scope. Any organization that interacts with people in the European Union may fall under GDPR, especially of course if they collect personal info.
4	GDPR privacy-related terms are formally defined here.	3	ISO/IEC 27000 defines most ISO27K terms including some privacy terms. Many organizations have their own glossaries in this area. **Check that any corporate definitions do not conflict with GDPR.**
Chapter II Principles			
5	Personal data must be: (a) processed lawfully, fairly and transparently; (b) collected for specified, explicit and legitimate purposes only; (c) adequate, relevant and limited; (d) accurate; (e) kept no longer than needed; (f) processed securely to ensure its integrity and confidentiality. [This is the latest incarnation of the original OECD principles published way back in 1980 <tips hat>.]	6.1.2, A.8.1.1 A.8.2 A.8.3 A.9.1.1 A.9.4.1 A.10 A.13.2 A.14.1.1 A.15 A.17 A.18 ... in fact, almost all!	Business processes plus apps, systems and networks must adequately secure personal information, requiring a comprehensive suite of technological, procedural, physical and other controls ... starting with an assessment of the associated information risks. See also 'privacy by design' and 'privacy by default' (Article 25). In order to satisfy these requirements, organisations need to know where personal info is, classify it and apply appropriate measures to address (a)-(f).

- **ISMS Auditing Guideline:** This guideline is particularly aimed at those performing ISMS internal audits and management reviews – **not** formal certification audits.

- **ISMS Internal Audit Procedure:** A sample procedure includes planning, execution, reporting and follow–up of ISMS internal audits.
- **Audit related documents are based on ISO 27001, 27002 and 27007.**



2020

ISO27K TOOLKIT

ISMS Auditing Guideline

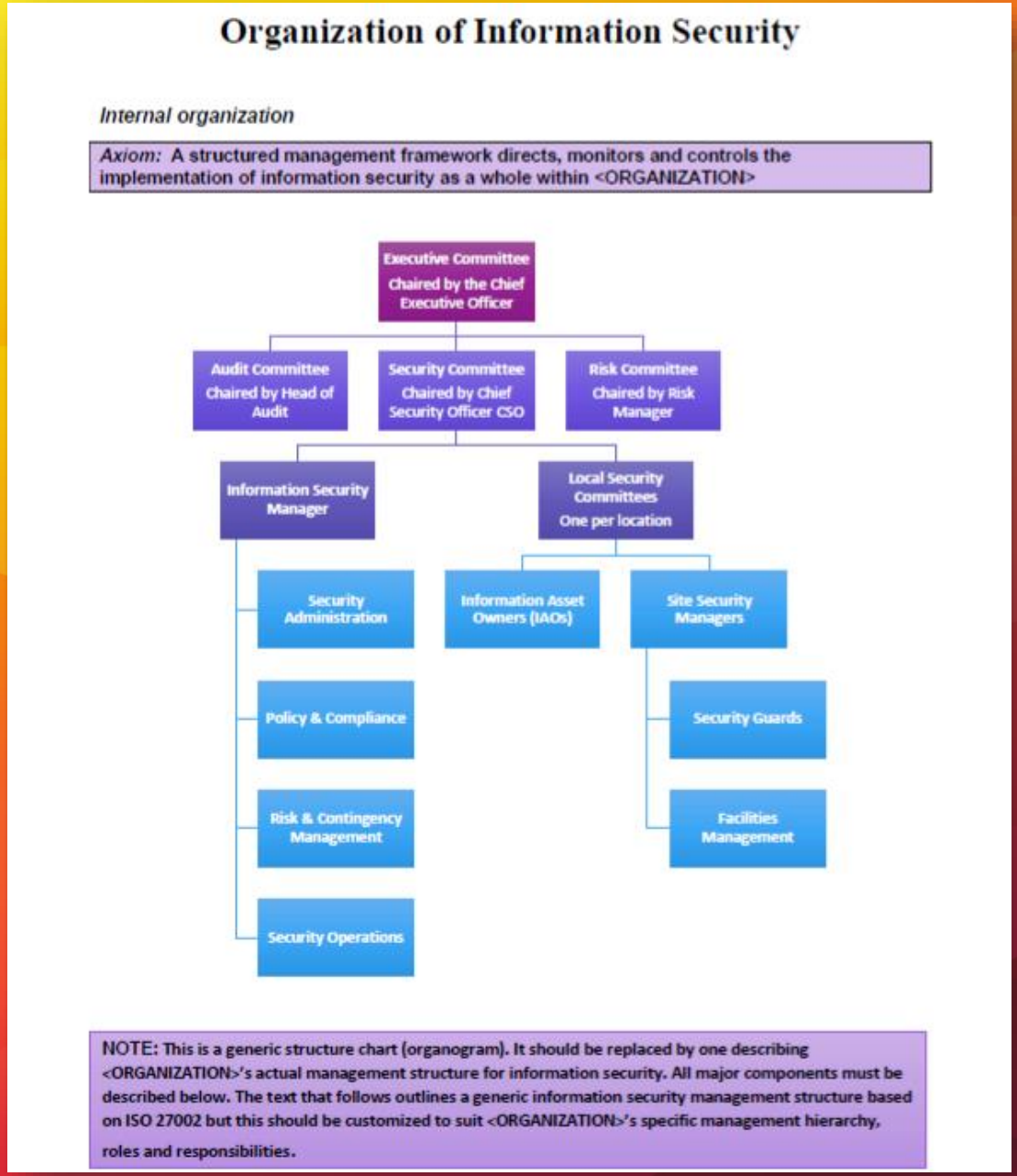
Generic, pragmatic guidance for auditing an organization's ISO27K information security management system, covering both the management system and the information security controls.
A template for internal audit use by IT auditors, written for practitioners.
Complements the ISO27K (ISO/IEC 27000-series) international standards on information security.

