

# Policy Management

## Guide

Policy Management is a crucial GRC practice that is seldom problematic for most organisations, although if no one knows how many policies are around, what they are used for, who owns them, or if they have been reviewed, Etc then they become useless

In this guide we share our methods that can be used with GRC systems, and deal with most of the common challenges found.

**Warning:** eramba core philosophy is simplicity: in our language, software and practices. This guide might includes ironic comments of all sorts just to make more digestible for the reader (and us, authors). Although this guide explains how to use our enterprise release it should still be useful for our community users (which might not have as many features as our enterprise release).

# Table of Contents

<b>Introduction</b>	<b>2</b>
Challenges	2
<b>General Concepts</b>	<b>2</b>
Policy Reviews	4
Policy Content	5
Policy Lifecycle	6
Policy Roles	6
Types of Policies	7
Policy Portal	8
<b>New Policy Checklist</b>	<b>9</b>
<b>Managing Policies</b>	<b>9</b>
Manual Input	9
Reviewing Policies (Work on Progress, please Ignore)	11
Notifications	12
Upload Policy Review Records	13
Useful Filters	15
Policy Notifications	15
Importing Policies with a CSV	17
Visualising Policies	17

# Introduction

## Challenges

The first challenge in our opinion is to have a list of policies in our organisation (regardless their usefulness) as for some reason over the years we had accumulated quite many.

We then want to make sure they are used for something, useful. Do they mitigate a risk? Which one? One or more compliance requirements? We wanted to be able to see the relationships as clear as possible, so if someone would challenge us on why we need this or that document - voila! The answer is there.

The other challenge is to keep them updated, we need a system that centralises policies and remind owners (and us, the GRC team) when their policies are not updated. We also want to keep tidy records of each review in order to keep auditors happy.

Speaking of auditors, they love having all policies in a single portal. In fact, many of us like that, just to be able to search for what we need without the need of checking ten different sharepoint, wikis, etc.

In the end policies are meant to be read and followed by the organisation, we needed some basic e-learning system that would reach out to the right audiences and be able to keep track on whether they read the policies or not.

## General Concepts

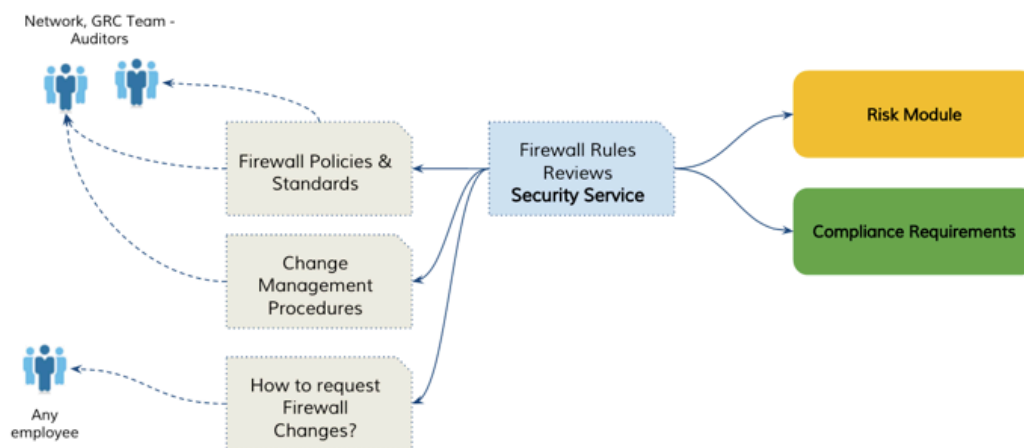
Eramba has a section (Control Catalogue / Policy Management) that allows you to document policies. Policies in eramba are used for:

- Compliance and risk treatment (Compliant Management / Compliance Analysis)
- Security Services (Control) Governance (Control Catalogue / Internal Controls)
- Data Flows (Asset Management / Data Flow Analysis)

You can use policies to mitigate risks, compliance requirements and make sure each one of your internal controls, for example ISO requires you on 5.1.1 to have a security policy, you can link to that requirement a policy uploaded in this section. That same policy can also be linked to PCI requirements which also state the need for security policy.



