alyne

happiest minds
The Mindful IT Company
Born Digital . Born Agile

WHITE PAPER

Written by Karl Viertel, Alyne

GETTING ISO 27001 CERTIFIED

Using Alyne

Ten detailed steps to becoming ISO 27001 certified using Alyne's Software as a Service.

August 2021

Getting **ISO 27001 certified** using **Alyne**

Our customers leverage Alyne for effectively managing their risk, information security and controls frameworks. Naturally their requirements for the protection of this sensitive information is an important factor for their trust in Alyne. The **ISO/IEC 27001:2013** certification remains one of the most trusted and widely recognised standards for Information Security Management across regions and industry sectors. We therefore embarked on our journey of obtaining a certification in late 2017 and obtained certification in early 2018. As of March 2019 we have also successfully passed our first supervisory audit without any findings.

Naturally, we used our own internal instance of Alyne for building our Information Security Management System (ISMS). As people at Microsoft used to say: Eat your own dogfood. I would like to share some of the learnings we gained along the way and provide a detailed guide for any organisation looking to obtain an **ISO/IEC 27001:2013** certification, and how to implement this using Alyne's Software as a Service. In the following, I will summarise the main steps to achieving the certification, explain how to implement the necessary actions in Alyne and leverage the solution's capabilities to reduce your effort and share lessons learned for each step.

Using Alyne to implement your **ISMS** provides you with some powerful advantages:

Content out of the box

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 Alyne, this is ready on day one.

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 that are then mitigated to continuously improve the ISMS. Identifying and quantifying the risks can be a difficult task. Alyne's risk analytics are a powerful tool for this.

Collaboration and Awareness

Involving management and people responsible for processes affected by the ISMS are core aspects 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 for the team. Alyne is that platform.

Framework Synergies

Likely ISO/IEC 27001:2013 is only one framework relevant to your overall governance program. With Alyne you can easily re-use 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.

IMPLEMENTATION GUIDE

STEP 1

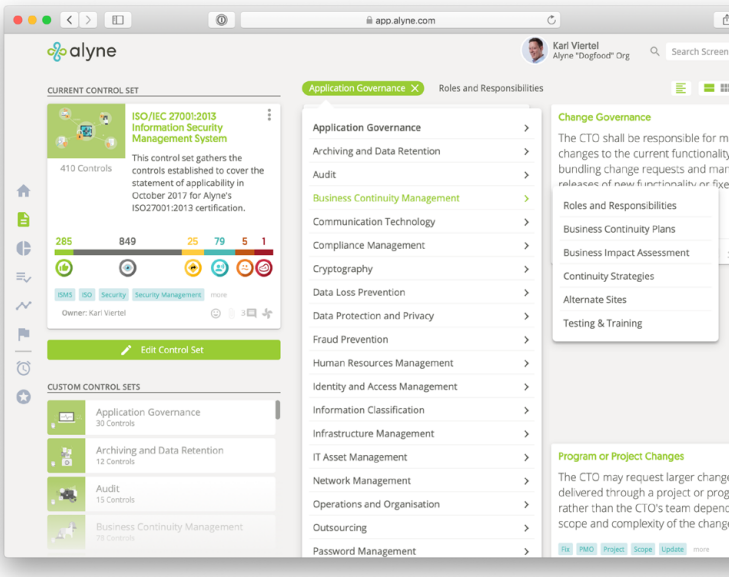
Kick off project and **define motivation**

When kicking off the implementation of the ISMS it is important to establish what you as an organisation are looking to gain from it. I believe it is legitimate to consider this essentially a sales tool as a bare minimum. You will certainly gain more value from the process if the stakeholders in your organisation also see this as a tool to increase cyber security maturity and resiliency. The motivation for your ISMS may influence the stakeholders that are required for this process.

