RISK-BASED AUDITING

Designing a world class risk-based regulatory monitoring and management system.

By Peter Mills, Chief Executive Officer,
Compliance Master

This article describes how world-best-practice acceptance sampling methods (ISO 2859.1) can be used to create a highly effective and efficient risk-based regulatory compliance monitoring and management system.

JANUARY 2015

Risk-based Regulation

In today's competitive business environment Regulators are being called upon to be more accountable for their performance while reducing their costs and the burden they place on businesses and the community at the same time.

In response to these growing demands the Australian National Audit Office (ANAO) published its Better Practice Guide: Administering Regulation in June 2014. Its main purpose is to help Regulators improve their performance by adopting a risk-based approach to the monitoring and management of Regulated Entities.

> *A key component of any regulatory regime is monitoring compliance with regulatory requirements and managing non-compliance. A risk-based approach to these activities assists a regulator in addressing the most serious risks, patterns of systemic non-compliance and effectively allocating its resources while avoiding imposing unnecessary costs on regulated entities.*
>
> *ANAO Better Practice Guide, Administering Regulation, p.7*

Acceptance Sampling

Acceptance sampling is a proven risk-based auditing methodology used widely throughout the manufacturing sector to assess whether large quantities of continuously produced products or materials have exceeded a maximum non-compliance limit.

What is not so widely appreciated is these same methods can also be used to monitor and control other types of risks; i.e. safety, environment, finance, fraud, regulatory noncompliance, etc.

There are many types of acceptance sampling but the "sampling by attributes" methods outlined in the International Standard ISO 2859.1 [1] are arguably the most popular and easiest to understand.

One of the Standard's more beneficial features is its ability to calculate the optimum sample-size for each audit by taking into account among other things, the prior compliance performance of the process or entity being assessed. In other words, the better their performance, the smaller their required sample-size.

This dynamic, risk-based approach to auditing is far more efficient than static methods and is achieved by "switching" a process or entity between three levels of audit severity (i.e. Normal, Reduced and Tightened) based on their capacity to meet, or do better than, specified non-compliance limits over prior audits. [2]

An entity's audit severity rating can also be used to quickly assess and benchmark their compliance performance and to standardise an organisation's response to observed non-compliances; refer to Defining Action Protocols in the following section.

How it Works for Regulators

This section describes how a risk-based regulatory monitoring and management system based on ISO 2859.1 acceptance sampling methods can be used by Regulators to effectively and efficiently monitor and manage the safety performance of Regulated Entities. This same approach can be used to monitor and manage other types of regulatory risks; e.g. environment, fraud, security, quality, etc.

[1] ISO 2859-1:1999 Sampling procedures for inspection by attributes – Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection. Duplicate versions of these methods are published by Standard Bodies worldwide; e.g. AS1199.1

[2] Switching rules and procedures ISO 2859.1. 1999, Section 9.3

1. Defining Compliance Measures

The Regulator informs Regulated Entities of their obligations under the relevant Act and the auditing methodology (ISO 2859.1) that will be used to monitor their performance against industry defined safety requirements and performance targets.

Regulated Entities and stakeholders are consulted to develop a list of Items to be audited together with their safety requirements. Each requirement is then assigned a risk category depending on its contribution towards achieving defined safety outcomes; (i.e. High, Medium and Low).

2. Defining Performance Benchmarks

Each risk category is assigned a maximum non-compliance limit (risk appetite) based on historic compliance performance data; i.e. The High risk category is assigned a smaller acceptable non-compliance limit than the Medium risk category, which in turn is assigned a smaller limit than the Low risk category.

3. Defining Action Protocols

Standard protocols are developed for each possible ISO 2859.1 audit outcome;

Possible ISO 1859.1 Audit Outcomes	Action Protocols (Examples)
1. Non-compliance limit exceeded	Suspend Entity, undertake 100% inspection and correction
2. Non-compliance limits not exceeded	No action
3. Severity switched Normal-to-Tightened	Increase audit frequency 12 to 6 months
4. Severity switched Normal-to-Reduced	Reduce audit frequency 12 to 24 months
5. Severity switched Tightened-to-Normal	Reduce audit frequency 24 to 12 months
6. Severity switched Reduced-to-Normal	Increase audit frequency 6 to 12 months

4. Defining Audit Frequency

The Regulated Entity's audit frequency is determined by referencing its current audit severity rating; i.e. Normal, Tightened or Reduced. In other words, the better its compliance performance the less frequently it's audited.

5. Registering Regulated Entities

When registering Regulated Entities onto the system for the first time those with an acceptable track-record are assigned a "Normal" severity rating, while those with an unacceptable or unknown track-record are assigned a "Tightened" severity rating. If necessary, the Standard will recommend a change to an entity's initial severity rating when analysing future audit results.

