Internal Audit Best Practices for Environment, Safety, Risk, and Quality

Authored by:
John Wolfe & Jonathan Brun

Nimonik

Executive Summary

Internal Health, Safety, Environment, and Quality (HSEQ) Audit Programs can be improved with some of the following items:

1. A continually improving HSEQ management system framework that facilitates the identification of risks, opportunities, and supportive controls.
2. Supportive leadership that sees HSEQ performance excellence as one of the keys to overall corporate performance?
3. Efficient monitoring and self-assessment programs by front line and business unit risk and control owners with leading performance metrics that drive desired outcomes.
4. An independent internal audit function with budget, staff, and expertise commensurate with the nature and depth of HSEQ risk and control maturity.
5. Involvement of outside experts where credibility and expertise are required.
6. Good data analytics and automation.
7. Risk based audit program design that focuses on critical controls, and business processes.
8. Robust incident investigation and analysis of causes and gaps identified during the audit.
9. Reporting audit results to senior management and the board for full transparency.
10. Collaborative, continual improvement philosophy

Introduction

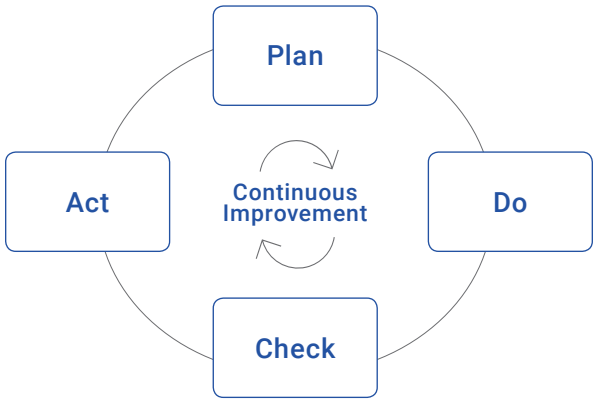
The design and focus of your internal audit (HSEQ) business process has a profound impact on your operations' safety culture and bottom line results.

This white paper explores the design and operational elements of an effective internal HSEQ audit program. The paper addresses the value that an Operations Excellence Management System framework, supportive culture, and operational discipline provide.

Key Attributes

What are the key attributes of a high performing internal audit program?

An Internal Audit Program is not effective in isolation. In well-run companies it is a critical component of the Plan-Do-Check-Act-Business improvement process and an essential element of the overall management system.



Plan-Do-Check-Act

As an example, the internal audit program at an Oil & Gas company mirrored the traditional financial internal audit program but looked at operational risks instead of financial risks. A traditional HSEQ group also existed and it managed over 400 HSEQ professionals embedded throughout global operations. In 2012, the company implemented an integrated Operations Excellence Management System that built off a clear and well-communicated set of long-term corporate strategies, policies, and values.

Operations Excellence Management System

This example of an Operations Excellence Management System (OEMS) has 18 management system elements to manage its HSEQ and process safety management programs.

Plan

1. Leadership & accountability
2. Risk Management
3. Legal Requirements & Commitments
4. Objectives, Targets and Planning
5. Management of Change

Do

6. Structure, Responsability & Ressources
7. Learning & Competence
8. Asset Life Cycle
9. Operations & Maintenance Controls
10. Contractor Management
11. Data Document & Information Management
12. Emergency Management
13. Communication & Stakeholder Management
14. Quality Assurance
15. Incident Management

Check

16. Audit & Assessments
17. Corrective Actions

Act

18. Management Review

18 elements

The actual number of elements is not particularly relevant since some can be combined. Almost all industrial organizations have 65 actual management system requirements that are integrated and interactive with data inputs and outputs flowing from one business process to another.

Audit and Assessment is one of the 18 elements in this exemple and is strongly linked to three other management system elements, which input data to and accept data from the Audit and Assessment element:

1. Legal Requirements & Commitments
2. Risk Management; and
3. Corrective Actions

Legal and Other Requirements*

The minimum expectation for any operationally excellent organization is to meet or exceed (where it makes business sense) all of its compliance obligations/requirements in the jurisdictions in which it operates.