IMPLEMENTATION STEPS

a. Involve the right stakeholders

Ensure you have support and availability from a core set of stakeholders that are 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 in your organisation. You can explore the topics in the ISO/IEC 27001:2013 Control Set in Alyne to get an overview of the topics covered to deduct potential further stakeholders for involvement.



b. Define objectives and overall scope

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

c. Identify in-scope processes

Once you have defined the overall scope, identify the processes that are in scope for the ISMS. 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 continuous management in the ISMS and a recurring annual audit.

Your scope should be influenced by your overall motivation for the ISMS and cyber risk exposure.

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 early exactly how much effort is required and when.

Develop **Management Statement**

STEP 2

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. You can see **Alyne's template for our Management Statement here.** Consider this document a guide for the rest of the ISMS. It covers the requirements of the main chapters of the ISO/IEC 27001:2013, while Annex A (where the majority of the effort lies) is covered in the actual control framework. This document should be continuously updated. To provide a frame of reference, our Management Statement is around 6 - 7 pages long, so do not over-engineer this.

IMPLEMENTATION STEPS

a. Structure Document

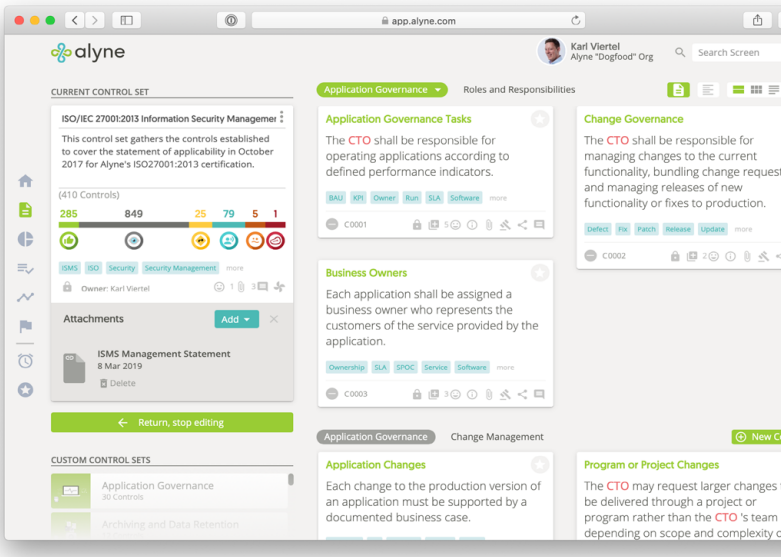
The document should follow the structure of the standard and describe your approach to these main topics. Using the exact wording of the standard makes the audit much easier.

b. Describe Implementation

Describe in a few paragraphs how you approach and implement the individual chapters. I would recommend to keep these brief. The details are in the control framework. The more you write, the more difficult reviews, sign-offs and audits become.

c. 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 (I would consider this however, optional). 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 re-inventing the wheel and to be honest this document is almost exclusively for the auditors.