6. Determining Sample Sizes

The total number of items (products / activities) to be assessed by an audit (audit population) is estimated by the Regulator and used in conjunction with the tables in the Standard to determine the optimum sample-size.

7. Collecting Audit Data

Items are randomly selected from the Regulated Entity's audit population for inspection. Each item is tested for compliance against its specified safety requirements. Any non-compliances are recorded against the associated safety requirement and its risk-category. The audit is concluded once the required sample-size is achieved for each risk-category.

8. Analysing Results

At the completion of the audit the total number of non-compliances identified for each risk-category is summated and used in conjunction with the tables in the Standard to determine whether its specified non-compliance limit has been exceed; or not.

The "switching" rules are then applied to the Regulated Entity's recent audit results to determine whether its severity rating should be changed.

9. Managing Outcomes

The protocols associated with each audit outcome are implemented. Possible protocols might include i) penalising the responsible entity for exceeding one or more risk-category non-compliance limits ii) cancelling their registration until they identify and correct the root-cause of the identified non-compliances, iii) reducing or increasing their audit frequency, etc.

10. Communicating Outcomes

Non-compliance information is forwarded to the responsible Regulated Entity for correction and continuous improvement and if required, to other government agencies, for consumer protection or taxation purposes, etc.

Key Benefits

The ANAO Better Practice Guide lists a series of key considerations to assist senior regulatory managers when reviewing the effectiveness of their agency's regulatory administration processes and to guide future practice. A number of the more important relevant considerations are used below to highlight the benefits of a regulatory monitoring and management system based on ISO 2859.1 methods.

i. Timeliness: The auditing methods outlined in the Standard are specifically designed to support continuous auditing and inspection. Accordingly, they are ideally suited to identifying unacceptable regulatory performance before something serious happens.

ii. Risk Focused: The Standard's "switching" functionality automatically focuses a Regulator's limited resources on its areas of highest risk by separating regulatory requirements into different risk-categories with individual compliance targets.

iii. Residual Risk: The Standard's ability to reliably assess whether one or more risk-category non-compliance limits have been exceeded provides Regulators and other Stakeholders confidence that residual risks are being managed within defined levels.

iv. Flexible Intensity: The Standard's ability to "switch" Regulated Entities between three levels of audit intensity ensures good performers are rewarded with reduced auditing intensity; i.e. smaller sample-sizes. This can also lead to substantial reductions in auditing costs over time.

v. Flexible Monitoring Frequency: The Standard's "switching" feature can also be used to align a Regulated Entity's auditing frequency with their previous compliance performance. In other words, the better their performance the larger the period between audits.

vi. Proportionate Response: The Standard's ability to link a Regulator's response to a series of possible audit outcomes ensures a Regulator's response to observed non-compliances is consistent and proportionate to the associated risk.

vii. Transparent: The Standard provides Regulators a highly transparent and objective method of assessing a Regulated Entity's compliance performance and for supporting important management decisions; e.g. imposing penalties and sanctions, publishing and reporting information, etc.

Conclusion

A risk-based auditing system based on ISO 2859.1 acceptance-sampling methods has a number of major advantages over conventional non-scientific auditing solutions; especially when it comes to monitoring and managing regulatory compliance performance.

Not only will it significantly reduce the amount of time and money needed to continuously monitor the compliance performance of Regulated entities, it also provides the consistency and transparency needed to manage their performance through a series of standard and proportionate responses to audit results. This also leads to greatly improved reporting to key Stakeholders.

An ISO 2859.1 based auditing system can also help Regulators and Regulated Entities understand the nature and extent of observed non-compliances and regulatory performance and the resulting impact on risk levels, how similar breaches can be avoided in the future, and how further breaches could lead to more severe enforcement action.

Once only the province of large manufacturing companies with highly centralised production processes recent advancements in cloud-based software and technology have made it possible for Regulators in every sector of government to benefit from this highly effective and efficient approach to risk-based compliance monitoring and control.

For further information on how your organisation can take advantage of the very latest in acceptance sampling technology please visit www.compliance-master.com.

PETER MILLS is the founder and Chief Executive Officer of Compliance Master International Pty Ltd. He has extensive experience as a senior business manager and consultant in the Australian electricity, gas, telecommunication and ICT sectors. Peter obtained his BEE from Footscray Institute of Technology and Grad Dip BA from Swinburne Institute of Technology.

COMPLIANCE MASTER™

Compliance Master International provides smart, risk-based compliance auditing and inspection solutions to organisations worldwide. The company is headquartered in Melbourne, Vic, Australia.