MITRATECH

ISO 27001 Certification
Alyne x Mitratech
White Paper

Achieving ISO 27001 Certification

A step-by-step guide into becoming ISO 27001 certified with the help of Mitratech's Alyne GRC platform of the future.

INTRODUCTION

Mitratech customers leverage the Alyne GRC platform for effectively managing their risk, information security and control frameworks. Naturally, their requirements for the protection of sensitive information are critical factors of importance.

The ISO/IEC 27001:2013 certification remains one of the most trusted and widely recognized standards for Information Security Management across regions and industry sectors. Mitratech's Alyne has been ISO 27001 certified since 2017 and has successfully passed the most recent audit in 2021 to maintain this certification.

Logically, Mitratech used the internal instance of Alyne for building its Information Security Management System (ISMS). As the famous Microsoft saying goes: 'Eat your own dogfood.'

In this document we share some of the key learnings we gained along the way and provide a detailed guide for any organization looking to obtain an ISO/IEC 27001:2013 certification with the help of Mitratech's Alyne GRC platform of the future. In the following pages you'll find a summary of the main steps to follow in order to achieve the certification, a brief explanation on how to implement the necessary actions within Alyne and how to leverage the platform's capabilities to reduce effort and increase efficiency.

Using Mitratech's Alyne to implement your ISMS provides your organization with some powerful advantages:

1. Out-of-the-Box Content

Defining the right policies and developing a control framework compliant with the ISO/IEC 27001:2013 requirements takes a lot of time if you are starting from scratch. With Mitratech's Alyne, this is ready on day one.

2. Risk Analytics

An ISMS is very much based on a Plan-Do-Check-Act cycle. A core lever for driving this cycle are identified risks, which should then be mitigated to continuously improve the ISMS. Identifying and quantifying the risks can be a difficult task. Mitratech's Alyne risk analytics are a powerful tool for this purpose.

3. Collaboration and Awareness

Involving management and people responsible for processes affected by the ISMS is a core aspect of an ISMS. Providing a platform that makes it easy for the team to collaborate and document the activities relevant to the management system is essential to limit the effort of the team.

4. Framework Synergies

Likely ISO/IEC 27001:2013 is only one framework relevant to your overall governance program. With Mitratech's Alyne you can easily reuse the ISMS aligned with ISO/IEC 27001:2013 for your privacy management, IT governance, extended security management and many other areas without reinventing the wheel.

STEP 1: IMPLEMENTATION GUIDE

When beginning with the implementation of the ISMS, it is important to establish what your organization is looking to gain from this. An ISMS is a powerful tool to increase cyber security maturity and resiliency.

Implementation Steps

Involve the Right Stakeholders

Ensure support and availability from a core set of stakeholders relevant to the ISMS. First, it is necessary to define the owner of the ISMS. This is generally the Chief Information Security Officer (CISO).

On a management level, managing directors responsible for risk, IT and cyber security need to be involved. On an operational level, you will need to involve stakeholders from operational risk, business continuity management, IT operations, IT strategy, internal controls, outsourcing, audit and potentially legal and compliance. Obviously this list may vary, depending on how roles and responsibilities are defined within your organization.

Define Objectives and Overall Scope

It is highly recommended to focus the scope of the ISMS on specific areas of your organization. For example, Mitratech's Alyne ISO/IEC 27001:2013 certification was focussed on areas that involve the processing of client data in sales and customer support processes, as well as on the provision of our service. Processes such as accounting, HR or legal have been excluded. Your organization's scope should, therefore, be influenced by the overall motivation for the ISMS as well as the cyber risk exposure.

Identify In-Scope Processes

Once the overall scope has been defined, processes that are in scope for the ISMS must be identified. Consider that processes should be core to the scope, involve the processing of sensitive information or facing specific threats that require management through an ISMS. Select cautiously, as this is not a one-off exercise. The defined scope will require both continuous management in the ISMS and a recurring annual audit.

Lessons Learned

1. Limit the Scope

Excessive coverage will increase management effort with potentially low returns in cyber resilience.