Policies are linked to Security Services (Controls) to define their governance (how are they built, why, how they are operated, Etc). If we plan to design a control for “Policy Reviews” we need a standard (that describes how firewalls are built, what firewall rules need to include, etc) a procedure (that explains how firewalls rules are to be managed or how firewall rules are requested).



Once you have your policies documented you can easily link them with each compliance requirement, risks, data flow analysis, etc.

6.1 - Internal Organization (Not Specified)													
Item ID	Item Name	Strategy	Mitigation Controls	Policy Items	Exception	Risks	Liabilities	Projects	Owner	Description	Status	Actions	Workflows
6.1.1	Information security roles ...	Compliant	No	No	No	No	No	No	None	Yes	Ok		Approved Owner
6.1.2	Segregation of duties	Compliant	Yes	Yes	No	No	No	No	None	Yes	Missing Reviews Last audit missing		Approved Owner
6.1.3	Contact with authorities	Compliant	No	No	No	No	No	No	None	Yes	Ok		Approved Owner
6.1.4	Contact with special interest...	Compliant	No	Yes	No	No	No	No	None	Yes	Missing Reviews		Approved Owner

As you can see in the screenshot above, the requirement 6.1.4 from ISO in my organisation is mitigated with the “Information Technology” policy (which by the way, is missing its last review).

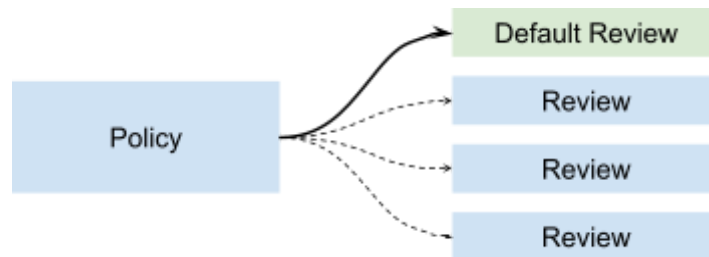
**In our experience:**

We meet many customers that rush to upload their policies to eramba as soon as they finish installing the software. Although that is not necessarily a bad thing we recommend holding up until you have understood risk and compliance modules in detail and are able to link your current policies to those two.

## Policy Reviews

Each policy you upload has one or more reviews attached, is each one of this reviews that lets eramba know what is the latest version of the document. When you create a policy eramba by default will attach two review records:

- Default Review Record (With the date you created the policy)
- Future Review (Based on the future review date you have defined)



This allows eramba to know what version the document is at the time it was created. You will then manage the document content, version, future review date by updating or creating reviews. Essentially, once you upload a policy most of its management is done through reviews.

[Add New](#)

Visualisation Active

You are in the admin group, you can see all items in this section

Planned Date	Actual Date	Description	Reviewer	Version	Completed	Action
2016-01-09	2016-01-09	Standards needed to be updated	Admin Admin	0.8	Yes	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Share</a> <a href="#">Print</a> <a href="#">Download</a>
2017-01-09	2017-01-09	Minor corrections	Admin Admin	0.9	Yes	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Share</a> <a href="#">Print</a> <a href="#">Download</a>
2018-01-05	2018-01-05	This review was created by the system at the time the policy was created - If you used "attachments" as content, then don't forget to attach policies to this review.	Admin Admin	1.0	Yes	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Share</a> <a href="#">Print</a> <a href="#">Download</a>
2018-05-02	2018-05-30	Updated chapter 3, had grammar issues	Admin Admin	1.1	Yes	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Share</a> <a href="#">Print</a> <a href="#">Download</a>
2018-09-06 (Missing)		-	Admin Admin		No	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Share</a> <a href="#">Print</a> <a href="#">Download</a>

[Close](#) [Previous](#) [Next](#)

The screenshot above shows the review records for a policy, the latest review is the one at the bottom and one row above you will see the "Default Review". It seems in this case the admin clicked in "Add New" to create further reviews with past dates.

Every time you create a policy you must set a "Review Date", that is a date in the future when the policy needs to be "Reviewed". On that day eramba will expect you to update the

expected review record, if you don't, the status of the policy will change from “Ok” to “Missing Review”. Everything this policy touches (risks, compliance requirements, etc) will also inherit this status.