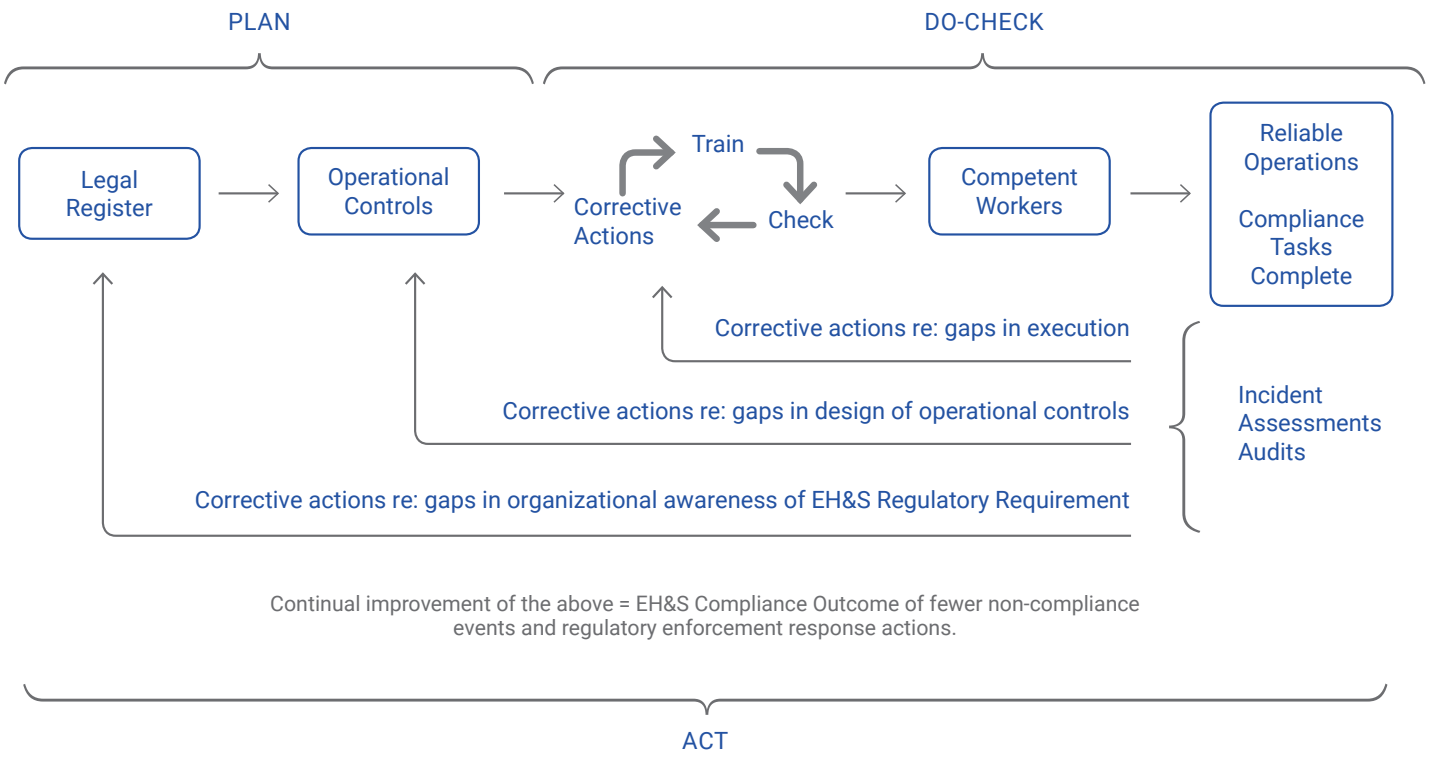
The journey to meet your Compliance Obligations involves research and the creation of information on the obligation. The information should be documented in a live “Obligations Registry” database and should include:

1. How, why, and where the obligation applies in the organization
2. What controls/evidence (tasks such as monitoring and reporting) exist that demonstrate the organization is meeting the obligation
3. Who owns the compliance requirement
4. Gaps, closure plans, etc.

A business process should also be in place to monitor any emerging regulations or changes to existing requirements.

The outputs of the monitoring and measuring business processes should provide adequate evidence of compliance if properly designed.

Means to control and mitigate obligation gaps and high consequence regulations should be identified and included as an input to the risk-based audit selection process and then audited as required. A proper management system ensures each operation identifies its HSEQ compliance obligations, documents them in a central location, and keeps the organization up-to-date on any changes in the identified regulations as well as corresponding changes to audit protocols.



Regulatory Compliance Obligation Management

** Note: For the remainder of this paper, we refer to Legal and Other Requirements as Compliance Obligations, the terminology used in ISO 14001:2015*

Compliance Assurance Metrics

Compliance Assurance Metrics should also be established to measure progress toward the following desired outcomes:

METRIC	EVIDENCE
1. Increase in knowledge and understanding of regulatory requirements	a. Accessible Compliance Obligations b. Documentation of Operational Controls
2. Appropriate actions on new regulatory requirements	Flagging significant new requirements
3. Effective regulatory operational controls to measure the 'Check' component of the Plan-Do-Check-Act system	a. Scheduling reviews to continually improve operational controls b. Completion of incident reviews, investigation and identification of root causes of high-risk incidents
4. Reduction in regulatory enforcement response actions and investigations	Improvement in compliance outcomes
5. Effective regulatory compliance elements of the management system	Effective overall compliance assurance performance business process (based on Key Performance Indicators, Operations Integrity Audit spot checks, etc.)

