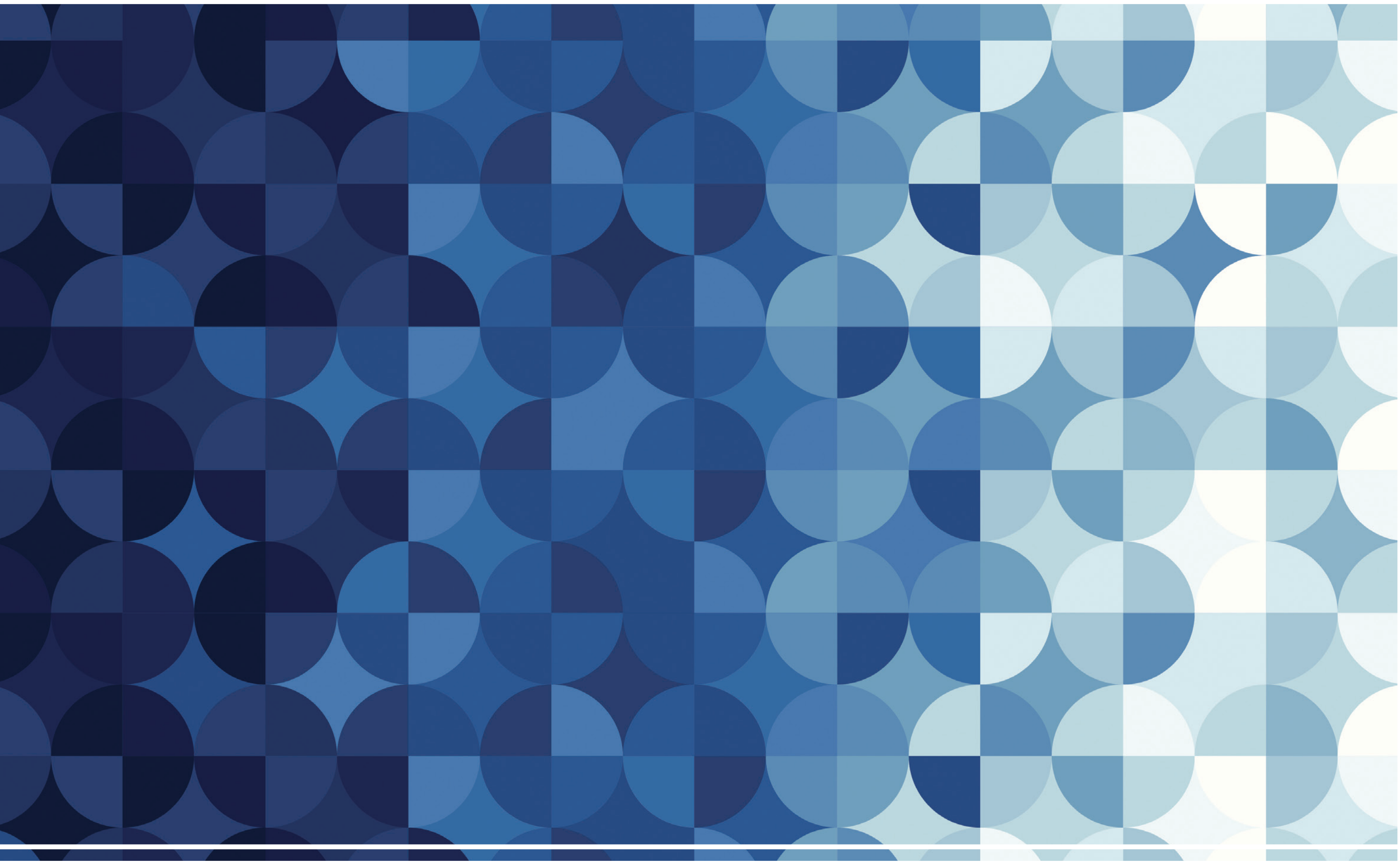
SAFER, SMARTER, GREENER

DNV·GL



BUSINESS ASSURANCE

THE NEW ISO 9001 & ISO 14001 REQUIREMENTS

6.1 - Actions to address risks and opportunities

VIEWPOINT ESPRESSO 3/2015

DEAR READER,

ISO (International Organization for Standardization) has recently released both standards: ISO 9001:2015 and ISO 14001:2015.

As ISO is moving to improve how their standards support companies in building sustainable business performance, the big question for certified companies and organisations seems to be how they will meet the new requirements.