2. Use a document with version control

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

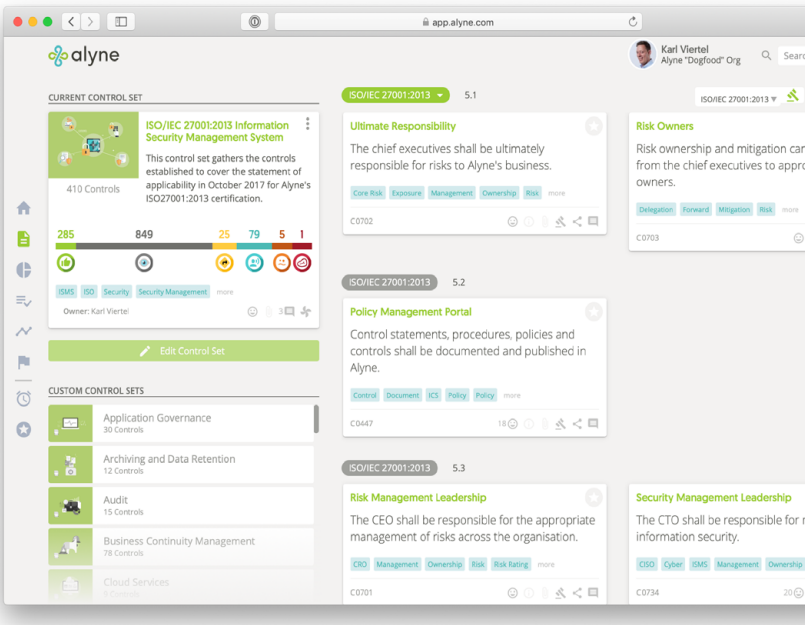
STEP 3

Define Statement of **Applicability**

The second 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.

a. Identify potentially out-of-scope controls

There are two ways of approaching this: Either get a spreadsheet with all of the control statements from the ISO/IEC 27001:2013 or create a control set using the ISO/IEC 27001:2013 template in 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 we execute? Is the control applicable to the processes in scope of our ISMS? Is the control applicable to the nature of our business?

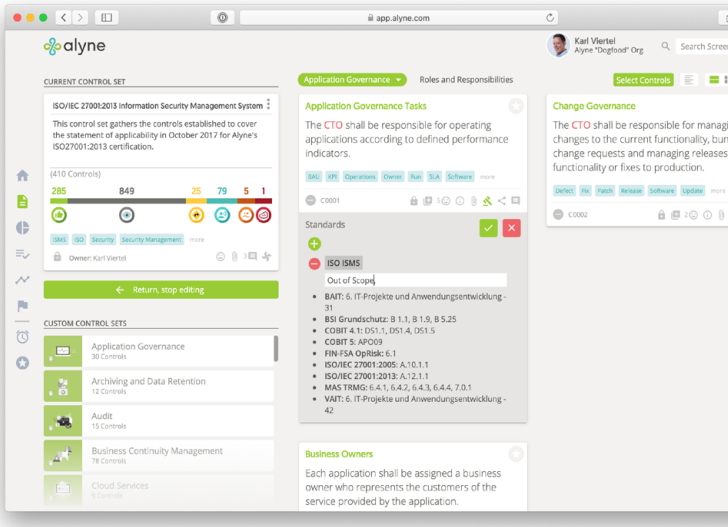


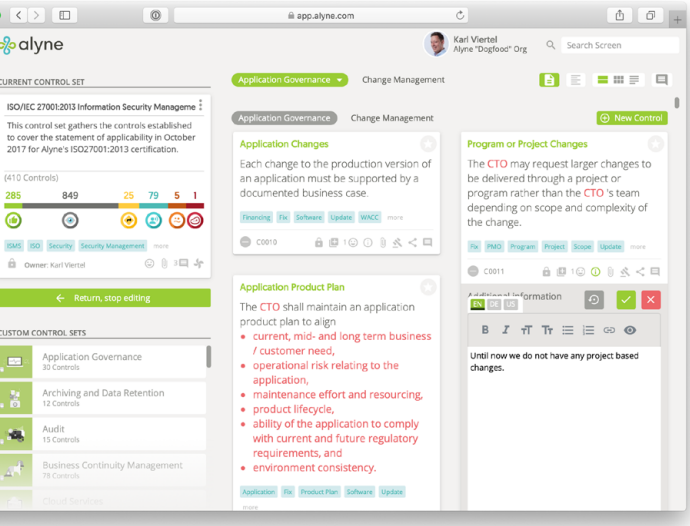
b. Explore the Alyne Controls

It is important to understand that the control statements in Alyne document the hands-on implementation of the controls defined in the ISO/IEC 27001:2013 standard, so you will find multiple Alyne controls covering one ISO control. This gives you a head start, as one of the core steps in implementing the ISMS requires you to document how the ISO/IEC 27001:2013 controls are implemented.

c. 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 e.g. “ISO/IEC 27001:2013 Certification - Out of Scope” marking these as out of scope for the ISMS. That way you can easily find the in-scope controls for later work.





d. 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. You will need to add enough detail so an auditor will understand the reasoning.

