# Comprehensive Compliance Workshop Workbook

**Comprehensive Compliance - Obligations, Actions, Audits**

Last Updated: January 2020

Created by Nimonik (www.Nimonik.com)

info@nimonik.com

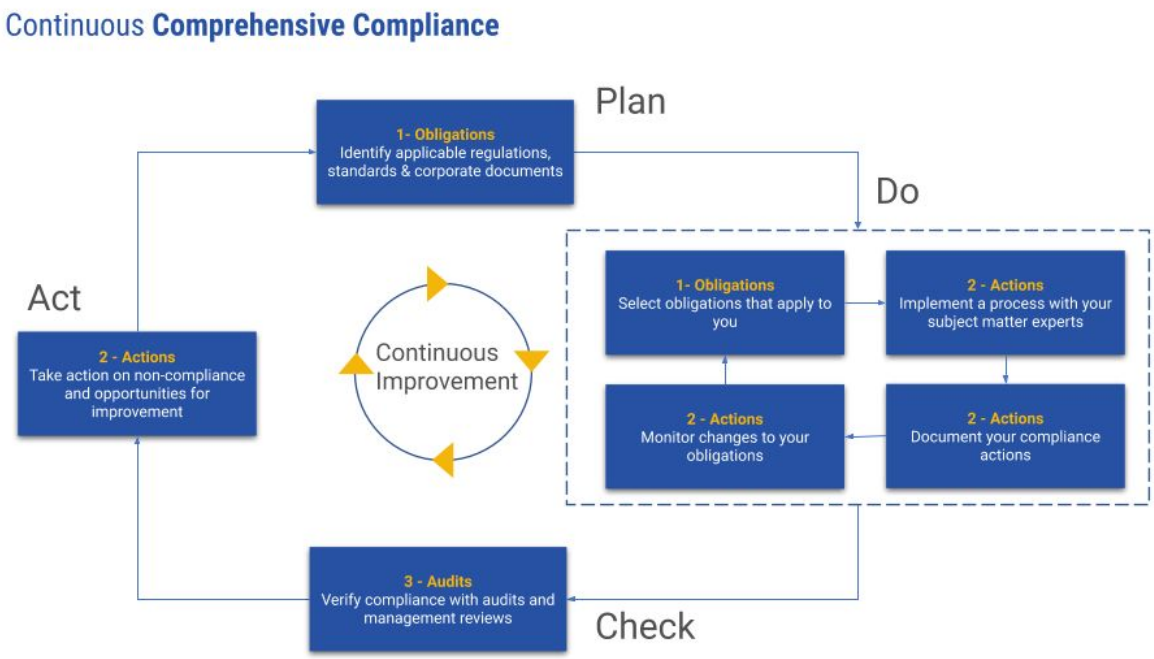
# Introduction

***Regulations and standards exist to incite behaviour that would not naturally occur.***

Compliance may not always be fun, but we believe that it is the critical foundation of a well-run organization. We hope this workbook will help you align your management, staff, contractors and stakeholders around a compliance program that keeps your organization running smoothly.

# Nimonik 7-Step Comprehensive Compliance Program

Nimonik has developed a 7-step program to ensure comprehensive compliance. This workbook is designed to guide you through the process. The seven steps are outlined below and the workbook contains information on each step. This document is being updated frequently. To obtain the most recent copy, contact info@nimonik.com and please do not hesitate to share your thoughts and comments on this document with us.



# General Information

| Information | Notes | Example |
|---|---|---|
| Organization name | | |
| Headquarters location | | |
| Description of operations | | General Manufacturing and Distribution |
| # Sites | | |
| Type of Sites | | Office, Manufacturing, Transport |
| # Jurisdictions organization operates in | | |
| Compliance team headcount | | |
| Describe organization structure | | |
| Identify main organizational components with compliance roles | | Environment, Safety, Finance, Legal, HR... |

| | | |
|---|---|---|
| Fines or penalties received in past 5 years | | |
| Company size (market cap) | | |
| Company size (staff) | | |
| Management systems in place | | Quality, Safety... |
| Certifications in place | | ISO 9001, ISO 14001, EMS... |

| Current Context - Assessment | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Describe the culture of the society you operate in and how it regards compliance. | | Japan takes compliance very seriously and it is well embedded in the average person's behaviour. | 4.1 Understanding the organization and its context | The organization should determine external and internal issues, such as those related to compliance risks, that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its compliance management system. In doing so, the organization should consider a broad range of external and internal aspects, such as the regulatory, social and cultural contexts, the economic situation and the internal policies, procedures, processes and resources. |
| Describe the government culture with regards to compliance. Discuss specific government agencies you work with and how they treat compliance. | | The EPA and OSHA do regular and diligent inspections. Fines are levied regularly by government agencies. | | |
| Describe the current general company culture with regards to compliance. | | The company puts some emphasis on compliance, but it is not a core message for our EHS teams. | | |
| Does your company have a compliance policy? What are the general lines of the policy? | | Yes. Not sure about the general lines. | | |

| | | | | |
|---|---|---|---|---|
| Describe the management's perception of compliance. | | They understand it is important, but it is not a top priority for them. | 5.3.5 Management responsibilities | Management should be responsible for compliance within its area of responsibility. This includes:<br>a) cooperating with and supporting the compliance function and encouraging employees to do the same;<br>b) personally complying and being seen to comply with policies, procedures and processes and<br>attending and supporting compliance training activities;<br>c) identifying and communicating compliance risks in their operations; |