Risk Management Approach

Risk Management is the next management system element with key interdependencies to Internal Audit. Risk management is perhaps the most important element because if you get it right, management stands a better chance at allocating its scarce resources against the correct risks and opportunities.

Unfortunately, it is also one of the hardest element to implement effectively. Many companies have major incidents that have had a devastating impact on their bottom line, reputation, and morale because of weaknesses in risk management systems.

In some of these cases, well-run organizations had an unfortunate series of time-sensitive events which lined up and led to disaster. In other cases, a clear ticking time bomb could be seen: poor safety leadership and culture, lack of operational discipline, and high-risk tolerance in high-risk environments. Both of these situations can be avoided with a proper risk management strategy and supporting “Check” processes such as Internal Audit.

To Audit Is to Change

As an internal auditor you are a powerful agent of change. There is perhaps no other role in the organization that can affect behaviour at multiple levels simply by presenting the facts on critical risks and the way they are being managed - or not. Once a risk is identified, and the control weakness is clear, and well communicated, management becomes accountable, and they can decide on a path forward based on their risk appetite, tolerance, and available resources.

Denormalize Risk

Even today, most companies big and small, do not have a clear, coherent, live and documented picture of their operational risks and associated control efficacy. Many leaders Nimonik works with were not aware of significant risks they lived with daily, or were aware but had lived with the risks so long they had normalized them. All of us can have a hard time changing our perspective and taking a step back. Too many leaders normalize their operational risks, no longer seeing the danger that outsiders can see much more clearly.

Even worse, Nimonik often found evidence in many organizations that these risks had been identified at some point in the past and then were either “lost” in an uncontrolled study, or spreadsheet, or “hidden” due to perverse incentives around risk transparency. In other cases, the risks were transparent but not professionally managed with risk prioritization. In yet other cases, the organization’s business planning process did not facilitate interim risk management activity for those risks that required scarce capital and had to wait for budgeting and business planning cycles.

In all these situations, the organization exposes itself to significant legal and fiscal liability, because it could be proven that the organization was aware of the risk, but had not taken the appropriate steps to manage the risk.

Risk Registries

Operationally excellent companies develop facility-level risk and control inventories. In larger companies these facility registries are combined with the operations level risk registries. This helps identify more significant level risks and controls that require significant operating or capital expenditures.

In very large companies, these operations-level risk registries are then further refined to a list of about a dozen risks that the executive team and Board monitor on an ongoing basis. These **Principal Risks** and the **Operations Level Risk Registries** are the second critical input into what your internal audit program should consider when selecting audit targets in any given year.

Risk Register Hierarchy

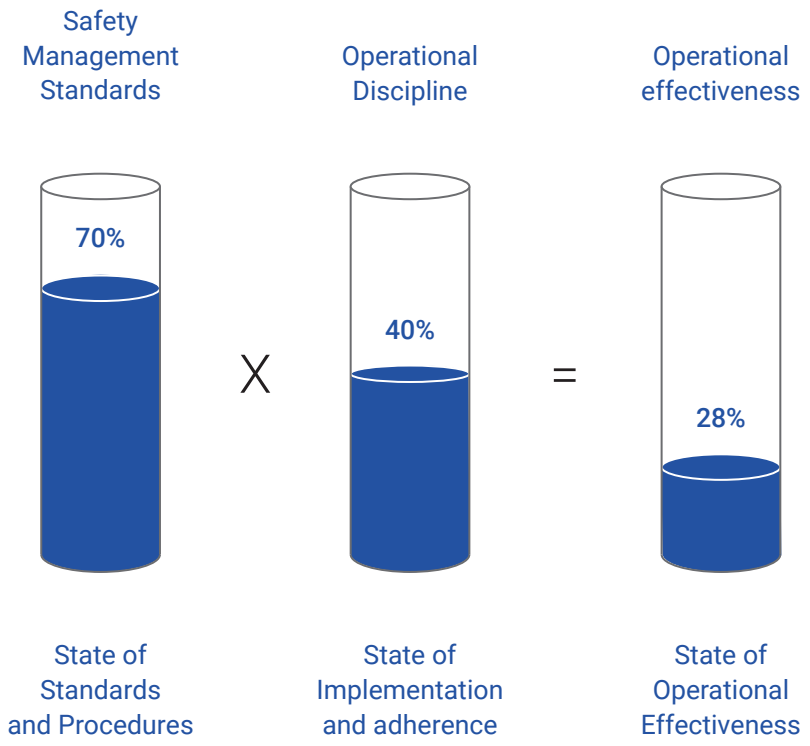
To normalize and prioritize risks, risk registers should be developed using the appropriate risk identification techniques and a common evaluation grid. Inherent and residual risk ratings should be included with:

1. Relevant control hierarchy data
2. Applicability
3. Ownership information to facilitate the identification of auditable critical controls
4. Gap closure and mitigation plans, and the whole process subject to management of change

This process reduces the chance of orphan risks with no clear owner, allows for the assessment of the adequacy of controls, aggregation of risk across operations and risk transparency to senior management. The inventory should be kept current through your management of change process. Having now identified and prioritized risks and critical controls, it is also logical that said operational controls must be followed if the risks are to be managed effectively.