This is the third release of our Viewpoint Espresso Survey. While the first two focused on requirements 4.1 “Understanding the organisation and its context” and 4.2 “Understanding the needs and expectations of interested parties”, this issue investigates clause 6.1 “Actions to address risks and opportunities”.

For the quality management system, this is largely a new requirement for certified companies. When it comes to the environmental management system, the requirements in 6.1 were to a large extent already present in the 2004-version. Some of the changes relevant for ISO 14001 are outlined at the end of this report. But for this reason, this Espresso Survey has polled companies certified to ISO 9001 only.

How compliant do companies certified to ISO 9001 think they are and what actions do they intend to implement in order to satisfy the requirement? We see that 11% of the companies responding find that they are compliant, while those evaluating themselves to be somewhat compliant account for 38%.

What is behind these numbers and how are these companies moving to close the gap? Are there significant differences between the three clauses? For a quick insight, turn the page to see what we found.

FACT BOX

THE VIEWPOINT ESPRESSO

- The Viewpoint Espresso is our way of sharing with you what your peers think and how they are moving on hot topics. Our hopes are that what we share may trigger some curiosity, improved understanding and possibly action on select topics.

- This is an extended initiative of ViewPoint, our customer community. While the main ViewPoint surveys provide in-depth analyses, the ViewPoint Espresso are meant to be more agile, providing a concentrated injection of insight.

THE REQUIREMENT IN FOCUS

6.1 - ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES

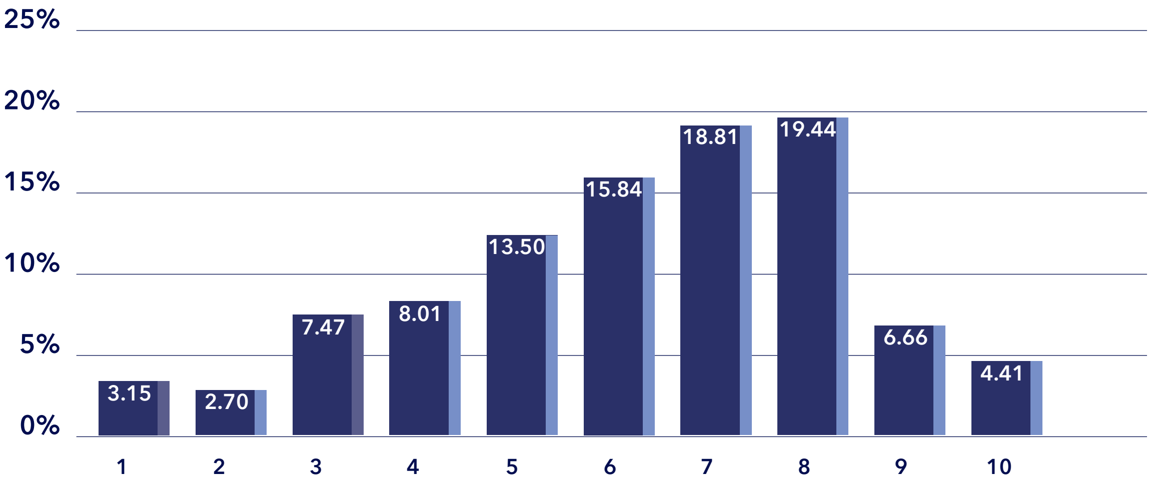
This clause requires that you determine the risks and opportunities that need to be addressed in order to:

a) give assurance that the management system can achieve its intended result(s);
b) enhance desirable effects;
c) prevent or reduce undesired effects;
d) achieve continual improvement.

Note that this survey has been addressed to ISO 9001 certified companies only. The requirement is also included in ISO 14001, but in the environmental standard this is to a large degree already a requirement in the previous version (2004). For the quality management system standard this is more strongly inserted as a new requirement.

ARE COMPANIES ALREADY COMPLIANT WITH 6.1 ?

? ON A SCALE 1 TO 10, WHERE 1 IS "NOT COMPLIANT AT ALL" AND 10 IS "FULLY COMPLIANT", TO WHAT EXTENT DO YOU CONSIDER YOUR ORGANISATION ALREADY COMPLIANT WITH SUCH A REQUIREMENT?



WHAT ARE THEY SAYING AND WHAT DO WE THINK?

- 11.1% say they are fully compliant (scores 9 to 10). This is lower than for the previous two clauses surveyed where approximately 14% indicated compliance.