| Interested Parties - Assessment | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Do employees and contractors understand their responsibility to meet compliance obligations and respect your compliance policy? | | | 5.3.6 Employee responsibility | All employees, including managers, should:<br>a) adhere to the compliance obligations of the organization that are relevant to their position and duties;<br>b) participate in training in accordance with the compliance management system;<br>c) use available compliance resources as a part of the compliance management system;<br>d) report compliance concerns, issues and failures. |
| Can employees, contractors and other parties easily report a non-compliance? | | | 7.3.2.2 Role of top management in encouraging compliance | d) creating an environment where the reporting of noncompliance is encouraged and the reporting employee will be safe from retaliation; |
| Are new compliance obligations, non-compliances and compliance issues regularly communicated to appropriate parties? | | | 7.4.1 General | The organization should determine the need for internal and external communications relevant to the compliance management system, including:<br>a) on what it will communicate;<br>b) when to communicate;<br>c) with whom to communicate;<br>d) how it will communicate. |
| Who is the most senior compliance official at the company? What are their reporting responsibilities and | | | 4.4 Compliance management system and principles of good governance | The organization should establish, develop, implement, evaluate, maintain and continually improve a compliance management system, including the processes needed and their interactions, in accordance with this International Standard, taking into consideration the following governance principles:<br>— direct access of the compliance function to the |

| | | | | |
|---|---|---|---|---|
| the size of their team? | | | | governing body;<br>— independence of the compliance function;<br>— appropriate authority and adequate resources allocated to the compliance function.<br>The compliance management system should reflect the organization's values, objectives, strategy and compliance risks.<br>The scope should be readily available as documented information. |
| What authority does the most senior compliance official have? | | | 5.3.4 Compliance function | Not all organizations will create a discrete compliance function, some may assign this function to an existing position.<br>The compliance function, working together with management, should be responsible for:<br>a) identifying compliance obligations with the support of relevant resources and translating those obligations into actionable policies , procedures and processes;<br>b) integrating compliance obligations into existing policies, procedures and processes ;<br>c) providing or organizing on-going training support for employees to ensure that all relevant employees are trained on a regular basis;<br>d) promoting the inclusion of compliance responsibilities into job descriptions and employee performance management processes;<br>e) setting in place a compliance reporting and documenting system;<br>f) developing and implementing processes for managing information, such as complaints and/or feedback by means of hotlines, a whistle-blowing system and other mechanisms;<br>g) establishing compliance performance indicators and monitoring and measuring compliance performance; |

| | | | | |
|---|---|---|---|---|
| | | | | h) analysing performance to identify the need for corrective action;<br>i) identifying compliance risks and managing those compliance risks relating to third parties, such as suppliers, agents, distributors, consultants and contractors;<br>j) ensuring the compliance management system is reviewed at planned intervals;<br>k) ensuring there is access to appropriate professional advice in the establishment and implementation and maintaining of the compliance management system;<br>l) providing employees with access to resources on compliance procedures and references;<br>m) providing objective advice to the organization on compliance-related matters.<br>NOTE Guidelines for complaints handling are provided in ISO 10002.<br>In allocating responsibility for compliance management, consideration should be given to ensuring that<br>the compliance function has no conflict of interest and has demonstrated:<br>— integrity and commitment to compliance;<br>— effective communication and influencing skills;<br>— an ability and standing to command acceptance of advice and guidance;<br>— relevant competence. |
| Do the compliance officials within the company have sufficient resources to carry out their duties? | | | 7.1 Resources | The organization should determine and provide the resources needed for the establishment, development, implementation, evaluation, maintenance and continual improvement of the compliance management system appropriate to its size, complexity, structure and operations.<br>Top management and all other levels of management should ensure that the necessary resources are |

| | | | | |
|---|---|---|---|---|
| | | | | deployed effectively to ensure that the compliance management system meets its objectives, and that compliance is achieved.<br>Resources include financial and human resources, as well as access to external advice and specialized skills, organizational infrastructure, contemporary reference material on compliance management and legal obligations, professional development and technology. |
| If there is a lack of resources, determine what are the immediate next steps? | | Pair down program, communicate to management, resign,... | | |
| Do the compliance officials have independence from operations and have the ability to halt operations if required? | | | 4.4 Compliance management system and principles of good governance | The organization should establish, develop, implement, evaluate, maintain and continually improve a compliance management system, including the processes needed and their interactions, in accordance with this International Standard, taking into consideration the following governance principles:<br>— direct access of the compliance function to the governing body;<br>— independence of the compliance function;<br>— appropriate authority and adequate resources allocated to the compliance function.<br>The compliance management system should reflect the organization's values, objectives, strategy and compliance risks.<br>The scope should be readily available as documented information. |
| Is your compliance policy easily available to all staff? | | | | |

| | | | | |
|---|---|---|---|---|
| Is your compliance policy known by all staff? | | | | |

| Policy - Improvement | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Describe the interested parties with regards to compliance | | Customers, Suppliers, Management, Shareholders... | 4.2 Understanding the needs and expectations of interested parties | "The organization should determine:<br>— the interested parties that are relevant to the compliance management system;<br>— the Obligations of these interested parties." |
| What are the interested parties' needs? | | Continuous operation to ensure on-time deliveries, regular audits to demonstrate ongoing compliance to a standard | | |