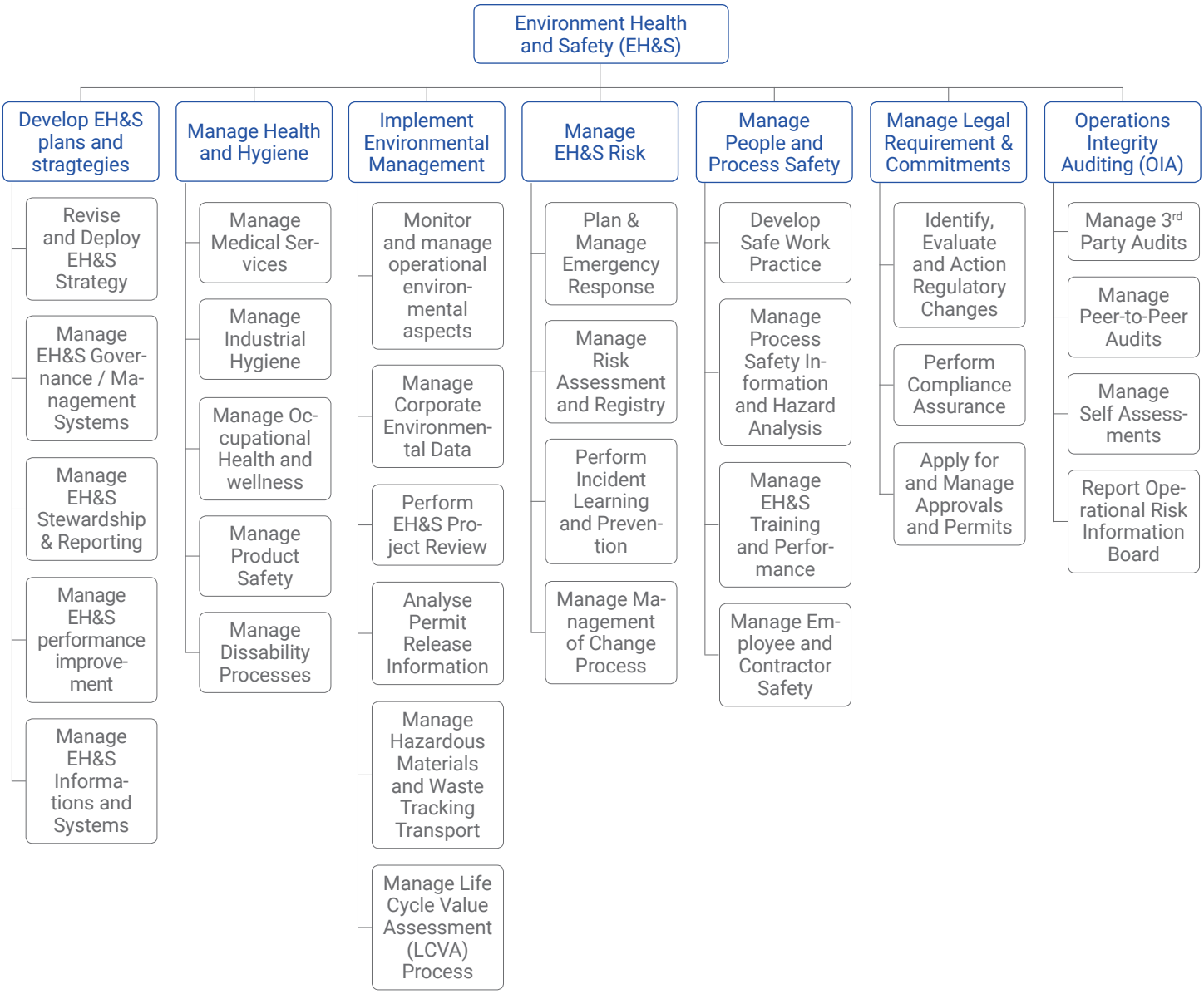
The diagram below illustrates how operational excellence is the product of both a structured controls program and operational discipline in following them.

This data is critical to a collaborative discussion with operations leadership. You can ask what risks and critical controls have good monitoring and metrics programs? Which are being assessed by the risk and control owner? And which will be audited by Internal Audit?