Security Policy: Clean Desk Policy										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
3	Admin Admin	Admin Admin	Policy	Use URL Q View	Public	1	2015-11-30	2017-04-11	Missing Review	Approved Owner
<b>Description</b> Defines the minimum requirements for maintaining a "clean desk" - where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight.										
Related Documents										
Reviews										
Mitigated Items by this Policy										
Awareness Programs										

*A policy showing “Missing review” status, clicking on Manage / Reviews will get you to the list of reviews for this policy*

If you configure notifications, eramba will email the roles you defined before (and after) the scheduled review deadline. Read our notifications documentation to understand how that works. You could also create a filter that lists all policies missing a review and have that emailed to you.

## Policy Content

When you create a policy in eramba you essentially upload metadata (who is the author, version, owner, what the policy talks about, when it must be reviewed, Etc) and you can also upload the policy itself. You have three options as to where the policy will actually be located:

- Attachments
- URL (you specify the URL where the policy is stored)
- Content (you document the policy in a built in editor eramba has included)

Every time you review a policy it is likely that you will do some update to its content (correct grammar, add sections, Etc). If you manage policies as attachments then you will upload the new version, if you used a URL you'll upload the new URL and if it was “Content”, then you will edit the policy on eramba directly.

Security Policy: Change Management Process										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
41	Admin Admin	Admin Admin	Procedure	Use URL Q View	Public	1.6	2015-07-06	2017-07-10	Ok	Approved Owner
<b>Description</b> This document describes the high level processes that govern changes in the infrastructure managed by Acme Infrastructure teams.										
Related Documents										
Reviews										
Mitigated Items by this Policy										
Awareness Programs										

*A policy with a content type URL (if you click on view you get the link to the place where the actual policy is located)*

## Policy Lifecycle

As most elements in the GRC ecosystem (risks, compliance items, exceptions, controls, etc) policies also have different stages. In eramba the stages a policy can go through are:

- Missing Reviews (Yellow)
- Ok (Green)

Security Policy: Acceptable Encryption Policy										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	
1	Admin Admin	Admin Admin		Use URL Q View	Public	2.2	2015-11-30	2017-12-31	Ok	
Description										
Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.										
Related Documents										
Reviews										
Mitigated Items by this Policy										
Awareness Programs										

Security Policy: Acceptable Use Policy										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	
2	Admin Admin	Admin Admin		Use URL Q View	Public	1	2015-11-30	2017-05-01	Missing Reviews	
Description										
Defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.										
Related Documents										
Reviews										
Mitigated Items by this Policy										
Awareness Programs										

These status are calculated automatically based on the review date you have set, and the review records that the system has uploaded. As usual, the status will be inherited by anything the policy touches, so if you miss reviews, items around this policy will also be tagged in yellow.

									Manage
tors	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status		
min		Use URL Q View	Public	1	2015-11-30	2017-05-01	Missing Reviews		
ices, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.									

Edit

Delete

Comments

Records

Attachments

Notifications

History

Share

Q Reviews

Direct Link

Clone

## Policy Roles

Policies need someone that will make sure they are kept updated and relevant to the goal they were set to meet. Without people being responsible for such actions, policies don't get enforced, reviewed or updated.

Security Policy: Remote Access Tools Policy									
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status ⓘ
17	Goran Galic	Esteban Ribicic, Goran Galic, Michelle Morrison	Policy	Use URL <a href="#">Q View</a>	Public	1	2015-11-30	2018-01-16	<span>Ok</span>
Description									
Defines the requirements for what type of remote desktop software can be used and how it must be configured.									
Related Documents									

*Two roles must be described in each policy, owner and collaborators.*

When you create a policy in eramba, you need to define two roles, owner and collaborator. The people you put in there are user accounts created under System / Settings / User Management (and of course can be AD tied).

These can be used anyway you want, for example in our case:

- Collaborator: is one or more individuals responsible for writing, reviewing and enforcing policies. If a policy sets standards for network devices, then is likely the network manager is the right person.
- Owner: is typically the person within your GRC department who is responsible for this policy being kept up to date and reviewed.

*Every company has different “roles” with “different” names for them. Your task is to fit your roles in those two fields eramba has for each policy.*

You can set up notifications that will be get sent to these roles and notify people when a review is missing.

## Types of Policies

Although this section is called “policy management”, any type of document can be uploaded: policies, procedures, templates, standard configurations, contracts, Etc. Anything that needs to be reviewed, linked to controls, risks, compliance requirements can be linked here too.