| | | | | |
|---|---|---|---|---|
| Describe the <u>desired</u> general company culture with regards to compliance | | | 7.3.2.3 Compliance culture | The development of a compliance culture requires the active, visible, consistent and sustained<br>commitment of the governing body, top management and management towards a common, published standard of behaviour that is required throughout every area of the organization.<br>EXAMPLE Examples of factors that will support the development of a compliance culture include:<br>— a clear set of published values;<br>— management actively seen to be implementing and abiding by the values;<br>— consistency in the treatment of similar actions, regardless of position;<br>— mentoring, coaching and leading by example;<br><br>ISO 19600:2014(E)<br>— appropriate pre-employment assessment of potential employees;<br>— an induction or orientation program that emphasizes compliance and the organization's values;<br>— ongoing compliance training, including updates to the training;<br>— on-going communication on compliance issues;<br>— performance appraisal systems that consider assessment of compliance behaviour and take into account<br>performance pay to achieve compliance key performance measures and outcomes;<br>— visible recognition of achievements in compliance management and outcomes;<br>— prompt and proportionate disciplining in the case of wilful or negligent breaches of compliance obligations;<br>— a clear link between the organization's strategy and individual roles, reflecting compliance as essential to<br>achieving organizational outcomes;<br>— open and appropriate communication about compliance.<br>Evidence of a compliance culture is indicated by the degree to which:<br>— the items above are implemented;<br>— stakeholders (particularly employees) believe that the items above have been implemented;<br>— employees understand the relevance of the compliance obligations related to their own activities |

| | | | | |
|---|---|---|---|---|
| | | | | and to those of their business unit;<br>— remediation of noncompliance is 'owned' and actioned at all appropriate levels of the organization<br>as required;<br>— the role of the compliance function and its objectives are valued;<br>— employees are enabled and encouraged to raise compliance concerns to the appropriate level of<br>management. |
| Describe the <u>desired</u> perception by management of compliance. | | | 7.3.2.2 Role of top management in encouraging compliance | Top management has a key responsibility for:<br>a) aligning the organization's commitment to compliance to its values, objectives and strategy in order<br>to position compliance appropriately;<br>b) communicating its commitment to compliance in order to build awareness and motivate employees<br>to embrace the compliance management system;<br>c) encouraging all employees to accept the importance of achieving the compliance objectives for<br>which they are responsible or accountable;<br>d) creating an environment where the reporting of noncompliance is encouraged and the reporting<br>employee will be safe from retaliation;<br>e) encouraging employees to make suggestions that facilitate continual improvement in compliance<br>performance;<br>f) ensuring compliance is incorporated into the broader organization culture and culture change initiatives;<br>g) identifying and acting promptly to correct or address noncompliance;<br>h) ensuring that organizational policies, procedures and processes support and encourage compliance;<br>i) ensuring that operational objectives and targets do not compromise compliant behaviour. |

| | | | | |
|---|---|---|---|---|
| Describe the roadblocks to changing management and company culture. | | Lack of awareness of risks, cost sensitive, top management does not believe compliance and culture and profits go together. | | |

| Scope & Authority | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Describe the scope of the compliance policy you would like to implement in this workbook. | | Our Compliance Policy and Management System will apply to all employees, contractors, suppliers at all times. It will cover our direct operations as well as any joint ventures and partnerships we have. The Compliance Policy will be implemented at contractors and vendors based on the services they Provide. The Compliance Policy will be shared publicly and annual reports will be provided to upper management. | 4.3 Determining the scope of the compliance management system | The organization should determine the boundaries and applicability of the compliance management system to establish its scope.<br>When determining this scope, the organization should consider: — the external and internal issues referred to in 4.1;<br>When determining this scope, the organization should consider: — the Obligations referred to in 4.2 and 4.5.1.<br>NOTE The scope of the compliance management system is intended to clarify the geographical and/or organizational boundaries to which the compliance management system will apply, especially if the organization is a part of a larger organization at a given location. |
| What is the desired knowledge of compliance policy by employees, management, contractors and other interested parties? | | Awareness of policy and understanding that it is a critical business Obligation | 7.3.1 General | Persons doing work under the organization's control should be aware of:<br>a) the compliance policy;<br>b) their role and contribution to the effectiveness of the compliance management system, including the benefits of improved compliance management system performance;<br>c) the implications of not conforming with the compliance management system Obligations. |

| | | | | |
|---|---|---|---|---|
| What type of rewards and punishment for compliance issues could you introduce at your organization? | | | 7.3.2.1 General | Behaviour that creates and supports compliance should be encouraged and behaviour that compromises compliance should not be tolerated. |

| Risk Assessments (post Step 2, 5, 6) | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Has a risk assessment been done in Step 2 - Obligations? | | | 4.6 Identification, analysis and evaluation of compliance risks | The organization should identify and evaluate its compliance risks. This evaluation can be based on a formal compliance risk assessment or conducted via alternative approaches. Compliance risk assessment constitutes the basis for the implementation of the compliance management system and the planned allocation of appropriate and adequate resources and processes to manage identified compliance risks.<br>The organization should identify compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations in order to identify situations where noncompliance can occur. The organization should identify the causes for and consequences of noncompliance.<br>The organization should analyse compliance risks by considering causes and sources of noncompliance and the severity of their consequences, as well as the likelihood that noncompliance and associated consequences can occur. Consequences can include, for example, personal and environmental harm, economic loss, reputational harm and administrative liability.<br>Risk evaluation involves comparing the level of compliance risk found during the analysis process with the level of compliance risk the organization is able and willing to accept. Based on this comparison, priorities can be set as a basis for determining the need for implementing controls and the extent of these controls (see 6.1).<br>The compliance risks should be reassessed periodically and whenever there are:<br>— new or changed activities, products or services;<br>— changes to the structure or strategy of the organization;<br>— significant external changes, such as financial-economic circumstances, |