Standards and Discipline

High performing companies go one step further and map out their core business processes. On the next page are the businesses processes for the HSEQ function which were also potential audit targets, depending on their criticality and whether the process was identified as a root cause failure in incidents.



Environment Health and Safety (EH&S)

Location and Role of Audit Functions

Where do audits fit in amongst other governance functions?

Are more internal audits the answer? In addition to their day jobs, front line managers must manage many diverse governance initiatives ranging from corporate initiatives coming from HQ HSEQ and Operational Excellence groups, which increase in number over time. They are also subjected to other types of audits such as:

- Board-mandated audits
- Industry organization audits (API, AFPM, ACC in the U.S. or equivalents elsewhere)
- Constantly changing regulatory requirements
- Local, state/provincial and federal audits
- Insurance underwriter audits

How do audits add value?

Although each of the above mentioned audits may add value individually, add them up and it is no wonder that facility leadership teams are distracted from systematically identifying, prioritizing, then aggressively mitigating their HSEQ Risks through “critical” controls implementation. It is also no surprise that industry associations are reporting increases in incidents despite all the efforts to prevent them. That said, routine auditing and assessment is an essential element in the operation of any business concerned about operational excellence.

At your company, perhaps you audit for properly maintained equipment or facilities. Maybe you concentrate on HSEQ Management Systems or operating procedures or unsafe behaviours. However, if you are the only one doing audits/assessments and you are not using a risk-based approach to audit target selection or tracking the necessary corrective actions to completion with a through effectiveness assessments - are you really getting the most out of what the audit and assessment business process should be providing?

The Internal Audit function should be part of a structured governance program that builds off the front line and facility management assessment of the efficacy of their own risks and controls. This should be done through effective self-assessment and monitoring programs with performance metrics that build off leading versus lagging indicators. You should look at the effectiveness of the audit program vs. say the number of completed audits.

In short, you and your Internal Audit team should not be the only and last line of defence, you should be checking the checkers (management system audits). The path to great internal audits is to audit the efficacy of the HSEQ management system itself and associated critical controls, the high consequence compliance obligations, and the efficacy of important corrective and preventive actions.

Internal Audit Role

What would an ideal world look like and what role does the internal audit function play?

Ideally, top leadership and Boards would demand effective governance of all significant Operational/HSEQ issues, but too often top leadership is rewarded for the wrong things such as an over-riding focus on maximizing short-term returns, and in many cases, the Boards themselves lack the background or competency to provide effective oversight.

What are the hallmarks of companies that get it right – those that are operationally excellent?

First, they have top management that is committed to a safety first culture. They understand that if the company safety culture and its business processes continually improve, so will their business performance. If top management doesn't make HSEQ excellence a priority, neither will the employees.

Great management understands the value in hiring facility managers who are also good leaders, adept at getting their organizations to adapt to and follow a HSEQ Management System framework, culture, and discipline that promotes operational excellence.

In most companies the Internal Audit HSEQ function usually reports through to a senior leader in operations or HSEQ. Where and who you report to is not as important if you have the right corporate culture. Where audits and assessments are a critical component of continual improvement, you must determine if the organization has a collaborative or confrontational and positive or punitive actions.

Any well-designed program should have an experienced professional auditor leading the team. The person must have enough technical and operations experience to converse professionally with his or her clients and understand the risk environment in which they must audit.

What does an ideal internal auditor look like?

The leader should be supported by a small team of trained auditors that draws professionals from operations into the audit function and then back out to operations on a two or three-year cycle. In addition to their technical skills, these individuals should be trained to

- Observe (people and facilities)
- Interview and listen
- Analyze data, draw conclusions and make recommendations
- Communicate (in writing and orally)
- Identify root causes
- Maintain independence and objectivity

External professionals (technical expertise) should be utilized where internal competency cannot be made available.

What to Audit

How do you know what the Internal Audit Function should be auditing?

There is never any shortage of audit targets. The trick is to have operations self-identify their risks and establish controls to a nature and depth commensurate with the potential risk consequences. Operations should also develop performance metrics which monitor the effectiveness of the controls on an ongoing basis avoiding the need for regular audits.

Are self-assessments helpful?

Best-in-class companies develop self-assessment programs that monitor their management system framework and critical controls for systemic weakness and best practices that can be shared. This ongoing assessment of the management system framework is foundational to continual improvement since well-managed incident investigation business processes usually identify the failure of one or more management system elements as the true root cause of most incidents.

How to set audit priorities?