LESSONS LEARNED

Do not de-scope too many controls

Our auditors were not willing to accept de-scoping of many controls. The effort for trying to fight the auditors on this is likely not worth the effort.

Mark inactive controls as ‘currently not applicable’

we simply included all but two controls in the ISMS scope. With Alyne you automatically have a description of how the controls should be implemented. We simply added additional information that this control currently is not applicable, but the relevant controls are in place. E.g. we do not operate physical hardware apart from laptops. Should we operate hardware in the future, we have a set of controls that will then apply. This is certainly the path of least resistance.

STEP 4

Build **Control Framework**

Now that you have defined the controls you want to cover within your ISMS, you need to actually implement and document your current implementation and make evidence available for the audit. For each control where you can 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

a. Create one or multiple control sets

We went down the path of going topic by topic and limiting scope to the ISO/IEC 27001:2013 according to the defined SOA. This enables you to create target audience specific control sets that are helpful for awareness. Be aware that many controls in the ISO/IEC 27001:2013 standard essentially require the definition and rule setting of a certain aspect. By leveraging Alyne's content and control framework, you are inherently meeting this control. For example, taking a certain topic in Alyne is effectively creating an ISO/IEC 27001:2013 conform policy for this specific topic at the same time.

b. Set variables

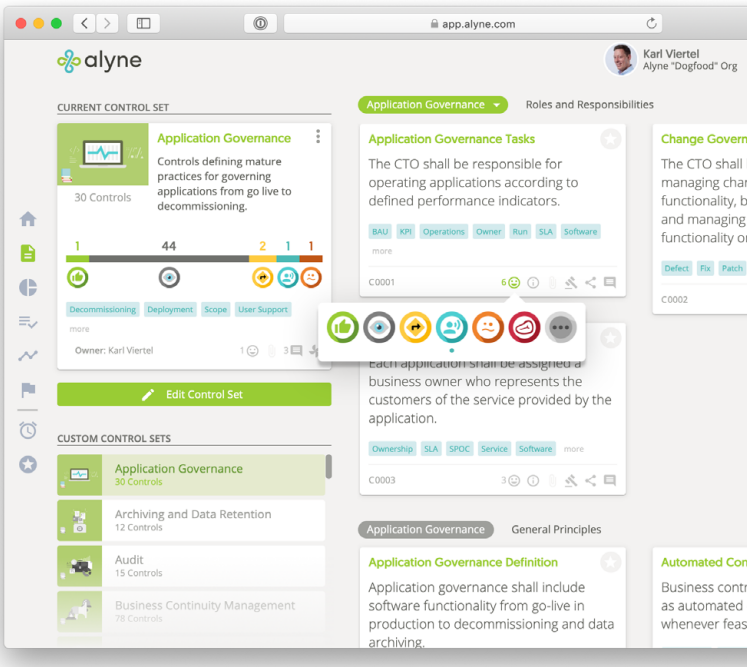
We have defined a number of controls to include variables. This allows you to adapt a control to your organisation, while retaining the original intent of the control while also enabling the Alyne team to update and expand mappings to the controls as our library develops. Be aware that variables may be used in multiple control statements. Changing a value once will affect change in all other locations where this variable is used.