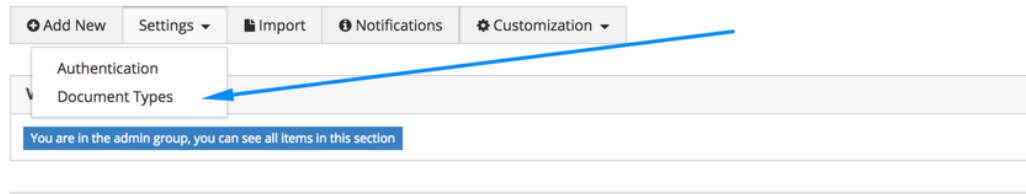
You must tell eramba what type of policy (document) you are uploading, you are provided three basic options but you can add more if you want at Settings / Policy Types

- Policies
- Standards
- Processes



## Security Policies

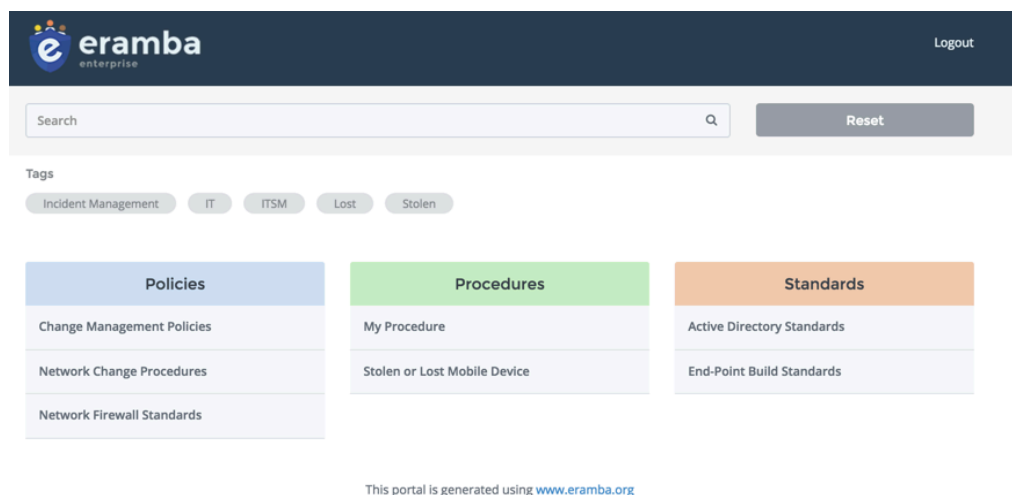
You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Complia



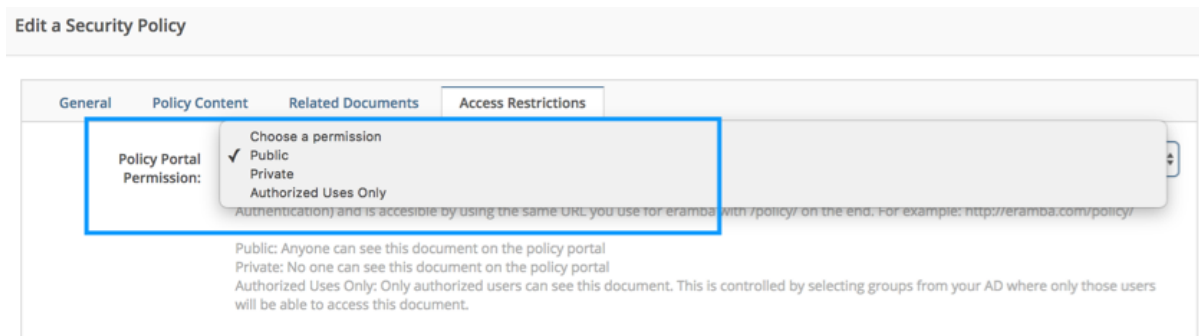
The reason why we set these three as minimum goes back to the idea that [controls need proper governance](#) to operate correctly and therefore these three are typically used.

Sometimes you'll find that you have a document that is a bit of each type, in those situations we recommend just choosing the one you think represents the document best.

## Policy Portal



Having all policies documented in eramba make it possible to show them in a portal, just like in the screenshot above. You can choose what gets shown at the time of creating a policy, your options are:



*When you create a policy, you define if it will be shown on the portal or not. You can also make it available only to AD authenticated users.*

You access the portal appending the URI /policy/ to your eramba install (you first need to enable it at System / Settings / Authentication).