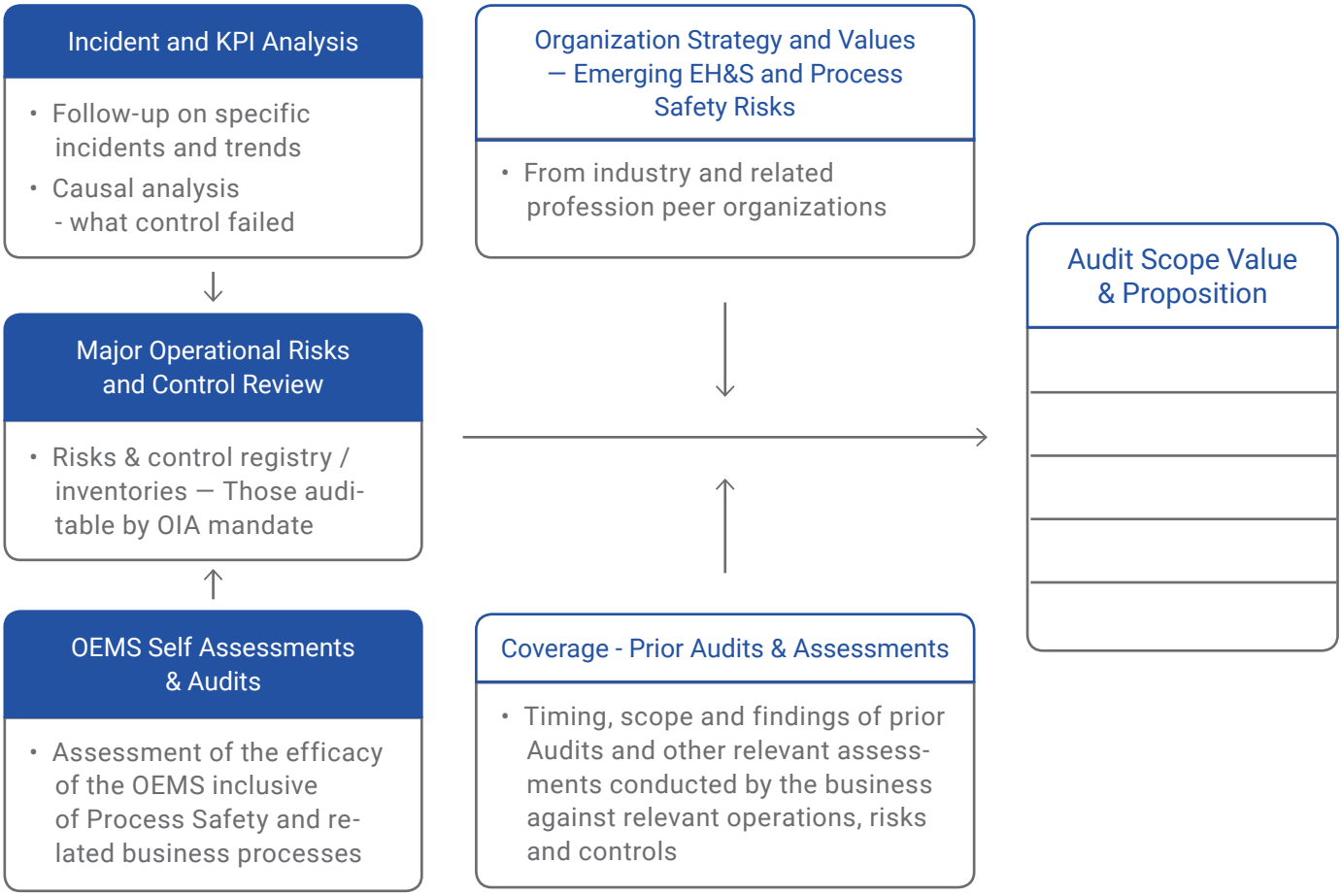
Failure to identify critical controls can also manifest itself through the classic case of “too many priorities mean you have no priorities.” Front line managers need to focus their attention on the effectiveness of the controls that have the potential to really hurt the company if they fail.

In the absence of a robust analysis, organizations focus too many resources, including management attention, on HSEQ personal safety issues such as slips, trips and falls versus operational discipline around or the adequacy of critical process safety risk and controls that can impact greater numbers of employees, contractors and the public.

In our experience the most effective internal audit programs are risk-based and have a series of data inputs which include the following:

- Incident Analysis – across the company and the industry
- Major Operations Risks and Associated Critical Control Analysis
- Management System Self Assessments and Audit
- Organization Strategy and Emerging/Industry Issues
- Auditable Unit risk rating – based on operations risk and complexity profile, duration since the last audit, and perceived management strength and weakness based on performance

Internal audit should avoid duplication of effort and focus on those areas that add the most value through an analysis of existing governance programs.