c. Document implementation

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

d. Track endorsements

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

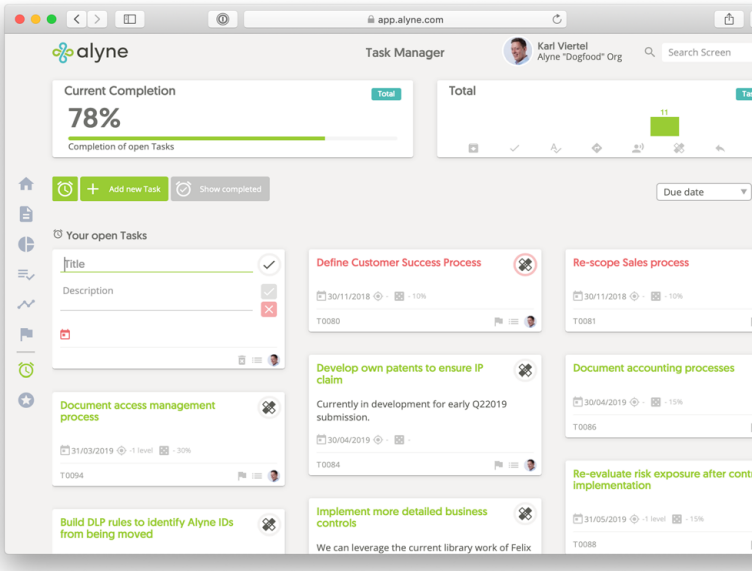


e. Attach evidence

You can either add links or attach files to provide evidence of your implementation of a specific control statement. For example, I performed a user access review of access to our team drive and added the review report with a comment to the respective control statement.

f. 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.



g. Reference your existing framework

Should you 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 enable you to perform reporting and risk analysis not just based on the ISO/IEC 27001:2013 standard but also your internal documents.

LESSONS LEARNED

Document as much as you can

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.

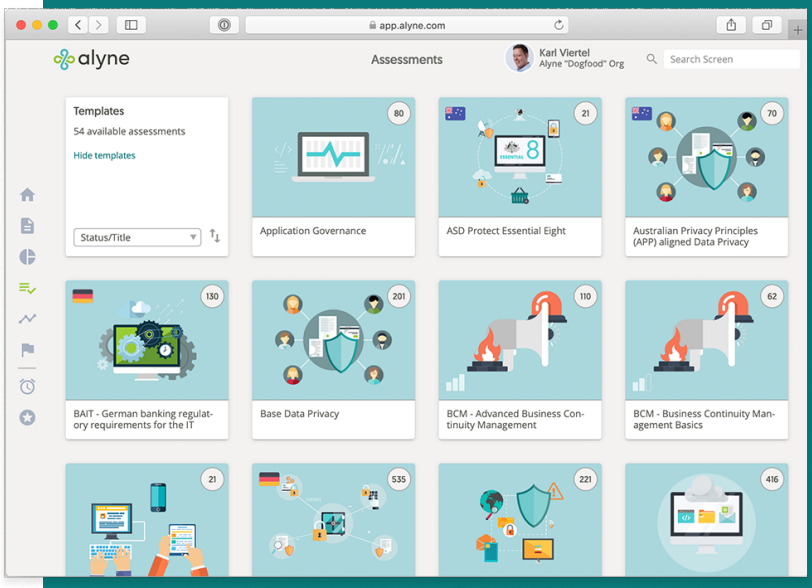
Add comments for management review

We have a dual signatory policy in place at Alyne. As such we marked our sign-offs through reactions on control sets. Additionally we documented the reviews through comments. That made it very easy for auditors to see dates and review cycles.

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 we will create an assessment based on the Statement of Applicability in Alyne and perform a self assessment.