| | | | | |
|---|---|---|---|---|
| | | | | market conditions,<br>liabilities and client relationships;<br>— changes to compliance obligations (see 4.5);<br>— noncompliance(s).<br>NOTE 1 The extent and level of detail of the compliance risk assessment are dependent on the risk situation,<br>context, size and objectives of the organization and can vary for specific sub-areas (e.g. environment, financial, social).<br>NOTE 2 The risk-based approach to compliance management does not mean that for low compliance risk<br>situations, noncompliance is accepted by the organization. It assists organizations in focussing primary attention<br>and resources on higher risks as a priority, and ultimately will cover all compliance risks. All identified compliance<br>risks/situations are subject to monitoring, correction and corrective action." |
| Have risk assessments been updated in Step 5? | | | | |
| Have risk assessments been validated in Step 6? | | | | |
| Who is responsible for compliance in the supply chain or outsourced parties? | | | 8.3 Outsourced processes | The organization should ensure that outsourced processes are controlled and monitored.<br>Outsourcing of an organization's operations usually does not relieve the organization of its legal<br>responsibilities or compliance obligations. If there is any outsourcing of the organization's activities, the<br>organization needs to undertake effective due diligence to ensure that its standards and commitment<br>to compliance will not be lowered. Controls over contractors should also be in place to ensure that the<br>contract is complied with effectively (e.g. third-party performance appraisals).<br>The organization should consider compliance risks related to other<br>third-party-related processes, such |

| | | | | |
|---|---|---|---|---|
| | | | | as supply of goods and services and distribution of products, and put controls in place, as necessary (e.g.<br>compliance obligations in contractual clauses). |

| Training | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Are staff trained appropriately on compliance? What type of training is missing? | | | 7.2.2 Training | The governing body, management and all employees have compliance obligations should be competent to discharge these effectively. The attainment of competence can be achieved in many ways, including<br>skills and knowledge required through education, training or work experience.<br>The objective of a training program is to ensure that all employees are competent to fulfil their job role in a manner that is consistent with the organization's compliance culture and its commitment to compliance. Properly designed and executed training can provide an effective way for employees to communicate previously unidentified compliance risks. Education and training of employees should be:<br>a) tailored to the obligations and compliance risks related to the roles and responsibilities of the employee;<br>b) where appropriate, based on an assessment of gaps in employee knowledge and competence;<br>c) undertaken at commencement with the organization and be on-going ;<br>d) aligned to the corporate training program and be incorporated into annual training plans;<br>e) practical and readily understood by employees;<br>f) relevant to the day-to-day work of employees and illustrative of the industry, organization or sector concerned;<br>g) sufficiently flexible to account for a range of techniques to accommodate the differing needs of organizations and employees;<br>NOTE Interactive training might be the best form of training, if noncompliance could result in serious consequences.<br>h) assessed for effectiveness;<br>i) updated as required;<br>j) recorded and retained.<br>Compliance retraining should be considered whenever there is a:<br>— change of position or responsibilities;<br>— changes in internal, policies, procedures and processes;<br>— changes in organization structure;<br>— change in the compliance obligations, especially in legal or interested parties |

| | | | | |
|---|---|---|---|---|
| | | | | Obligations;<br>— change in activities, products or services;<br>— issues arising from monitoring, auditing, reviews, complaints and noncompliance, including stakeholder feedback. |

| Reporting | | | | |
|---|---|---|---|---|
| Question | Notes | Example | ISO 19600 Element | ISO 19600 Guidance |
| Are audit reports from Step 6 shared? | | | 9.1.7 Compliance reporting | The governing body, management and the compliance function should ensure that they are effectively informed on the performance of the organization's compliance management system and of its continuing adequacy, including all relevant noncompliances, in a timely manner and actively promote the principle that the organization encourages and supports a culture of full and frank reporting. Internal reporting arrangements should ensure that:<br>a) appropriate criteria and obligations for reporting are set out;<br>b) timelines for regular reporting are established;<br>c) an exception reporting system is in place which facilitates ad hoc reporting of emerging<br>noncompliance;<br>d) systems and processes are in place to ensure the accuracy and completeness of information;<br>e) accurate and complete information is provided to the correct functions or areas of the organization<br>to enable preventative, corrective and remedial action to be taken;<br>f) there is sign-off on the accuracy of reports to the governing body, including by the compliance function.<br>An organization should choose a format, content and timing of its internal compliance reporting that is appropriate to its circumstances, unless otherwise specified by law.<br>Reporting on compliance should be incorporated in standard organizational reports.<br>Separate reports should only be prepared for major noncompliance and for emerging issues.<br>All noncompliance need to be appropriately reported. While the reporting of systemic and recurring<br>problems is particularly important, a one-off noncompliance can be of equal concern if it is major or deliberate. Even a small failure may indicate serious weakness in the current process and the compliance management system. If not reported in a timely manner, it can lead to the view that the failure does not matter and can result in such failure becoming a systemic problem. |