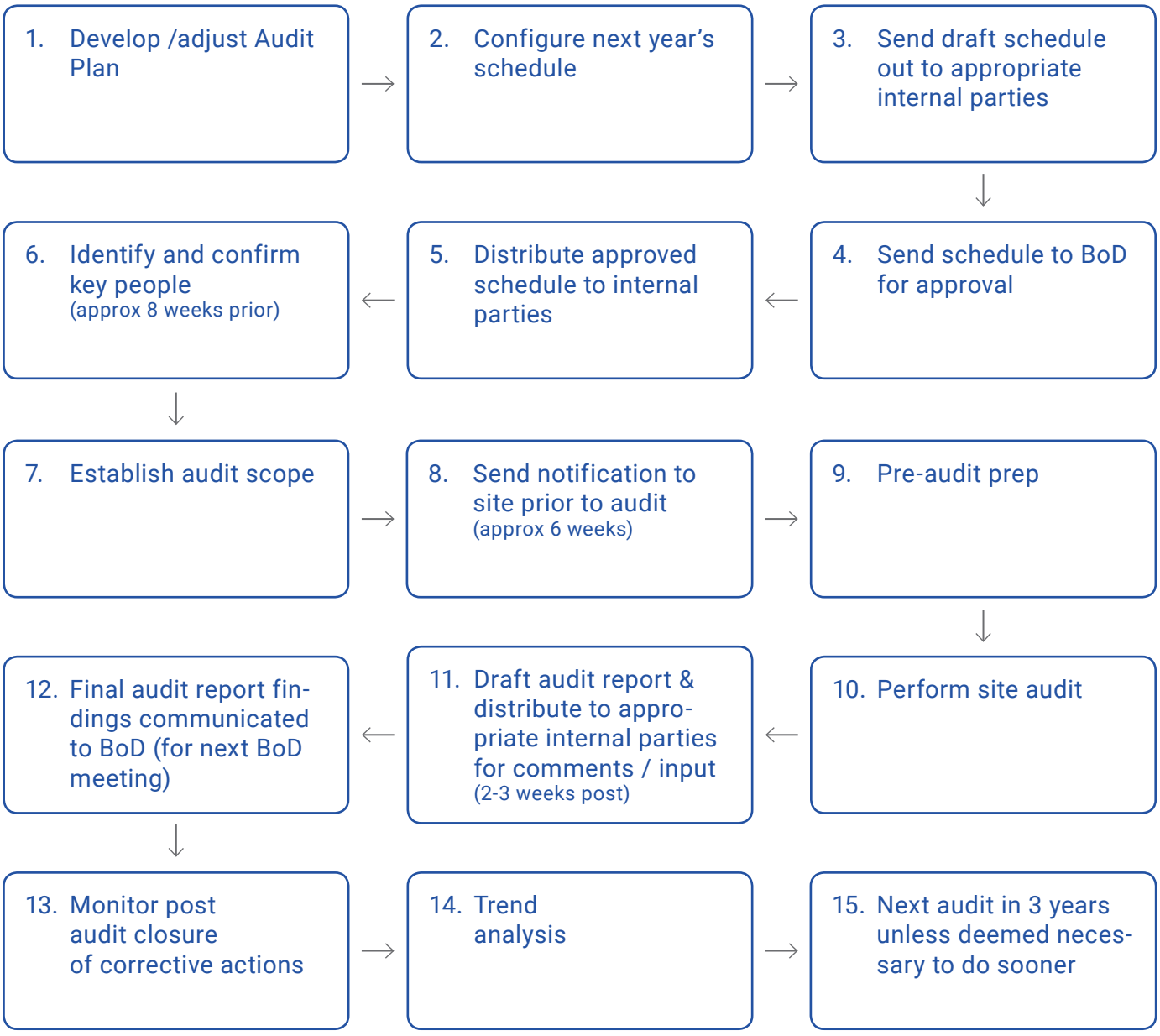
Analysing Performance

What is the ideal frequency and scope of audit?

The major Oil & Gas company discussed previoulsy developed a seven-year risk based audit program cycle that covered over 50 auditable operations around the world on a three to five-year cycle. Higher risk units with hazardous process safety operations, environmentally sensitive locale, or high incident frequency, low self-assessment ratings were covered on a three-year cycle and lower risk operations on a five-year cycle.

At a minimum, these audits covered critical management system elements and usually included a deep dive on specific risks and controls or business processes in one or more facilities in the unit. The audit team size and makeup and duration of the audit were commensurate with the complexity of the audit criteria/controls involved.

A typical audit schedule/business process that outlines the steps taken to plan, conduct an audit and follow-up on its findings is illustrated in the following figure;



Audit Scheduling

Some Frequently Asked Questions

Should you provide an outline of what criteria you will be using to audit?

It is generally desirable to provide as much information on the scope of what you will be auditing and the criteria you will be using as possible. In the case of regulatory compliance, or management system audits, the criteria are generally well defined. If the organization has mature operating controls, criteria can also be easily developed. Where a risk has been identified, and controls are immature, the audit may be a bit of a fishing expedition to determine what controls are being utilized.