2. Drive from Top Down

This needs to come from management to work.

3. Make Required Effort Transparent

Let people know from the beginning exactly how much and when effort is required.

STEP 2: MANAGEMENT STATEMENT

The guiding document for the ISMS is the management statement. This defines the overall approach to the management system, documents the support of management, outlines core management structures and documents the completed reviews.

Implementation Steps

Structure Document

The document should follow the structure of the standard and describe your organization's approach to these main topics. Using the exact wording of the standard makes the audit much easier.

Describe Implementation

Describe in a few paragraphs how your organization approaches and implements the individual chapters. Keep these brief, the details are in the control framework. The longer the description, the more difficult reviews, sign-offs and audits become.

Link Document to Control Framework

In Alyne, link the document to the control set covering your ISMS control set. Additionally, there are further controls where you can link the Management Statement. The objective here is to make the linkage between the management statement and the applicable controls as easy and transparent as possible.

Lessons Learned

1. Stick to the ISO/IEC 27001:2013 Structure

It is not worth reinventing the wheel as this document is almost exclusively for auditors.

2. Use a Document with Version Control

Google Docs is perfect for this use case as you have traceability of all changes, you can define major versions in the version history and multiple people can edit simultaneously. Additionally, you are able to link one document and do not need to continuously update the links every time you update a new version of the document.

STEP 3: MANAGEMENT STATEMENT

The next phase of shaping the scope of the ISMS, after selecting the process applicability, is defining the scope of applicability. This means selecting which controls, out of the Annex A of the ISO/IEC 27001:2013 standard, shall be included in the Management System. This can be a powerful lever for scale and implementation effort of the project. You will need to provide a very good reason for excluding controls from the scope that will withstand audit scrutiny.

Implementation Steps

Identify Potentially Out-of-Scope Controls

There are two ways of approaching this: either getting a spreadsheet with all of the control statements from the ISO/IEC 27001:2013 or creating a control set using the ISO/IEC 27001:2013 template within Alyne and then sort the control set based on the ISO/IEC 27001:2013 standard.

Both ways lead to the same outcome. Some questions to ask when considering the scope of the ISMS: Does this control cover technology or processes the organization executes? Is the control applicable to the processes in scope of the ISMS? Is the control applicable to the nature of the business?

Explore Mitratech's Alyne Controls

It is important to understand that the control statements within Alyne document the hands-on implementation of the controls defined in the ISO/IEC 27001:2013 standard, therefore multiple Alyne controls cover one ISO control. This provides a head start, as one of the core steps in implementing the ISMS requires documenting how the ISO/IEC 27001:2013 controls are implemented.

Mark the Out-of-Scope Controls

For each chapter of the ISO standard, use the search function to find all Alyne controls linked to the ISO/IEC 27001:2013 controls you want to exclude. Switch to edit mode and add a custom reference. This way you can easily find the in-scope controls.

Document a Reason for Exclusion

Use the additional information field to document the reason you believe the control should not be in scope for the ISMS. Add enough detail so an auditor will understand the reasoning.

Lessons Learned

1. Do not Exclude too Many Controls

Auditors are usually not willing to accept excluding too many controls.

2. Mark Inactive Controls as Currently Not Applicable

Mitratech's Alyne automatically provides a description of how the controls should be implemented. Add additional information stating that a control is currently not applicable, but the relevant controls are in place.

STEP 4: BUILD A CONTROL

Once the controls your organization wants to cover within its ISMS have been defined, it is necessary to document current implementation and make evidence available for the audit. For each control where it is possible to go into more detail, add a description to the additional information or add a link to a reference or upload evidence of the implementation as attachments.

Implementation Steps

Create One or Multiple Control Sets

Go topic by topic and limit the scope to the ISO/IEC 27001:2013 according to the defined SOA. This enables the possibility of creating target audience specific control sets that are helpful for awareness.

Many controls in the ISO/IEC 27001:2013 standard essentially require the definition and rule setting of a certain aspect. By leveraging Mitratech's Alyne content and control framework, you are inherently meeting this control.