For example, <https://eramba.mycompany.com/policy/>

## New Policy Checklist

The following is our policy checklist for creating new policies and for reviewing policies, you might find this useful.

Step	Name	Description
2	Design	Draw the drivers for policies (all risks, all compliance requirements) and map controls to them. Define how many policies each one of these controls needs and who is the audience.
2	Development	Meet control / risk / compliance stakeholder as needed and draft the guidelines for each document. Let them do the writing. Review what they wrote and ensure it meets your design requirements.
3	Sign Off	You and the author must get approval from the individual with authority to approve this.
4	Distribution	Upload policy to eramba
5	Awareness	Optional - create an awareness program and launch it.

Review activities include:

Step	Name	Description
1	Review	Ensure you meet the author and you discuss updates on the content, changes on the audience's, awareness compliance, etc.
2	Sign Off	Regardless of if there were changes or not, get approval and update your GRC system to reflect changes.
3	Distribution	If changes on the document existed, update them into the portal and notify audiences.
4	Awareness	If changes on the document existed, update your awareness program.

## Managing Policies

### Manual Input

In order to create a policy you need to use the Control Catalogue / Policy Management module and click "Add New".

Security Policies

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance Management and others.

[Add New](#)
[Workflow](#)
[Settings](#)
[Import](#)
[Notifications](#)
[Q Filters](#)

ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
1	Admin Admin	Admin Admin	Policy	Use URL Q View	Public	2.2	2015-11-30	2017-12-31	OK	Approved Owner

**Description**

Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.

Although the fields on the form are pretty clear is worth giving a few bits of advice for each tab.

Edit a Security Policy

[General](#)
[Policy Content](#)
[Related Documents](#)
[Access Restrictions](#)

Title: Acceptable Encryption Policy

This is usually the title of the policy, for example: "Network Policies".

#### General:

- Make sure you have agreed with the [owner and collaborator](#) the scope and audience for this policy and that they are ok to take over policy reviews.
- Once you set a "Next Review" date, you won't be able to change it by editing the policy, all updates will be [handled with "Reviews"](#)

#### Policy Content:

- Here you define where your policies are kept, your options are to upload them as attachments to eramba, use URLs (to your sharepoint, Etc) or use our built in content editor (which is going to be removed sometime soon).
  - If you choose "Attachments", once the policy is created you need to upload your policy "Attachments" to a review (we'll explain this later)
  - If you choose "URL", you need to include the URL, future changes on this URL will be handled [by "Reviews"](#).
- You must include the current policy version, updates to this version will also be handled [by "Reviews"](#).

#### Access Restrictions:

- You define if this policy will be shown on the [policy portal](#) or not.
- If you choose "Authorized Users Only" then you will need [LDAP configurations](#).

Once you save this newly created policy you will notice that under "Manage" / "Reviews" there will be two entries:

Security Policy: Encryption Key Management										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	
42	Admin Admin	Admin Admin	Policy	Use URL, Q, View	Public	1.1	2014-09-15	2017-11-13	On	
Description										
The creation, management and disposal of keys are documented in this document.										
Related Documents										
Reviews										
Mitigated Items by this Policy										

One entry refers to the initial review, the review that was created with today's date. Eramba uses reviews to know which is the latest version of the policy and that's why it needs this initial review. Unless you used "Attachments" as content, you don't need to do anything with it (if you used "attachments" then you need to attach to this initial review the policy).

Reviews for "Change Management"										
Add New										
Planned Date	Actual Date	Description	Reviewer	Version	Completed	Actions	Workflows			
2017-04-30	2017-04-30	This review was created by the system at the time the policy was created - if you used "attachments" as content, then don't forget to attach policies to this review.	Admin Admin	1.5	Yes		Approved Owner			
2017-12-31	-	-	Admin Admin		No		Approved Owner			
Cancel										
										Previous Next

The other entry will refer to the future review you set while creating the policy. We explain on the Reviews chapter how to manage them, so keep reading!

