NimonikApp Best Practices

Introduction

Nimonik is here to help you achieve integrated Compliance management through a three part solution that allows you to:

- Identify **Obligations** from legislation, corporate policies and other relevant documents
- Issue **Actions** to your colleagues to ensure that you remain in compliance
- Set up and conduct **Audits** to ensure your operations comply with your identified requirements

The purpose of this guide is to help you set up your account so that your Requirements Actions and Audits are being assigned to the right People in the right Places, and to help you avoid any future data restructuring.

In this document you will find a brief overview of the different components of the Nimonik compliance management system, as well as our recommendations for how to:

- Choose the correct nomenclature for your account
- Create and manage your Facilities
- Setup Users and User Teams
- Create and maintain Company Audit Templates
- Create and manage Compliance Obligations
- Add Equipment to manage your high-risk Equipment

We recommend reading it before you start generating data in your account.

Overview of Nimonikapp Structure

1. **Facilities:** Act as folders for other account items such as audits and compliance obligations.
    - **Document Level Compliance Obligations :** Lists of documents that contain requirements for your operations.
        - **Clause Level Compliance Obligations:** A more granular version of Compliance Obligations that allows you to select and monitor specific clauses within the documents.
    - **Audits:** List based inspections that are done at Facilities. They can be anything from full blown compliance audits to lite safety walkthroughs.

    - **Equipment:** On site equipment that you would like to audit
    - **Scheduler**: Manage your audit and inspection schedule and manage Internal Obligations with reporting dates
2. **Users & Teams:** People or groups of people who can be assigned responsibilities and can take action in your account.
3. **Audit Templates:** A public or company specific lists of questions, with requirements and scores, that are used to create Audits.

Determine your Account Terminology

The terminology you use in NimonikApp should be :

1. Consistent across your account
2. In line with your own corporate terminology

We recommend that you establish a naming structure for all Facilities, Audit Templates, Teams, and other account elements. The specific terminology will be dependent on your corporate structure, geography, and languages, but once it is established it should be used consistently across the app. This requires documentation for your staff and some regular training.

Please continue reading for more information about the specific account elements that you should include in your consideration.

Users

Responsibility for requirements, actions and audits can be assigned to Users and groups of Users (Teams).

Roles

What users can see and edit in your account is determined by their Role and Permissions. You can find more information on the Roles and Permission on our help page, but generally, we recommend the following:

Type of Person	Nimonik Role
Someone who: • Has global access	Account Administrator

• Adds and removes users • Generates reports • Manages the account	*We recommend limiting this to 5 people or less.*
Someone who: • Creates new Facilities, Audits, Audit Templates and other account elements • Does NOT need global access • Is NOT responsible for Account management	General User *We recommend this role for managers and support people for areas of your business that require ongoing maintenance on NimonikApp.*
Someone who: • Conducts Audits, reviews regulatory changes, issues Actions, and generally uses the system. • Does NOT need to create new Audit Templates, Compliance Obligations, or Facilities	Restricted General User *Most of your users.*
Someone who: • Requires access to all of the account data and management reports • Does NOT create or edit anything.	Read-Only Administrator *We recommend this role for users who need an overview of account activity, but are not involved in generating data.*

Permissions

User Roles determine the default access levels of your users. Once their roles have been assigned, you can use Permission to further customize what each user can do in the account. Here are some examples of access requirements and how they can be achieved using the permission and role options in Nimonik.

Access Requirements	**Permission and Role Suggestion**
• See and Edit everything	Account Administrator Role

• Manage a specific Facility • Grant access to staff • Issue audits, create compliance obligations, and perform management Actions at the Facility	General User Role with Facility Administrator permission to the designated Facility
• Permission to see and interact with specific audits, compliance obligations, and other account elements within facilities.	• General User - if they should be able to create new facilities and account elements. • Restricted General User - If they should NOT be able to create new facilities and account elements.
• See everything • Edit nothing	Read-Only Administrator *Please note that they cannot be restricted to a specific Facility, Audit or Compliance Obligation*

Teams

If you plan to have more than five users in your account, we recommend using Teams. Teams allow you to assign Actions and responsibility to groups of users. When a user team is made responsible for an account element, all team members will receive the associated notifications and access.

Since users can be added and removed from teams without affecting the Action assignment status, you can use them to easily grant access to new staff members and remove users who no longer need access.

Facilities

Facilities should reflect your physical operations. Since many parts of the site are linked to Facilities, and they are the primary filter for management reports, it is important to set them up based on your organizational structure and desired reporting output.