Set Variables

Adapt a control to your organization, while retaining the original intent of the control as well as enabling the Alyne team to update and expand mappings to the controls as the Alyne library develops. Be aware that variables may be used in multiple control statements. Changing a value once will affect change in all other locations where this variable is used.

Document Implementation

Use the additional information field to document specifics of implementation and attach or reference relevant documents such as operations manuals or processes.

Track endorsements

Use the reactions on each control to mark as endorsed and implemented as applicable. Use the comment fields to document any discussions around the control.

Attach Evidence

Add links or attach files to provide evidence of implementation of a specific control statement.

Assign Tasks to the Team

Leverage Alyne's task management feature to assign implementation or documentation tasks across the team. This has the added benefit of an audit trail that can be shown to the auditors to document involvement of various stakeholders.

Reference Your Existing Framework

Should your organization have existing controls, policies or other rule setting documents, make sure to link them or add a custom mapping to the control framework. Creating custom mappings will allow reporting and risk analysis not just based on the ISO/IEC 27001:2013 standard, but also on internal documents.

Lessons Learned

1. Document, Document, Document

Alyne makes it very easy to link, comment, attach and react to control statements. The more you document, the easier your audit will be. Documenting discussions is valuable to show the development of the control framework and the multiple people involved.

2. Add Comments for Management Review

At Mitratech's Alyne, there is a dual signatory policy in place. As such, sign-offs are marked through reactions on control sets. Additionally, reviews are documented through comments making it very easy for auditors to see dates and review cycles.

STEP 5: RUN SELF ASSESSMENT

Part of the process for developing an ISMS is also measuring the current level of maturity and deducting risks that may result from these deviations. This also creates the baseline for your information security risks, which are also a large focus in the plan, do, check, act cycle. For this step, create an assessment based on the statement of applicability within Alyne and perform a self assessment.

Implementation Steps

Start Assessment Configuration

Alyne has pre-defined templates for running a self assessment. Either select the pre-defined template or create a new assessment from your control set.

When using the template, remove the out of scope questions by using a filter view. When creating a new assessment remember to set your own maturity targets.

Refine Assessment Setup

Adapt or set the maturity targets to values that match up to your organization's requirements – it is important to document the decision in the management statement, as this is core to setting your benchmark for evaluating the maturity. It is recommended to adapt the maturity targets by topic based on threats, strategic objectives of the organization and protection needs of the information assets.

Split up assessments if you are not in a position to cover the entire scope. It is possible to combine the outcomes in a single report later. Make sure to use the scope setting 'Internal' so that your organization's variable settings are applied to the questions.

Respond to Assessment

Respond to the scope of the self assessment. Adding a comment to the individual responses is helpful to document the reasoning behind a certain response.

Create Report

Once all responses have been gathered, create a report and analyze the outcomes. Remove risks, where they are not applicable and try to find common patterns of identified risks in preparation for the security risk register.

Lessons Learned

1. Call Out Weaknesses and Gaps

Known weaknesses are not a reason preventing your organization from obtaining the certification. Just because the risk self assessment reveals weaknesses, this does not mean your organization is going to fail the certification. It is far more essential to provide governance around the issues, either through formal risk acceptance or a mitigation plan to resolve. Translation: raise risks and document as much as possible.

2. Add Evidence and Descriptions

Make rating as transparent as possible by adding a quick comment or relevant evidence as applicable to the answers. This makes the auditors reviewing much easier.

STEP 6: SETUP RISK REGISTER

Risk management is a core aspect of the ISMS according to the ISO/IEC 27001:2013 framework. As mentioned before, a weakness in implementation or insufficient maturity is not a reason for failure. Failure to demonstrate governance and management is. Alyne's functionality to demonstrate active management of threats is the risk register.

Risks should be clustered based on management focus and organizational priorities. The risk register should be able to reflect risk exposure for the area of responsibility of every stakeholder. Alyne provides a very powerful capability for this purpose.