## Reviewing Policies (Work on Progress, please Ignore)

Once a policy is created the version of the policy is handled by its review records, there are a few typical scenarios when handling reviews and we'll try to describe each one of them in this section:

- Update the policy version, description, etc
- Update when the new review should happen
- Update the policy due some error keeping or updating the version

Before we continue is important to understand that from the many review records a policy can have they all basically fall into three types:

- Current: This is the latest, "completed" review that eramba uses to know what is the version and document for the policy.
- Future: this are reviews planned for the future (Planned date is in the future) which are not "Completed". Based on this records eramba will know when a policy is missing review updates or not.
- Past: These are records that are "Completed" and its "Planned Date" is in the past and "Actual Date" in the past or present. The one with the latest "Actual Date" is actually the "Current" review explained above.

When you create a policy, subsequent changes to the reviews work as stated:

	<b>When Creating Policy for the first time</b>	<b>Edit existing review</b>	<b>Add a new review</b>
Publish Date	Present or Past date	NA	Same as column on the left
Planned Date	NA	You can not edit it	Present or Past
Actual Date	NA	Present or Past (but not before the "planned date")	Same as column on the left
Next Review Date	Future Date	<p>Eramba here suggest any date for any review that is:</p> <ul style="list-style-type: none"> <li>- Not completed</li> <li>- Has a "Planned date" in the future</li> </ul> <p>Instead of suggesting that date we should force the date (disable the field) to that specific date.</p>	Same as column on the left
Version	anything	<p>If there is a previous record with the following conditions:</p> <ul style="list-style-type: none"> <li>- Is completed</li> <li>- The closest actual Actual date to now()</li> </ul> <p>Then suggest the policy version of that review and complete the field.</p>	Same as column on the left

## Notifications

If you configured email notifications, everyone (the authors, collaborators, etc) should be aware of the need for a review. Once their review is completed (perhaps no modifications were required) you can review their work and if all is ok get an ACK.

## Upload Policy Review Records

The process for reviewing them is simple, just select the policy you want to review and click Manage / Review.

Security Policy: Clean Desk Policy

ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Wo
3	Admin Admin	Admin Admin	Policy	Use URL Q View	Public	1	2015-11-30	2017-04-11	Missing Reviews	

Description  
Defines the minimum requirements for maintaining a "clean desk" - where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight.

Related Documents

Reviews

Mitigated Items by this Policy

Awareness Programs

The review process applies equally to policies no matter if they miss reviews or not (you might just want to create a new version and for that purpose you also create a review by clicking on "Add New").

The list of review records will be shown in a new window, you can click on "Edit" on the review you want to complete or click "Add New" if you just want to create one ad-hoc.

Reviews for "Clean Desk Policy"

[Add New](#)

Planned Date	Actual Date	Description	Reviewer	Version	Completed	Action	Workflows
2017-04-11 (Missing)		-	Admin Admin		No	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Comments</a> <a href="#">Records</a> <a href="#">Attachments</a> <a href="#">Notifications</a> <a href="#">Reviews</a> <a href="#">Direct Link</a> <a href="#">Clone</a> <a href="#">Export PDF</a> <a href="#">View</a>	Approved Owner

Cancel Previous Next

The same form will popup in either case, make sure that on the first tab you complete the date when the review took place and tick the "Completed" checkbox (otherwise reviews are not considered completed)

Actual Date:

This is the date when the Policy actually got updated. If this is an ad-hoc review (you clicked on "Add new") then this date will be empty and most likely should be completed with todays day.

Description:

Update the policy details on the next tab.

Completed?: ☒ Yes

Unless you click on this checkbox the review will not be considered completed.

The next tab is important since you will need to define:

- The new version of the policy
- In the case of policies that use URL, you will need to include the new URL.

If eramba has a previous completed review, it will remind you what were the previous values for both these fields.

General

Policy Updates

New Version:

1.6

Enter the document new version.

The last version for this document is 1.5

Next Review Date:













2017-07-31

Enter the date in which this document should be reviewed again. Based on this date you enter here another row will be included on the system for review (you can later remove them if needed).

Dont forget to upload the policy as an attachment to this review.

You will also need to provide a date for a next review, if eramba finds a review with a date in the future that has not been completed it will suggest you to use that date (in order to avoid creating more reviews with future dates).

Once you save the review it should be completed. If you used “Attachments” don't forget to attach your new policies and sign-off documents (emails, Etc) as attachments on the policy you have just reviewed.