- 38.3% consider themselves somewhat compliant (scores 7 to 8) compared to numbers in the range of 43% in the two previous surveys.

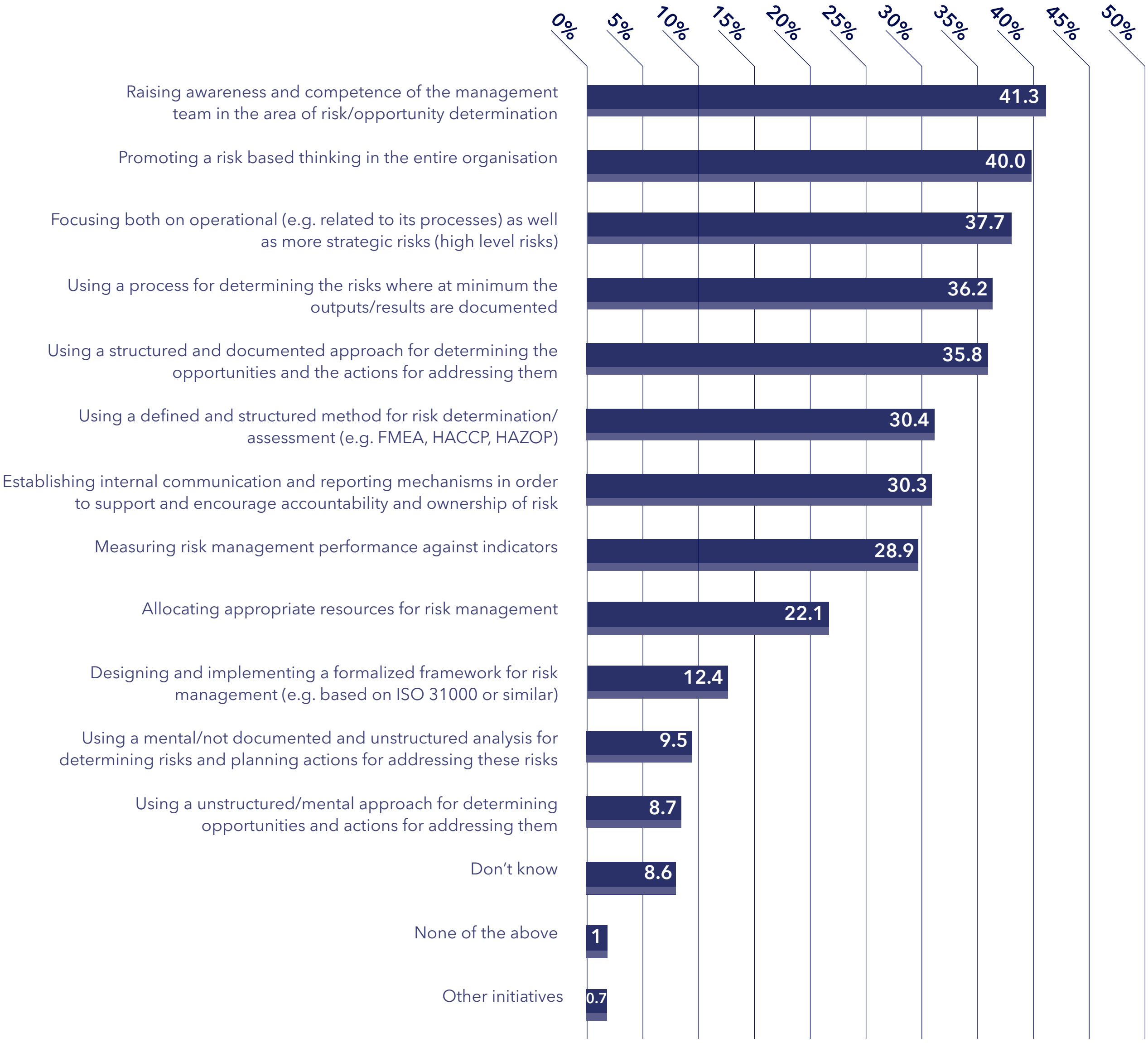
- 21.3% indicate that they are not compliant (scores 1 to 4). This is slightly higher compared to past surveys where companies indicating non-compliance were in the range of 17%.

The above indicate that clause 6.1 is considered more challenging. To satisfy requirements 4.1 and 4.2 common sense can go a long way. When it comes to applying a risk-based approach, more professional skills and insight are needed. Consequently, companies may feel less confident and consider themselves less prepared.