STEP 5



IMPLEMENTATION STEPS

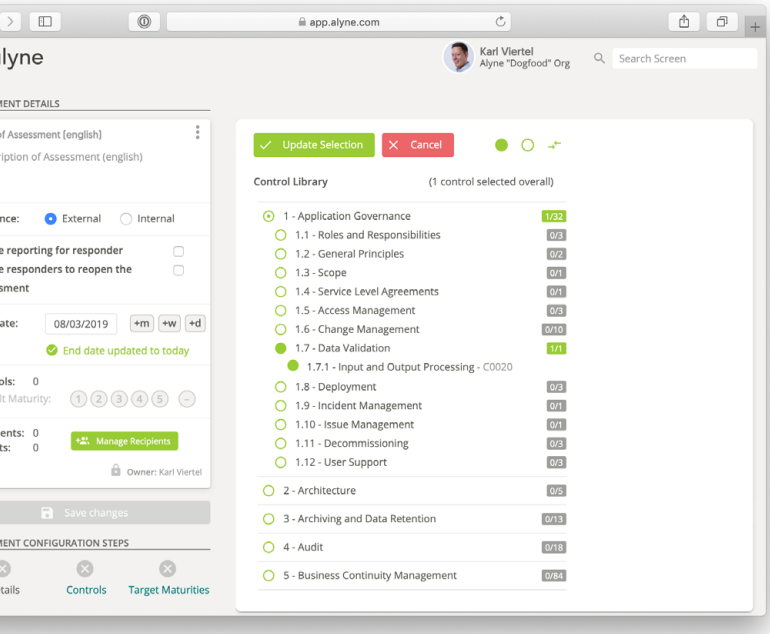
a. Start Assessment configuration

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, you will have to remove the out of scope questions by using a filter view. When creating a new assessment you will need to set your own maturity targets.

b. Refine Assessment setup

Adapt or set the maturity targets to values that match up to your organisation'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 organisation and protection need of the information assets. Split up assessments if you are not in a position to cover the entire scope. You can easily combine the outcomes in a single report later. Make sure to use the scope setting "Internal" so that your own variable settings are applied to the questions.

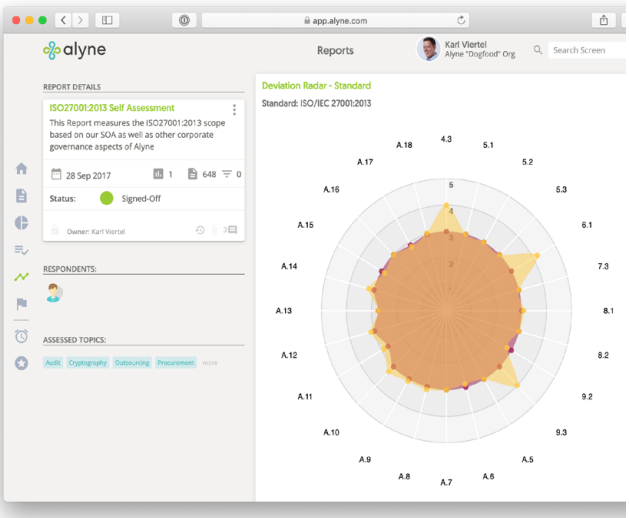


c. Respond to Assessment

Respond yourself or with other subject matter experts to the scope of the self assessment. Adding a comment to the individual responses is helpful to document the reasoning behind a certain response.

d. Create Report

Once all responses have been gathered, create a report and analyse the outcomes. Remove risks, where they are not applicable and try and 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 you from obtaining certification. Just because the risk self assessment reveals weaknesses does not mean you are going to fail the certification. What is more essential is proving governance around the issues be it through formal risk acceptance or a mitigation plan to resolve. This means: Raise risks and document as much as possible.

LESSONS LEARNED

2. Add evidence and descriptions

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

Setup **Risk Register**

STEP 6

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. The tool to demonstrate active management of risks in Alyne is the risk register. Risks should be clustered based on management focus and organisational priorities. The register should be able to reflect risk exposure for the area of responsibility of every involved stakeholder. Alyne provides a very powerful capability for this.