| | | | | |
|---|---|---|---|---|
| | | | | Employees should be encouraged to respond and report noncompliance with the law and other<br>incidents of noncompliance, and to see reporting as a positive and<br>non-threatening action without fear of retaliation.<br>Reporting obligations should be set out clearly in the organization's compliance policy and procedures<br>and reinforced by other methods, such as informal reinforcement by managers during their day-to-day<br>work with employees. |
| When and who can prepare an overall compliance plan at your organization based on the reports provided after audits, policy development and the assessment done in this workbook? | | | 6.2 Compliance objectives and planning to achieve them | The organization should establish its compliance management system objectives at relevant<br>functions and levels.<br>The compliance objectives should:<br>a) be consistent with the compliance policy;<br>b) be measurable (if practicable);<br>c) take into account applicable Obligations;<br>d) be monitored;<br>e) be communicated;<br>f) be updated and/or revised as appropriate.<br>When planning how to achieve its compliance objectives, the organization should determine:<br>— what will be done;<br>— what resources will be required;<br>— who will be responsible;<br>— when it will be completed;<br>— how the results will be evaluated, e.g. pursuant to identified compliance key performance measures<br>and outcomes.<br>The organization should retain documented information on the compliance objectives and on the<br>planned actions to achieve them." |

# Step 1 - Identification of Sources

| Obligations | Sources | Describe the culture the source organization | Applies to which part of your organization | Documents Identified? | Last Updated | Reviewed By |
|---|---|---|---|---|---|---|
| Obligations | Government agencies (i.e. EPA, OSHA...) | | | No | | |
| Commitments | Industry Standards | | | | | |
| Obligations | Other Legislation, Regulations, Codes, Rules... | | | | | |
| Obligations | International Treaties | | | | | |
| Obligations | Government Permits and Authorization | | | | | |
| Obligations | Court Judgements | | | | | |
| Commitments | Stakeholder Engagements | | | | | |
| Commitments | Customer Requests | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Commitments | Contractual Obligations | | | | | |
| Commitments | Organizational Policies | | | | | |

**ISO 19600 Guidance**

4.5.1 Identification of compliance obligations
The organization should systematically identify its compliance obligations and their implications for its activities, products and services. The organization should take these obligations into account in establishing, developing, implementing, evaluating, maintaining and improving its compliance management system. The organization should document its compliance obligations in a manner that is appropriate to its size, complexity, structure and operations. Sources of compliance obligations should include compliance requirements and can include compliance commitments.

# Step 2 - Requirements

| Source (see Step 1) | Responsible part of organization | Document Type | Unique Obligation Number | Document Name | Document Identifier | Clause identifier | Clause Text | Explanation | Applicability to Organization | Risk |
|---|---|---|---|---|---|---|---|---|---|---|
| EPA | Environment | Obligation | 1 | 40CFR Part 10 | | 40CFR Part 10 Clause 126 | | | | |
| | Public Safety | Commitment | | | | | | | | |
| Internal Obligation | HR | Recommendation | 3 | Sexual Harassment Policy | | Sexual Harassment Policy Article 9 | | | | |
| | Customer | | | | | | | | | |
| | Finance | | | | | | | | | |
| | Occupational Safety | | | | | | | | | |
| | Outsourced | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

**ISO 19600 Guidance**

6.2 Compliance objectives and planning to achieve them
The organization should establish its compliance management system objectives at relevant functions and levels.
The compliance objectives should:
a) be consistent with the compliance policy;
b) be measurable (if practicable);
c) take into account applicable requirements;
d) be monitored;
e) be communicated;
f) be updated and/or revised as appropriate.
When planning how to achieve its compliance objectives, the organization should determine:
— what will be done;
— what resources will be required;
— who will be responsible;
— when it will be completed;
— how the results will be evaluated, e.g. pursuant to identified compliance key performance measures and outcomes.
The organization should retain documented information on the compliance objectives and on the planned actions to achieve them.

# Step 3 - Subject Matter Experts (SMEs)

| Person/Team | Job Title | Competence Assessment | Applies to which part of your organization (Step 1) | Location | Reports to | Unique Obligations (Step 2) |
|---|---|---|---|---|---|---|
| Corporate Environment Team | VP EHS | Yes, has competence | Environment | HQ | CEO | 1 |
| | | No, reuquires training | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**ISO 19600 Guidance**

7.2.1 Competence

The organization should:
a) determine the necessary competence of employee(s) doing work under its control that affects its compliance management system performance;
b) ensure that these employees are competent on the basis of appropriate education, training and/or work experience;
c) where applicable, take actions to acquire the necessary competence and evaluate the effectiveness of the actions taken;
d) retain appropriate documented information, including evidence of competence.
NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the reassignment of employees; or the hiring or contracting of competent persons.