Information Security Management System
Auditing Guideline

Contents

ISMS RELATED JOB DESCRIPTIONS / ROLES AND RESPONSIBILITIES

- This module provides documents related to the organisational hierarchy, job descriptions related to the ISMS, their roles and responsibilities in the ISMS.
- **Organisation of Information Security:** This is a sample policy to define the roles and responsibilities of ISMS according to organisational hierarchy.
- **Roles and Responsibilities for Contingency Planning:** This document describes the responsibilities and competencies commonly associated with Contingency, Business Continuity, Business Resumption and IT Disaster Recovery Planning roles in organisations.

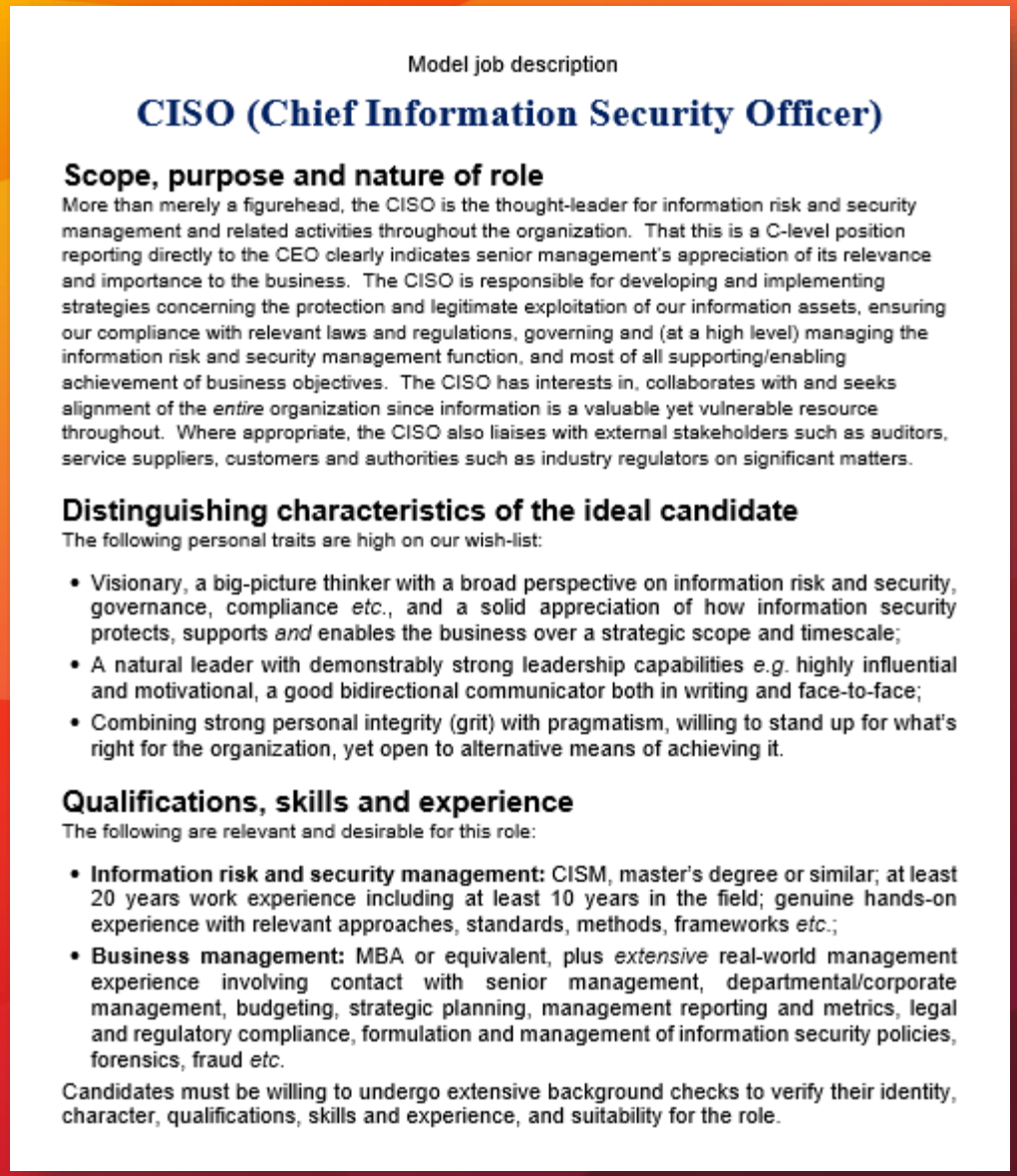


- **Technical Briefing on Information Security Roles and Responsibilities:** This briefing discusses the definition of information security roles and responsibilities based on 35 control objectives identified in ISO/IEC 27002:2013
- **RASCI Table:** The RASCI (Responsible, Accountable, Supporting, Consulting, Informed) table is a sample approach that associates roles in the organization with the all 114 controls of ISO/IEC 27002:2013.

ISO/IEC 27002 Section	Information Security Control	Department, Function or Role							
		CEO	CIO	ISM	RM	HR	LRC	Sec	IAO
5.1	Information security plus policy management support and commitment	A	C	C	O	C	C	C	R
6.1	Management framework and roles for information security management	A	C	C	O				R
6.2	Secure mobile computing and teleworking		R	C	O				A
7.1	Pre-employment screening			C	O	A			R
7.2	During employment: awareness, training and education		C	R	O	A			R
7.3	Post-employment exit processes			C	O	A			R
8.1	Information asset owners identified and held accountable		R	C	O			R	A
8.2	Classify information assets		R	C	O			R	A
8.3	Secure handling of storage media		A	C	O				
9.1	Business requirements for access to information assets including networks		A	R	O				A
9.2	Networks/systems access rights for users		R	C	O				A
9.3	User responsibilities including access passwords		R	C	O				A
9.4	Access rights for systems and applications		A	R	O				A
10.1	Cryptographic policy e.g. algorithms, key management		A	R	O				
11.1	Physical security for computer facilities		R	C	O			A	
11.2	Physical security for IT equipment, cabling etc. including safe disposal and clear desk policy		R	C	O			A	R
12.1	IT operating procedures and responsibilities		A	R	O				
12.2	Malware protection		A	R	O				

* CEO = Chief Executive Officer. CIO = Chief Information Officer and IT Department Generally. ISM = Information Security Management. RM = Risk Management. HR = Human Resources. LRC = Legal and Regulatory Compliance. Sec = Physical/site security. IAO = Information Asset Owners or Managers. A= Accountable. R = Responsible. O = Oversight and Review. C = Consultancy and advice.