Most of our customers use a system based on physical location. Some common examples include

- **Country Based** - One facility per country
- **State/Province Based** - One facility per state/province
- **Factory Based** - One facility per individual factory
- **Area of Interest Based** - Each facility represents a different area of interest, such as Environment, Health and Safety, or Quality, rather than a specific physical location.

Within these facilities, you can use Tags to further separate your Audits, Actions and Compliance Obligations in reports.

Set up Tags

While Facilities are the major unit of data classification in Nimonik, Tags offer a second level of classification. Tags can be associated with Facilities, Audits and Audit Templates, and can be used to filter management reports. Please note you can use multiple tags to filter at the same time.

Tags can be used to group data both within and between facilities. As such, we recommend establishing an account wide naming convention that takes your facility structure into account. For example, if your facilities are based on Countries, you may want to use tags to designate states/provinces, or individual factories. You may also wish to use tags to indicate areas of interest, such as Environment or Health and Safety, that are common to all of your facilities.

Some popular options include:

- "**Business Unit / Department**", Ex: "Facility Management / Cleaning Services"
- "**Geographic division / Business Unit / Reporting Line**" Ex: "North America / Cosmetics / Quality Director".

Company Audit Templates

All of the Audits in your account are created from Audit Templates. These templates fall into three categories:

- **Purchased Templates** - Jurisdiction Specific Templates Created and updated by Nimonik that are available for purchase
- **Public Templates** - Free templates available to all users on the Templates Page
- **Company Audit Templates** - Templates that you create

In this section we will be focusing on Company Templates.

Naming Convention for your Templates

The name that you chose for your template will be the default title of any audits created from it. The specific naming convention that you choose will depend on your operations, but we recommend a descriptive name that can either be used as is, or that is easily modifiable by the users creating audits.

Naming Convention for Groupings and Questions

We also recommend establishing a uniform naming convention for groupings, template headings that group multiple questions together. Groupings are used to determine which questions are included when an audit is started, so we recommend giving them simple but descriptive titles.

Establishing a naming convention for individual audit questions will also make audits easier to navigate, and produce more uniform reports.

When Making Major Changes to your Templates, Create a New Version

Making major changes to an audit template may have a negative impact on the reports that consider specific audit templates and questions. As such, we recommend uploading a new version of a template for any changes that require adding, removing, or moving multiple questions. For small changes like typos, there is no need to create a new version.

Ensure that the appropriate people have access to your templates

Any user that needs to start or schedule an audit must have access to the associated audit template. For larger accounts, creating teams to grant this access may be more effective than assigning it individually.

Compliance Obligations

Compliance Obligations are where you track your requirements. Nimonik offers two levels of granularity for compliance obligations.

- **Document Level** - Allows you to track requirements on a document by document basis
- **Clause Level** - Allows you to track requirements on a requirement by requirement basis.

Set up Document Level Compliance Obligations

Whether or not you are subscribed to clause level compliance obligations, the first step to tracking your requirements is to create your document level compliance obligations. This can be done in several different ways. Depending on your specific needs, you may find it best to mix and match the different approaches described below.

Requirements	Suggested Approach
• Evaluate compliance independently at each facility • Generate a seperate review history at each facility • Receive actions for new documents at each facility • Restrict access to compliance obligations by facility	Separate Compliance Obligations at each facility
• Centrally evaluate compliance for multiple facilities • Generate a single review history for multiple facilities • Receive a single action for new documents • Allow users from different facilities to access compliance obligations	A Single Shared Compliance Obligations
• Evaluate applicability at a single facility • Evaluate compliance independently at each facility • Generate a seperate review history at each facility • Receive a single action for new documents • Restrict access to compliance obligations by facility • Issue guidelines and notes to multiple facilities	Connected Compliance Obligations

Whether they are shared or facility specific, we recommend that you organize your compliance obligations to reflect the structure of your organization. For example, if you have seperate teams to manage environmental and health and safety requirements, then you may want to create two sets of Compliance Obligations. If all of your requirements are managed by the same team, then you may prefer to create a single set of Compliance Obligations.

We also recommend that you use groupings and subgroupings to further organize documents within your compliance obligations.

Actions

The users and teams responsible for compliance obligations will receive the following Actions:

- **New Document Action** - When a new document that matches the parameters of the compliance obligations is added.
- **Document Update Action** - When a document in the compliance obligations is updated by the issuing body.
- **Internal Review Action** - When someone at your organization puts a document or clause with the status Requires Review.

Since a separate action will be issued for every matching compliance obligations or document in your account, we recommend that you minimize the number of duplicate documents, and consolidate compliance obligations that are managed by the same teams as much as possible.