# Step 4 - Planned Actions

| Trigger | Unique Obligations (Step 2) | Information Source | Action | Expected Notes Content | Delay to Respond | Controls |
|---|---|---|---|---|---|---|
| Issues from General Information Tab | | | | | | |
| Issues from Step 2 - Obligations | | | | | | |
| Regulatory Change | 1 | Mailing List of Regulatory Agency | Review change and assign to SME | Notes should contain - affected part of the site, - responsible departments, -actions required... | - 5 days for internal triage<br>- 2 weeks for SME to review | |
| Company Policy Change | 3 | Internal Email | Retraining of all staff | They sign that they received sexual harassment training | 2 months | |
| Permit Renewal | | Internal Document Management System | | | | |
| Operational Change | | Quarterly Engineering Meetings | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## ISO 19600 Guidance

6.1 Actions to address compliance risks
When planning for the compliance management system, the organization should consider the issues referred to in 4.1, the requirements referred to in 4.2, the principles of good governance referred to in 4.4, the compliance obligations identified in 4.5 and the results of the compliance risk assessment referred to in 4.6 to determine the compliance risks that need to be addressed to:
— assure the compliance management system can achieve its intended outcome(s);
— prevent, detect and reduce undesired effects;
— achieve continual improvement.
The organization should plan:
a) actions to address these compliance risks and
b) how to:
— integrate and implement the actions into its compliance management system processes;
— evaluate the effectiveness of these actions.
The organization should retain documented information on the compliance risks and on the planned actions to address them.

6.2 Compliance objectives and planning to achieve them
The organization should establish its compliance management system objectives at relevant functions and levels.
The compliance objectives should:
a) be consistent with the compliance policy;
b) be measurable (if practicable);
c) take into account applicable requirements;
d) be monitored;
e) be communicated;
f) be updated and/or revised as appropriate.
When planning how to achieve its compliance objectives, the organization should determine:
— what will be done;
— what resources will be required;
— who will be responsible;
— when it will be completed;
— how the results will be evaluated, e.g. pursuant to identified compliance key performance measures and outcomes.
The organization should retain documented information on the compliance objectives and on the planned actions to achieve them."

| |
|---|
| 4.5.2 Maintenance of compliance obligations<br>Organizations should have processes in place to identify new and changed laws, regulations, codes and other compliance obligations to ensure ongoing compliance. Organizations should have processes to evaluate the impact of the identified changes and implement any changes in the management of the compliance obligations.<br>EXAMPLE Examples of processes to obtain information on changes to laws and other compliance obligations include:<br>— being on the mailing lists of relevant regulators;<br>— membership of professional groups;<br>— subscribing to relevant information services;<br>— attending industry forums and seminars;<br>— monitoring the websites of regulators;<br>— meeting with regulators;<br>— arrangements with legal advisors;<br>— monitoring the sources of the compliance obligations (e.g. regulatory pronouncements and court decisions). |
| 8.1 Operational planning and control<br>The organization should plan, implement and control the processes needed to meet compliance obligations, and to implement the actions determined in 6.1, by:<br>— defining the objectives of the processes;<br>— establishing criteria for the processes;<br>— implementing control of the processes in accordance with the criteria;<br>— keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.<br>The organization should control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. |

8.2 Establishing controls and procedures

Controls should be put in place to manage the identified compliance obligations and associated compliance risk and to achieve desired behaviour. Effective controls are needed to ensure that the organization's compliance obligations are met and that non compliances are prevented or detected and corrected. The types and levels of controls should be designed with sufficient rigour to facilitate achieving the compliance obligations that are particular to the organization's activities and operating environment. Such controls should, where possible, be embedded into normal organizational processes.

— clear, practical and easy to follow documented operating policies, procedures, processes and work instructions;
— systems and exception reports;
— approvals;
— segregation of incompatible roles and responsibilities;
— automated processes;
— annual compliance plans;
— employee performance plans;
— compliance assessments and audits;
— demonstrated management commitment and exemplary behaviour and other measures to promote compliant behaviour;
— active, open and frequent communication on expected behaviour of employees (standards and value, codes of conduct).

These controls should be maintained, periodically evaluated and tested to ensure their continuing effectiveness.

Procedures should be established, documented, implemented and maintained to support the compliance policy and translate the compliance obligations into practice.
In developing these procedures consideration should be given to:
a) integrating the compliance obligations into procedures, including computer systems, forms, reporting systems, contracts and other legal documentation;
b) consistency with other review and control functions in the organization;
c) ongoing monitoring and measurement;
d) assessment and reporting (including management supervision) to ensure that employees comply with procedures;
e) specific arrangements for identifying, reporting and escalating instances of noncompliance and risks of noncompliance.

# Step 5 - Monitor for Changes

| Unique Obligations (Step 2) | Source (Step 1) | Frequency of Checking for Updates | Responsible Role (Step 1) | Internal Communication Method | Expected Actions | Internal Reporting Expectations | Re-evaluate Risk Required? |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 1 | Government Agencies | Weekly | Corporate Environment Team | Email blast to all Environmental People in the Organization | Update their policies and their procedures | Email back confirming action | Yes |
| | Industry Standards | | | | | | |
| | Other Legislation, Regulations, Codes, Rules... | | | | | | |
| | International Treaties | | | | | | |
| | Government Permits and Authorization | | | | | | |
| | Court Judgements | | | | | | |
| | Stakeholder | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Engagements | | | | | | |
| | Customer Requests | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## ISO 19600 Guidance

7.5.1 General
The organization's compliance management system should include:
a) documented information recommended by this International Standard;
b) documented information determined by the organization as being necessary for the effectiveness of the compliance management system.
EXAMPLE Examples of documented information include:
— the organization's compliance policy;
— the objectives, targets, structure and content of the compliance management system;
— allocation of roles and responsibilities for compliance;
— register of relevant compliance obligations;
— compliance risk registers and prioritization of the treatment based on the compliance risk assessment process;
— register of non compliances and near misses;
— annual compliance plans;
— personnel records, including, but not limited to, training records.
NOTE 1 Documented information can include matters relating to regulatory reporting requirements.
NOTE 2 The extent of documented information for a compliance management system can differ from one organization to another due to:
— the size of organization and its type of activities, processes, products and services;
— the complexity of processes and their interactions;

— the competence of employees;
— the maturity of the compliance management system.