Implementation Steps

Understand Risk Tags

The core element within Alyne to structure risks are risk tags. A risk can be assigned to one or many risk tags – these can enforce access control, define risk appetite and enable dynamic reporting.

Set-up Risk Tags

We recommend between 5 and 15 risk tags to start with if you do not have a predefined risk register in place. The risk tags should cover both functional areas (Physical Security, Data Privacy, BCM, Finance, Web Security, ...) as well as some reporting verticals (Top Risks, Region X Risks, ...).

Add Existing Risks

If your organization has an existing repository of information security risks, enter these into Alyne to get started. The self assessment is the next source of risks. Analyze risks in the risk report and add relevant risks to the register.

Manage Risks

Accept threats that owners are comfortable with. The more documentation through comments, descriptions or attachments the better.

For other risks, build mitigation plans. This documents the actual management of the risks that have been identified in the self assessment. Assign the mitigation tasks to the relevant people within the organization.

Specify Financial Loss Potential

Define the risk appetite for each risk tag and quantify the financial loss exposure.

Lessons Learned

1. Track a Reasonable Number of Risks

Obviously this is highly dependent on the size and complexity of your organization. A useful range would be between 30 and 300 risks as a rough figure.

2. Do not Overengineer the Structure

Getting the risks input is the first priority. You can always refine later.

3. Add Financial Loss

If possible, add financial risk exposure. As in the previous point, you can always add this later.

STEP 7: RUN AUDIT

The ISO/IEC 27001:2013 standard requires that the ISMS is subject to an internal audit and there is an internal audit process operating effectively within the organization. Depending on the size of your organization, this may already be a given.

Implementation Steps

Define Audit Plan

Define an audit plan that documents your assurance tasks (both completed and planned) for aspects related to the ISMS scope.

Run ISMS Focussed Audit

Key control areas of the ISMS need to be subject to an audit before beginning the stage 1 certification audit. Certification bodies will focus on a full audit of the entire ISMS scope over a three year period. While an internal employee can perform audit tasks, it might prove difficult to facilitate sufficient independence from operational tasks in a small team.

Capture Findings in Risk Register

Outcomes of the audit should be captured in the risk register. Potentially add a risk tag 'Audit' in order to get a full view of all audit related risks and their current level of mitigation.

Build Mitigation Plans

Define mitigating actions for each of the identified findings. This way it becomes easy to demonstrate immediate remediation and improvement of the observations. Aim to implement the mitigations by the time you start the stage 1 certification..

Document Audit Outcomes in Management Statement

As the audit requirements are referenced in the management statement, update the core results of the audit in the document.

Lessons Learned

1. Anticipate Certification Audit Focus

Select key setup of the ISMS, core aspects such as: access management, risk management and incident management, as scope for your organization's initial audit. This reduces the probability of core findings in the certification.

2. Address Findings Quickly

The faster observations are addressed, the more likely it is to rate issues as "closed during audit" or at least mitigated by the time the certification starts.

STEP 8: SOCIALIZE AND SIGN OFF

Management needs to be involved. This is best documented through management actively commenting, endorsing content they are responsible for and generally demonstrating regular interaction through documented meeting agendas and comments.

Business users need to be involved from an awareness perspective. Specific parts of the ISMS relevant to specific audiences should be part of an awareness campaign. The objective should be to create an active risk culture with daily interaction with the ISMS.

Implementation Steps

Document Sign Offs

Ensure that responsible managers have documented implementation and endorsements for all control sets they are responsible for.

Comment Reviews

Make sure all reviews by managers or peer reviewers are documented as comments. This drastically speeds up the review process with the auditors.

Launch Awareness Campaign for Employees

Select a subset of controls from the ISMS. Use the 'Alyne Campaigns' feature to launch an awareness campaign across affected populations within your organization. This is a highly effective and fast way to document awareness across your team.

Include Awareness Check In Onboarding

In order to make the process sustainable within the organization, we made the awareness check mandatory in our onboarding process. We also repeat the awareness campaign periodically.