Internal Obligations

Internal Obligations are obligations that your organization has imposed on itself voluntarily or through an agreement with a third party. In contrast to External Obligations which are imposed by a third party (i.e. Government), Internal Obligations are generated through the activities you engage in. Examples include corporate policies, environmental permits, contracts, stakeholder engagements and other agreements you have chosen to adopt.

There are two places where you can add Internal Obligations in Nimonik. You can add Internal Obligations in:

- **The Scheduler Module**
- **In a Compliance Obligations List**

Scheduler Module - Internal Obligations

This module allows you to link to or upload a document that contains Internal Obligations. You can then outline Reporting Requirements and indicate dates where you need to issue reports or take actions. You will receive Actions on your Actions dashboard as these dates appear.

For example, you could also use this module to manage an internal policy which requires a monthly company wide email to remind employees to conform to a prescribed standard..

Compliance Obligations - Internal Obligations

In your Compliance Obligations, you can add Internal Obligations. The functionality is the same as External Obligations. Internal Obligations can be assigned to different responsible parties or teams. They can also be assigned different statuses, for example “Requires Review”, to trigger an Internal Review Action to assess whether a Facility is in Compliance with the Internal Obligation. .

Internal Obligations can be added to existing Groupings, given an Item Name and have detailed Notes. A hyperlink to a networked document, or web page can be created in the Notes field, or in a Custom Field your organization’s Compliance Obligations. (See below, “Custom Fields in Compliance Obligations”)

An option to manage Internal Obligations is to create a Compliance Obligation list that contains only a certain type of Internal Obligation. For example, you could create a list of all of your Corporate Policies and store that in a Compliance Obligation list called “Corporate Policies”. This could then be shared across all your facilities so they can access the policies and see the guidance. If you set this up as a Connected Compliance Obligation,each Facility can add their own compliance notes and assessment to your Corporate Policies.

Link Compliance Obligations to Scheduler - Internal Obligations

If you wish, you can link Internal Obligations in the Scheduler module to Compliance Obligations. To do this, both the Internal Obligation and the Scheduler need to be in the same facility. A situation where this may be helpful is:

Link an environmental permit from the Scheduler module to the legislation that the permit is based on or that it helps you comply with. If you have a permit under The Environmental Assessment Act for your operations, you may want to link that to the Compliance Obligations that contains The Environmental Assessment Act.

Custom Fields in Compliance Obligations

Custom Fields and Notes provide text fields where you can add additional information, such as Control Measures, Risk Assessments, and facility specific information, to the documents in your compliance obligations.

While Notes are present in all Document Level compliance obligations, custom fields can be added and removed on the edit page. Since custom fields are included in reports and exports, we recommend standardizing them for all compliance obligations.

Clause Level Compliance Obligations (CLCO)

Clause Level Compliance Obligations, or CLCOs, allow you to view and evaluate entire documents on a clause by clause level. Since many documents are extremely long, we recommend using the Ignore option to hide clauses that are not relevant to your operations.

All Clauses that have been assigned a status other than “un-assessed” or “non-applicable” will be included in Document Level Compliance Obligations exports. The first five such clauses will also be included in your Document Level Compliance Obligations view on Nimonik. This will allow your team to see documents and their individual requirements side by side.

Equipment

Key pieces of equipment with compliance requirements, such as forklifts, heavy machinery, and storage units, can be entered into Nimonik as Equipment. These Equipment can be linked to Audit Templates, Audits, and Audit Questions, allowing you to periodically assess their compliance, and issue targeted findings.

For each asset, Nimonik allows you to enter a description and link relevant documents. You can also include a bar or numerical code that can be used to link the asset when auditing on the mobile app. If you have your Equipment listed in a CMMS or ERP system, they can be imported to Nimonik automatically.

Mobile Compliance Auditing software

Mobile compliance audit app can be a huge time saver. To ensure you get the most out of your mobile experience, it is critical that you set up your account properly, as described above. The most important settings are User Permissions and Facilities. Getting the right information to the right people will help make the experience better and synchronization faster.

Synchronization of Mobile Apps

Synch often and ensure permissions are properly set up. Administrators get all the data on the website, so it is critical that you limit the number of administrators.

On iOS, to synchronize, you need to leave the app open. Closing it will stop synchronization after a couple minutes.

On Android, the synchronization should continue in the background.

In order to reduce syn time, we recommend using the Mobile On/Off feature to limit the number of audits that are available on Mobile. This feature can be used manually, or set up to work automatically.

Conclusion

As with any system, it is critical that you set up your account properly to ensure you receive the correct alerts and reports, and that you benefit from the full value of your subscription.

For assistance in setting up your account, please do not hesitate to contact us at support@nimonik.com or by telephone at +1-888-608-7511