7.5.2 Creating and updating
When creating and updating documented information the organization should ensure appropriate:
— identification and description (e.g. a title, date, author, or reference or version number);
— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
— review and approval for suitability and adequacy.

7.5.3 Control of documented information
Documented information recommended by the compliance management system and by this International Standard should be controlled to ensure:
a) it is available, accessible and suitable for use, where and when it is needed;
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
For the control of documented information, the organization should address the following activities, as applicable:
— distribution, access, retrieval and use;
— storage and preservation, including preservation of legibility;
— control of changes (e.g. version control);
— retention, disposition and disposal;
— the role of third parties in documented information creation and control.
Documented information of external origin determined by the organization to be necessary for the planning and operation of the compliance management system should be identified, as appropriate, and controlled.
Documented information may be prepared for the purpose of obtaining legal advice and therefore may be the subject of legal privilege.
NOTE Access implies a decision regarding the permission to view the documented information only, or the
permission and authority to view and change the documented information, etc.

# Step 6 - Compliance Audits

| Unique Obligations (Step 2) | Type of Audit | Unique Audit Number | Location | Audit Frequency | Effectiveness Assessment included in Audit? | Outcome | Risk Re-Evaluated during Audit? |
|---|---|---|---|---|---|---|---|
| 3 | Internal 1st Party Audit | 234 | Scranton Location | Annual | Yes | Report to Corporate and to HR | |
| | Internal 2nd Party Audit | | | | | | |
| | External 3rd Party Audit | | | | | | |
| | Safety Walkthrough | | | | | | |
| | Environmental Walkthrough | | | | | | |
| | Pop Quiz on EHS Principles | | | | | | |
| | Assessment of Training of Staff | | | | | | |
| | Management Review | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## ISO 19600 Guidance

9.1.2 Monitoring
The compliance management system should be monitored to ensure compliance performance is achieved. A plan for continual monitoring should be established, setting out monitoring processes, schedules, resources and the information to be collected. Compliance monitoring is the process of gathering information for the purpose of assessing the effectiveness of the compliance management system and of the organization's compliance performance. Monitoring of the compliance management system typically includes:
— effectiveness of training;
— effectiveness of controls, e.g. by sample testing outputs;
— effective allocation of responsibilities for meeting compliance obligations;
— currency of compliance obligations;
— effectiveness in addressing compliance failures previously identified;
— instances where internal compliance inspections are not performed as scheduled.
Monitoring of compliance performance typically includes:
— noncompliance and "near misses" (i.e. incidents without adverse effect);
— instances where compliance obligations are not met;
— instances where objectives are not achieved;
— status of compliance culture;
— leading and lagging indicators established under 9.1.6.

9.2 Audit
The organization should conduct audits at least at planned intervals to provide information on whether the compliance management system:
a) conforms to:
1) the organization's own criteria for its compliance management system;
2) the recommendations of this International Standard;
b) is effectively implemented and maintained.
Additional audits can also be conducted as required.
The organization should:
— plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) should take into consideration the importance of the processes concerned and the results of previous audits;

— define the audit criteria and scope for each audit;
— select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
— ensure that the results of the audits are reported to relevant management;
— retain documented information as evidence of the implementation of the audit programme and the audit results.

9.3 Management review
Top management should review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The actual depth and frequency of such reviews will vary with the nature of the organization and its policies.
The management review should include consideration of:
a) the status of actions from previous management reviews;
b) the adequacy of the compliance policy;
c) the extent to which the compliance objectives have been met;
d) adequacy of resources;
e) changes in external and internal issues that are relevant to the compliance management system;
and measurement results,
— communication from interested parties, including complaints;
— audit results;
g) opportunities for continual improvement.

The outputs of the management review should include decisions related to continual improvement opportunities and any need for changes to the compliance management system. It should include also recommendations on:
a) the need for changes to the compliance policy, its associated objectives, systems, structure and personnel;
b) changes to compliance processes to ensure effective integration with operational practices and systems;
c) areas to be monitored for potential future noncompliance;
d) corrective actions with respect to noncompliance;
e) gaps or lack in current compliance systems and longer term continual improvement initiatives;
f) recognition of exemplary compliance behaviour within the organization.

The organization should retain documented information as evidence of the results of management reviews and a copy should be provided to the governing body.

# Step 7 - Follow-Up Actions

| Action Tracking Location | Linked Unique Obligations (Step 2) | Effectiveness Assessment Delay after Action is Taken | Risk Re-Evaluation Needed? | New Obligation Identified? |
|---|---|---|---|---|
| Nimonik Software | 3 | 6 months | | |
| | | 2 months | | |
| | | 1 months | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

ISO 19600 Guidance

9.1.9 Record-keeping
Accurate, up-to-date records of the organization's compliance activities should be maintained to assist in the monitoring and review process and demonstrate conformity with the compliance management system. Record-keeping should include recording and classifying complaints, disputes and alleged noncompliance and the steps taken to resolve them.
Records should be stored in a manner that ensures they remain legible, readily identifiable and retrievable. These records should be protected against any addition, deletion, modification, unauthorized use or concealment. The organization's compliance management system records can include:
a) information on compliance performance, including compliance reports;
b) complaints, their resolution and communications from interested parties;
c) details of noncompliance and corrective and preventive actions;
d) results of reviews and audits of the compliance management system and actions taken.