Attach Evidence of Management Awareness Measures

To further document management engagement in the process, attach relevant evidence such as emails to the team, meeting agendas, and others, to relevant controls mandating awareness.

Lessons Learned

1. Combine Multiple Awareness Measures

Launch a campaign of emails, all hands meetings, Alyne campaigns, and others, to convey the importance of this ISMS implementation.

2. Add the ISMS to the Agenda of Regular Meeting Invites

Put the ISMS on the agenda of some recurring meetings to make sure it becomes a recurrent topic.

STEP 9: PREPARE FOR AUDIT

Make sure all steps are documented, reviewed and signed off. Create a document trail for all the activities performed to prepare for the audit. The Audit runs in two stages:

Stage 1: Preparation and Initial Review

Stage 2: In Depth Audit and Certification

Usually there are only a few weeks between stage 1 and stage 2 audits. During this period, it is expected that the observations from stage 1 are addressed. Should the findings in stage 1 prevent an audit, the stage 2 may be postponed until the larger findings are mitigated.

Implementation Steps

Check Reviews

Check all active control sets that have been marked as reviewed, implemented and endorsed. Additionally, document the review with comments and dates.

Check Implementation Notes

Make sure that additional information on control level has been added where applicable.

Check Links and Uploads

Ensure all relevant supporting documents are linked or attached as needed.

Provide Guidance During the Audit

Guide the auditors through your organization's ISMS and show evidence of the items they are testing.

Attach Evidence of Management Awareness Measures

To further document management engagement in the process, attach relevant evidence such as emails to the team, meeting agendas, and others, to relevant controls mandating awareness.

Lessons Learned

1. Think Like an Auditor

They don't want you to fail, they just want easy evidence that they can reference in their testing. Have the information location, date of review and date of sign off ready for every control area.

2. Be Quick at Remediation

Most of the time the observations will be pretty straightforward. Solve them immediately (capture a risk, add comments or additional information) and demonstrate proactive management of information security. That way the observations can be classified as mitigated during audit.

STEP 10: OBTAIN CERTIFICATION

Following the stage 2 audit, the certification body will perform a peer review of the evidence gathered by the auditor. The certification body will then decide if the certification will be awarded. Potentially demonstrate resolution of observations from the stage 2 audit in your management comments on the stage 2 audit report.

Be aware that observations in the current audit will be topics for review in the supervisory audit in the following year, so be sure to keep your resolution well documented - this is a quick win.

Implementation Steps

Track Issues

Capture the observations as audit issues in the risk register.

Document Mitigations

Document all resolution of the observations directly in the risk register. That way your organization will be well prepared for the following supervisory audit in 12 months time.

Lessons Learned

1. Don't Fight It

Do not fight observations that are not preventing the certification . Rather look at them as an easy option to demonstrate improvement in the supervisory audit next year.

2. Get the Wording Right

Make sure that the wording on the certificate accurately describes the scope of processes that have been covered in your business. If you are getting a certification for a specific customer, consider how meaningful the wording is for a specific audience.

IN CLOSING

Mitratech's Alyne received top marks from auditors regarding its ISMS. We were very pleased to have proof that our vision for a simplified ISO/IEC 27001:2013 certification process can be in fact realized. Looking back at both our initial audit and our supervisory audit, some common success factors stood out:

Explain and Document Reasoning Behind Decisions

This demonstrates involvement of management and an active security culture.

Use Links and References in Alyne

This makes the ISMS as interactive as possible, easy to navigate and always up to date.

Use Campaigns or Funnels to Document Awareness

These are quick and powerful tools to demonstrate how all relevant stakeholders were involved in the process without costing much effort for management or the affected people.

Don't Hide Weaknesses

Demonstrate that you are aware of them and are actively managing them. A good auditor will see the opportunity to call this out - without failing your certification.

Think Like an Auditor

Provide evidence, a clear source, date of sign off and date of last review - that's all the auditor wants to make a tick mark.

MITRATECH

info@mitratech.com
www.mitratech.com