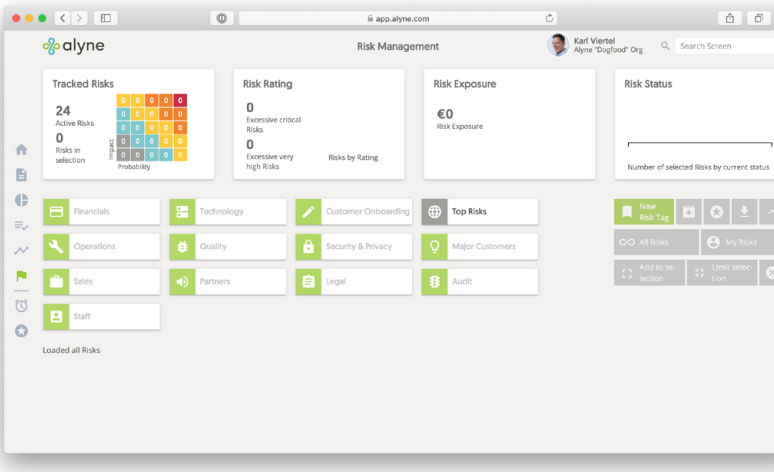
IMPLEMENTATION STEPS

a. Understand Risk Tags

The core element we use in 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.

b. 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, ...)



c. Add existing risks

If you have an existing repository of Information Security Risks, you can enter these in to Alyne to get started. Your self assessment is the next source of risks. Analyse risks in the risk report and add relevant risks to the register.

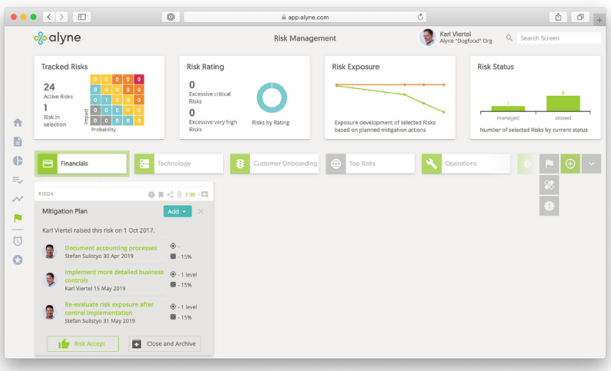
d. Manage risks

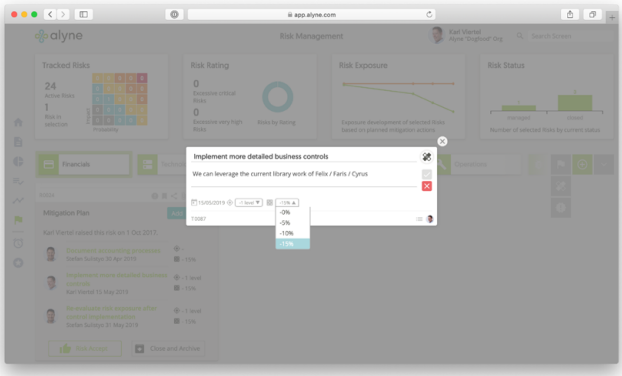
Risk accept risks that your risk owners are comfortable with. The more documentation through comments, descriptions or attachments the better.

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 in the organisation.

e. Specify financial loss potential

If you are able to define the risk appetite for each risk tag and quantify the financial loss exposure.





LESSONS LEARNED

Track a reasonable number of risks

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

Do not overengineer the structure

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

Add financial loss if you can

If you have an understanding of the financial risk exposure, add it. You can always add this later, so do not get hung up on it.

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 operating effectively in the organisation. Depending on the size of your organisation, this may already be a given. In our case we leveraged an external auditor to support us.

IMPLEMENTATION STEPS

a. Define audit plan

Define an audit plan that documents your assurance tasks (both completed and planned) for aspects related to the ISMS scope. We set up a very simple spreadsheet based tracker that we regularly review and update as we progress our assurance tasks.

b. Run ISMS focussed audit

Key control areas of the ISMS need to be subject to an audit before you can start your stage 1 certification audit. Our auditors made us aware that certification bodies will focus on a full audit of the entire ISMS scope over a three year period. While you can nominate an internal employee to perform audit tasks, you will struggle to facilitate sufficient independence from operational tasks in a small team.

c. Document audit outcomes in Management Statement

As the audit requirements are referenced in the Management Statement, I would update the core results of the audit in the Management Statement document - as this is a living document.

d. Capture findings in risk register

Outcomes of the audit should be captured in the risk register. Potentially add a risk tag “Audit” so that you can also get a view of all audit related risks and their current level of mitigation.

e. Build mitigation plans

Define mitigating actions for each of the identified findings. This way you can demonstrate immediate remediation and improvement of the observations. You should aim to implement the mitigations by the time you start the stage 1 certification.