10.1 Nonconformity, noncompliance and corrective action
10.1.1 General
When a nonconformity and/or noncompliance occurs, the organization should:
a) react to the nonconformity and/or noncompliance and, as applicable:
— take action to control and correct it; and/or
— manage the consequences;
b) evaluate the need for action to eliminate the root causes of the nonconformity and/or noncompliance, in order that it does not recur or occur elsewhere, by:
— reviewing the nonconformity and/or noncompliance;
— determining the causes of the nonconformity and/or noncompliance;
— determining if similar nonconformities and/or non compliances exist; or could potentially occur;
c) implement any action needed;
d) review the effectiveness of any corrective action taken;
e) make changes to the compliance management system, if necessary.

The failure to prevent or detect a one-off noncompliance does not necessarily mean that the compliance management system is not generally effective in preventing and detecting noncompliance.
Corrective actions should be appropriate to the effects of the nonconformities and/or non compliances encountered. The organization should retain documented information as evidence of:
— the nature of the nonconformities and/or non compliances and any subsequent actions taken;
— the results of any corrective action.
Information from analysing nonconformity and/or noncompliance can be used to consider:
— assessing product and service performance;
— improving and/or redesigning products and services;
— changing organizational practices and procedures;
— retraining employees;
— re-assessing the need to inform interested parties;
— providing early warning of potential noncompliance;
— redesigning or reviewing controls;
— enhancing notification and escalation steps (internal and external).

10.1.2 Escalation
A clear and timely escalation process should be adopted and communicated to ensure that all noncompliances are raised, reported and eventually escalated to relevant management, and that the compliance function is informed and able to support the escalation. Where appropriate, escalation should be to top management and the governing body, including relevant committees. The process should specify to whom, how and when issues are to be reported and the timelines for internal and external reporting.
When organizations are required by law to report noncompliance, regulatory authorities need to be informed in accordance with the applicable regulations or as otherwise agreed.
Even if organizations are not required by law to report noncompliance, they may consider voluntary self disclosure of noncompliance to regulatory authorities to mitigate the consequences of noncompliance. An effective compliance management system should include a mechanism for an organization’s employees and/or others to report suspected or actual misconduct or violations of the organization’s compliance obligations on a confidential basis and without fear of retaliation.

10.2 Continual improvement
The organization should seek to continually improve the suitability, adequacy and effectiveness of the compliance management system.

The information collected, analysed and evaluated accordingly, and included in compliance reports, should be used as basis to identify opportunities for improvement of compliance performance of the Organization.

7.4.1 General
The organization should determine the need for internal and external communications relevant to the compliance management system, including:
a) on what it will communicate;
b) when to communicate;
c) with whom to communicate;
d) how it will communicate.
NOTE Guidance on internal and external compliance reporting is given in 9.1.7 and 9.1.8.

7.4.2 Internal communication
The organization should adopt appropriate methods of communication to ensure that the compliance message is heard and understood by all employees on an ongoing basis. The communication should clearly set out the organization's expectation of employees and those non compliances that are expected to be escalated and under what circumstances and to whom.

7.4.3 External communication
A practical approach to external communication, targeting all interested parties, should be adopted in accordance with organization policy. Interested parties can include, but are not limited to, regulatory bodies, customers, contractors, suppliers, investors, emergency services, non-governmental organizations and neighbours. Methods of communication may include websites and email, press releases, advertisements and periodic newsletters, annual (or other periodic) reports, informal discussions, open days, focus groups, community dialogue, involvement in community events and telephone hotlines. These approaches can encourage understanding and acceptance of an organization's commitment to compliance.

# Conclusion

Compliance is hard. Getting your entire organization to understand, manage, implement and correct compliance issues on an ongoing basis is one of modern business' greatest challenges. Governments are regulating more and more, and consumers and partners are demanding higher standards every day. We hope this workbook and the resources below help you focus your compliance initiatives, identify the high-risk issues and implement a robust comprehensive compliance program.

Should you wish to obtain assistance in implementing your compliance program, please do not hesitate to contact us at info@nimonik.com

# Additional Resources

- ISO 19600 – Compliance Management System Guidelines
- Continuous compliance – Embed compliance throughout your operations
- The not so hidden costs of non-compliance
- The four key types of EHS regulations and how to comply
- Comprehensive compliance – Taming the compliance beast
- ISO 45001 (Health & Safety Management System) – Fundamentals and Requirements for Auditing and Legal Compliance
- Legal Compliance challenges in the Oil & Gas Industry
- ISO 14001 Fundamentals
- Taking the Stress out of Your Quality Management System
- Electronics Recycling: Operational Challenges, Solutions, Trends
- Mastering IATF 16949: 2016-The Universally Accepted Standard for Automotive Quality Management System
- Chinese EHS Trends: Improve your Organization's Operations in China

- Internal Audit Best Practices for Safety, Environment, and Quality Audits
- Rack Safety & Compliance
- Great ISO 14001 Legal Registers, What do They Look Like?
- The Link Between Risk Management, Critical Controls, and Auditing
- Lessons Learned in Mobile EHS Auditing