- **Job Description:** This describes the job roles related to the ISMS. It includes scope, purpose, nature of role, distinguishing characteristics of the ideal candidate, relevant qualifications, skills and experience of a particular job role. ISO27K toolkit provide job descriptions for 30 most common roles in the ISMS, researched through different employment websites.



Model job description

CISO (Chief Information Security Officer)

Scope, purpose and nature of role

More than merely a figurehead, the CISO is the thought-leader for information risk and security management and related activities throughout the organization. That this is a C-level position reporting directly to the CEO clearly indicates senior management's appreciation of its relevance and importance to the business. The CISO is responsible for developing and implementing strategies concerning the protection and legitimate exploitation of our information assets, ensuring our compliance with relevant laws and regulations, governing and (at a high level) managing the information risk and security management function, and most of all supporting/enabling achievement of business objectives. The CISO has interests in, collaborates with and seeks alignment of the *entire* organization since information is a valuable yet vulnerable resource throughout. Where appropriate, the CISO also liaises with external stakeholders such as auditors, service suppliers, customers and authorities such as industry regulators on significant matters.

Distinguishing characteristics of the ideal candidate

The following personal traits are high on our wish-list:

- Visionary, a big-picture thinker with a broad perspective on information risk and security, governance, compliance *etc.*, and a solid appreciation of how information security protects, supports *and* enables the business over a strategic scope and timescale;
- A natural leader with demonstrably strong leadership capabilities *e.g.* highly influential and motivational, a good bidirectional communicator both in writing and face-to-face;
- Combining strong personal integrity (grit) with pragmatism, willing to stand up for what's right for the organization, yet open to alternative means of achieving it.

Qualifications, skills and experience

The following are relevant and desirable for this role:

- **Information risk and security management:** CISM, master's degree or similar; at least 20 years work experience including at least 10 years in the field; genuine hands-on experience with relevant approaches, standards, methods, frameworks *etc.*;
- **Business management:** MBA or equivalent, plus *extensive* real-world management experience involving contact with senior management, departmental/corporate management, budgeting, strategic planning, management reporting and metrics, legal and regulatory compliance, formulation and management of information security policies, forensics, fraud *etc.*

Candidates must be willing to undergo extensive background checks to verify their identity, character, qualifications, skills and experience, and suitability for the role.

ISO27K Toolkit by ComplyMate