In most audits, the lead auditor should also request information be sent to the Audit Team as background and familiarization prior to the Audit. Suggested items include:

- A process overview
- Facility layout (map or diagram)
- Block flow diagram for the unit
- A list of the hazardous materials handled in the area with a brief description of hazards (including raws, intermediates, waste streams, and final products, as applicable, especially if the audit covers process safety requirements)
- A simplified organization chart for the area leadership, showing names of key personnel who will be participating in the Audit or who have key technical or leadership roles involving the administration of one or more HSEQ elements
- Site/area relevant HSEQ guidelines and procedures
- A copy of the most recent second party HSEQ Audit and status of recommendations (corrective action plan)

This information will allow for more effective audit planning and interview scheduling, which should be completed several weeks before the actual audit.

This pre-audit effective audit communication theme should be continued throughout the audit itself, with daily debriefings on potential findings to ensure their defensibility, and to allow the organization to direct you to any missing data. You want no surprises, or push back at the exit and closing meeting(s) where you are presenting the findings to the senior leaders.

During the audit the lead auditor should ensure his or her team is honest, straightforward, tactful, courteous, and to the extent possible works standard site hours. The audit team should:

- Deliver on commitments
- Be punctual for all appointments
- Come to the Audit prepared
- Be interested and enthusiastic
- Never underestimate the significance and impact of their recommendations
- Wear proper personal protective equipment and follow the local safety rules
- Not be afraid to admit if they don't know something, and ask for clarification when needed, validating all potential findings with the lead auditor before communicating them to the site

Can software help leaders reduce cost and risk?

Tools such as NimonikApp can make the identification of compliance obligations easier by creating operations specific “Compliance Obligations” registers that capture legal and other commitments the organization may have made in permit or license obligations as well as commitments to third parties. These tools also aid in the management and documentation of compliance through their tasking tools.

Top performing companies also ensure normalization of risk data, through proper training and facilitate hazard and risk reviews that enable them to “roll up” the Operational/HSEQ Risks within each business on a consistent basis to identify aggregate risk and create a live picture of their entire risk and control universe.

Software tools are also available to facilitate this process and the best software has algorithms that help predict potential future incidents by identifying trends and deviation from steady state even before alarms are tripped.

For small and medium sized business, perhaps the most useful application are tools to facilitate the conduct of inspection and observation programs such as house-keeping, or adherence to life saving rules and procedures around hazards such as confined space entry, personal protective equipment, energized sources, etc. Many tools allow managers to use their phone or tablet to input data in the field with easy and flexible input forms.

Conclusion

A great internal auditing program is an investment and while the benefits of the investment are often not clearly visible, one avoided incident or product recall can pay for the entire program. There is no magic bullet, but all companies should conduct regular internal HSEQ audits based on their risks and activities.

For small and medium businesses, the process described above can seem burdensome. It should be noted however that the same principles can be applied to any organization and should be modulated to be fit for the purpose based on the complexity and resources of the organization. All organizations have risks. By conducting some key assessments and conducting regular audits to identify improvement opportunities, your organization will only become stronger - no matter its size.

To learn more about Internal Audit Best Practices and discover how they can be implemented as efficiently as possible, contact Nimonik at 1-888-608-7511 or at info@nimonik.com

About Nimonik

Nimonik believes every company can be safe, green and produce high-quality products. Nimonik, established in 2008, helps companies achieve their HSEQ and Quality goals with beautiful web and mobile software. Nimonik works with businesses in over 20 countries and helps environmental, health and safety and quality managers improve their operational excellence on a daily basis.

Find out more at http://nimonik.com

About Authors

John Wolfe

John Wolfe is a Partner at Nimonik inc. He has over 25 years of experience in the design, implementation and assessment of integrated HSEQ management systems in multiple industry sectors. He has held HSEQ leadership positions in Suncor Energy, IFC Kaiser, Boart Longyear, CSA and has successfully launched a number of companies, Management Horizons, Green Cone, Total Environment Solutions Trinidad, and Conformance Check. Most recently he was the Sr Director of Operations Integrity Audit at Suncor. John is also well known as an early leader in the sustainability field having managed the ISO Technical Committees that developed the ISO 9000 and 14000 series of standards and guidelines for corporate reporting, stakeholder consultation and environmental labelling. He was also a founding member of the Canadian Environmental Auditors Association.

Jonathan Brun

Jonathan Brun is the founder and president of Nimonik inc. An engineer by training, he has worked with businesses around the world and in nearly every industry to help them ensure they respect HSEQ regulations and Quality standards. Jonathan is passionate about technology, automation and making every operation safe, low risk and as efficient as possible. He can be reached at jbrun@nimonik.com or at +1-514-712-0637.