Planned Date	Actual Date	Description	Reviewer	Version	Completed	Action	Workflows
2017-07-31		-	Admin Admin		No	   	Approved Owner
2017-04-30	2017-04-30	This review was created by the system at the time the policy was created - If you used "attachments" as content, then dont forget to attach policies to this review.	Admin Admin	1.5	Yes	   	Approved Owner
2017-12-31	2017-05-31	Minor grammar corrections	Admin Admin	1.6	Yes	   	Approved Owner

Cancel

Previous

Next

Remember that when clicking on “View” for a policy eramba displays policies attributes based on the last completed review!

Security Policy: Change Management										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
43	Esteban Ribicic	Esteban Ribicic	Policy	Use Attachments Q View	Public	1.6	2017-04-30	2017-07-31	OK	Approved Owner
Description										

## Useful Filters

Filters are used in eramba to display data in a table format, you can select what fields you want to show, set conditions (such as only display policies with missing reviews, or policies used for PCI-DSS, Etc) and sort. The output can be exported in CSV or PDF so you can later use Spreadsheets for deep analysis or graphics.

## Security Policies

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance Management and others.














































Actions

Q Filters

Reset

Reviews

43 results

Title	Author	Tags	Publish Date	Status	Actions
Acceptable Encryption Policy	Admin Admin	Encryption Access Management	2015-11-30	Published	    
Acceptable Use Policy	Admin Admin	Equipment Use	2015-11-30	Published	    
Clean Desk Policy	Admin Admin	Physical Security Clean Desk	2015-11-30	Published	    
Data Breach Response Policy	Admin Admin	Incident Management	2015-11-30	Published	    
Disaster Recovery Plan Policy	Admin Admin	DRP BCM	2015-11-30	Published	    
Digital Signature Acceptance Policy	Admin Admin	-	2015-11-30	Published	    
Email Policy	Admin Admin	Email	2015-11-30	Published	    
Ethics Policy	Admin Admin	Privacy Ethics	2015-11-30	Published	    
Bandwidth Resource Management Policy	Admin Admin	Bandwidth Policy	2015-11-30	Published	    

You can filter data based on the policies or reviews, each will have a different scope, a few examples of useful filters:

Filter Type	Examples
Policies	<ul style="list-style-type: none"> <li>- What policies do we have, who owns them?</li> <li>- Which policies are missing reviews?</li> <li>- Which policies are used in PCI-DSS?</li> <li>- Which policies are missing reviews and are used in PCI-DSS?</li> </ul>
Reviews	<ul style="list-style-type: none"> <li>- What reviews are we missing?</li> </ul>

Once you find a filter you like, you can save it and get it sent to you as an email report. This will be useful to keep an eye on policies not being reviewed on time.

For more information on how filters work, please review our [filters documentation](#).

## Policy Notifications

Perhaps the most useful notification we can create are:

- Emails to remind of reviews (Warning type)
- Emails with reports of coming or expired reviews (you need a saved filter first)

In any case you can set up notifications by clicking on “Notifications”.

## Security Policies

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance Management and others.

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance management and others.

Add New
Workflow
Settings
Import
Notifications

Q Filters

Security Policy: Acceptable Encryption Policy

Manage

ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
1	Admin Admin	Admin Admin	Policy	Use URL Q View	Public	2.2	2015-11-30	2017-12-31	Ok	<div>Approved</div> <div>Owner</div>

Description



Clicking on “Warning” type of notifications you can set one or more notifications (10, 5 and 1 day before the review deadline). Customising the email will let you include on the subject and body of the email the policy name, description, version, review date, Etc.

### Setup Notifications

Define the notifications for current section. Notification can be either warning or awareness and their availability depends on each object

The interface shows two identical 'Warning Notification Settings' panels. The left panel has a blue box around the 'Add Warning' button and the 'Notification' dropdown menu. The right panel has a blue box around the 'Notification' dropdown menu which is open, showing a list of notification options like 'Security Policy Upcoming Review (-10 days)'.

Another useful notification is a “Report” type, that takes saved filters as inputs and sends them out in CSV or PDF at regular intervals. Having a filter that shows all policies with missing reviews to you might be useful to keep track on how on time reviews are being performed.

For details on notifications we recommend you reading [our notifications guide](#).