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 initial audit. This reduces the probability of core findings in the certification.

2. Address findings quickly

The faster you address observations, the more likely you can rate issues as “closed during audit” or at least mitigated by the time you start the certification.

STEP 8

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

a. Document sign offs

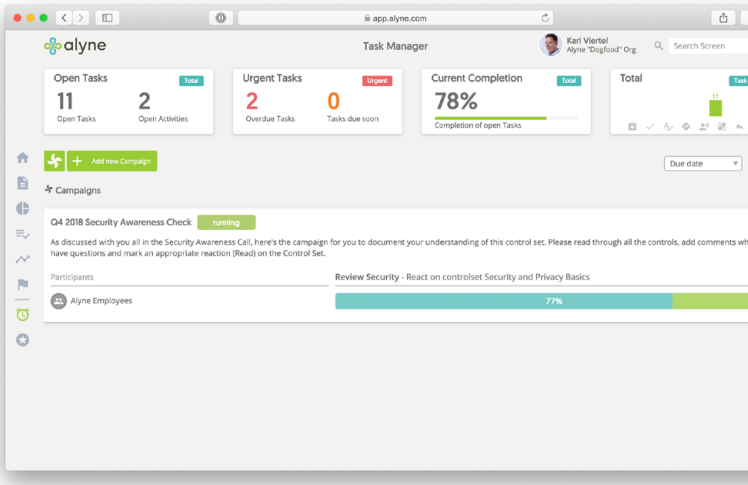
Ensure that responsible managers have documented implementation and endorsements for all control sets they are responsible for.

b. 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.

c. Launch awareness campaign for employees

Select a subset of controls from the ISMS. We created a control set we called “Security and Privacy Basics” that represent the core controls that are relevant to our people safely processing our information asset. Use the ‘Alyne Campaigns’ feature to launch an awareness campaign across affected populations in your organisation. This is a highly effective and fast way to document awareness across the team.



d. Include awareness check in onboarding

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

e. 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, etc. to relevant controls mandating awareness.

LESSONS LEARNED

1. Combine multiple awareness measures

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

2. Add the ISMS to the agenda of regular meeting invites

Just put the ISMS on the agenda of some recurring meetings to make sure it is always a topic - even if just for a few minutes.

Prepare for **Audit**

Make sure all steps you have taken are documented, reviewed and signed off. Create a document trail for all the activities you have 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 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.

STEP 9

IMPLEMENTATION STEPS

a. Check reviews

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

b. Check implementation notes

Make sure that you have added additional information on control level where applicable.

c. Check links and uploads

Ensure you have all relevant supporting documents linked or attached as needed.

d. Provide guidance during the audit

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

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 an 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 to solve. 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

a. Track issues

Capture the observations as audit issues in the Alyne Risk Register.

b. Document mitigations

Document all resolution of the observations directly in the risk register. That way you are 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 certification unnecessarily - see 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 in your business that has been covered. If you are getting a certification for a specific customer, you need to consider that the wording is meaningful for this audience, for example.

Closing **Thoughts**

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

1. Explain and document reasoning behind decisions

This demonstrates involvement of management and an active security culture.

2. Use links and references in Alyne as much as possible

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

3. 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.

4. 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.

5. 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.

I hope you feel well prepared and confident in embarking on your own ISO/IEC 27001:2013 certification journey using **Alyne.** Do not hesitate to reach out to our customer success team at **support@alyne.com** if you would like further guidance.

OR

write to business@happiestminds.com

alyne

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**