## Importing Policies with a CSV

You can import policies in a bulk process with the Import feature located on the top of the screen, review our [import documentation](#) to understand how this feature works in detail.

### Security Policies

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance Management and others.

The screenshot shows the 'Security Policies' interface with a table of policies. A blue arrow points to the 'Import' button in the top navigation bar.

ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	Workflows
1	Admin Admin	Admin Admin	Policy	Use URL, Q, View	Public	2.2	2015-11-30	2017-12-31	OK	Approved Owner

You will need to download the template and complete as per its instructions. If you have policies already created, you can download an “Export” which could be used as a reference to create a blank template.

We have created a [template with NIST policies](#) that might help you as a reference to get started. We recommend you use CSV imports on a testing environment as sometimes you might import data that might not be right.

## Visualising Policies

Once you create policies is important to understand how to visualise them.

Security Policy: Acceptable Encryption Policy										Manage
ID	Author	Collaborators	Document Type	Content Type	Permission	Version	Published Date	Review Date	Status	
1	Admin Admin	Admin Admin	Policy	Use URL Q View	Public	2.2	2015-11-30	2017-12-31	Ok	
Description										<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Comments</a> <a href="#">Records</a> <a href="#">Attachments</a> <a href="#">Notifications</a> <a href="#">Reviews</a> <a href="#">Direct Link</a> <a href="#">Clone</a> <a href="#">Export PDF</a> <a href="#">View</a>
Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.										
Related Documents										
Reviews										
Planned Date	Actual Date	Description	Reviewer	Comments	Completed					
2017-12-31	-	-	Admin Admin	No	No					
2017-04-11	2017-04-11	We updated some wording around change requests when handling private keys.	Admin Admin	Yes	Yes					
2017-04-11	2017-04-11	Minor changes o the policy	Admin Admin	Yes	Yes					

On the top you will find who has been defined as author and collaborators, the content type (with a link to the policy, if clicked it will display the policy on a popup), the current policy version (remember, this is obtained based on your last completed policy review) and the publish and next review date among other things.

DOCUMENT NAME		
Acceptable Encryption Policy		
DESCRIPTION		
Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.		
AUTHOR	COLLABORATORS	LAST REVIEW
Admin Admin	Admin Admin	2017-04-11
View ( <a href="https://www.sans.org/security-resources/policies/general#acceptable-encryption-policy/2.2">https://www.sans.org/security-resources/policies/general#acceptable-encryption-policy/2.2</a> )		
Version 2.2, Updated by Admin Admin on 2017-04-11. Update notes: Minor changes o the policy		
Version 2.1, Updated by Admin Admin on 2017-04-11. Update notes: We updated some wording around change requests when handling private keys.		
RELATED PROCEDURES	RELATED POLICIES	RELATED STANDARDS
No related procedures found	No related policies found	No related standards found

When you click on “View”, the policy will be displayed with all its information based on the policy and latest review information. The policy status will be “Ok” or “Missing Reviews” if there are missing reviews. The list of reviews is shown as well under “Reviews”, look on the right to make sure they are “Completed”.

Awareness Programs	
Awareness Program	Compliant Users
Awareness Training	0 users (0%)
Encryption Standards	0 users (0%)

At the bottom of the form, if you have associated awareness trainings for this policy (Security Operations / Awareness Programs) you will be shown what compliance percentage has that program.

You can also use filters to visualise policies, they show data in table format which can be useful if you just need to pull certain attributes of each policy. You can also apply filters (show me policies used in SOX, Etc), sort data, export it on CSV, etc.

### Security Policies

You are able to define at high-level your Security Policies, Standards or Procedure. This is used across the system in multiple places such as: Risks, Control, Compliance Management and others.

Actions

Q Filters

Reset

Active Filters (2 results)

Expired Reviews: Yes

Title	Author	Tags	Publish Date	Status	Actions
Clean Desk Policy	Admin Admin	Physical Security Clean Desk	2015-11-30	Published	<div><div></div><div></div><div></div><div></div><div></div></div>
Digital Signature Acceptance Policy	Admin Admin	-	2015-11-30	Published	<div><div></div><div></div><div></div><div></div><div></div></div>

[We have documented a couple of useful filters](#) you might want to have a look on. Remember that filters can be saved and used later as “Views”, sent over email regularly on CSV or PDF format for you to keep an eye on the status of your policy management practices.