References to risks and opportunities (risk-based thinking) are included in several paragraphs in the standard. Thus risk-based thinking must be approached as an integrated part of the management system, making this requirement even more challenging. As such, to become compliant constitutes a significant move for companies. The expectation would therefore be that fewer companies would report that they feel compliant at this point in time.

HOW WILL COMPANIES MEET 6.1 IN THE FUTURE?

HOW DO YOU PLAN TO MEET THIS REQUIREMENT IN THE FUTURE? MARK THE APPROACH THAT YOUR ORGANISATION MOST LIKELY WILL BE IMPLEMENTING (MULTIPLE ANSWERS ARE ALLOWED).



WHAT ARE THEY SAYING AND WHAT DO WE THINK?

- Raising awareness and competence of the management team in the area of risk/opportunity determination is the action preferred by the highest number of respondents (41.3%). This makes good sense. If top management is committed and understand the importance of addressing risk and opportunity, consequent actions will follow easily.

- Promoting risk-based thinking in the entire organisation is a very close runner up (40%). This action is a natural follow-up after getting top management commitment. Companies where this is implemented clearly indicate that the risk management approach is pervasive of the entire organisation and not part of a few exercises or processes only.

- Focusing both on operational (process-related risks) as well as more strategic risks (high-level risks) was selected by 37.7% of the respondents. This underscores the view that risk-based thinking is not restricted to operational issues, which is well aligned with the intent of the standard.

The preferred actions indicate that companies should and will focus on both operational risks as well as strategic and high-level ones, thus working to integrate a risk-based approach in their management system.

We are pleased that unstructured approaches are selected by 8-9% of the respondents only. It seems to clearly indicate that companies do not consider an unstructured approach enough, a view we fully support.

Still there seems to be a way to go for companies to implement a truly structured and formalized risk management approach. Only 12% indicate that they will design and implement a formalized framework for risk management, e.g. based on ISO 31000 or similar standards. (See separate factbox on ISO 31000).

FACT BOX

A STRUCTURED APPROACH TO RISK MANAGEMENT

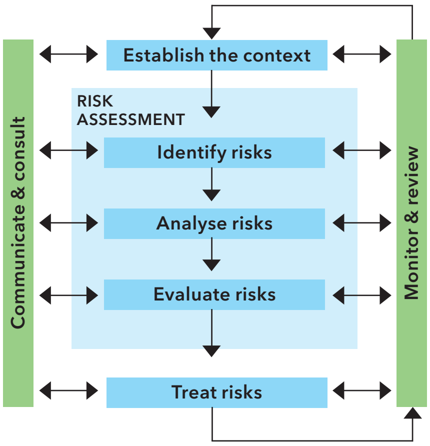
Organisations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organisation's objectives is risk (www.iso.org).

All activities of an organisation may involve risks. These may adversely impact organisations in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organisations to perform well in an environment full of uncertainty and build sustainable business performance.

ISO 31000:2009 – Risk management- principles and guidelines – provides a framework and a process for managing risk. It can be used by any organisation regardless of size, activity or sector. Using ISO 31000 can help organisations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk management.

ISO 31000 cannot be used for certification purposes but does provide guidance for internal or external audit programs. Organisations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance.

The key elements of a risk management process as defined by ISO 31000 are described in the picture below. The key elements are thoroughly explained in the guideline.



Reproduced from ISO 31000:2009

OTHER STANDARDS RELATED TO RISK MANAGEMENT

- ISO Guide 73:2009, Risk management - Vocabulary complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk.
- ISO/IEC 31010:2009, Risk management – Risk assessment techniques focused on risk assessment.

FINAL THOUGHTS ON ISO 9001

In basic terms, clause 6.1 of ISO 9001:2015 requires the organisation to determine and understand the range of risks and opportunities relevant to the scope of the organization and determine actions, objectives and plans to address them.

The strength of this clause lies in connecting risk and opportunity both to the organisation's processes (defined under 4.4) as well as to internal and external influencing factors (4.1) and needs and expectations from interested parties (4.2). We also believe that the inclusion of opportunities is good for the benefit of enhancing desirable effects and not solely focus on adverse effects.

Although the term risk is now used for the first time in ISO 9001, the concept of risk-based thinking has been implicitly embedded in previous editions. The result from the survey supports this notion. Even if scores are slightly lower than in the previous surveys when it comes to perceived level of compliance, a number of organisations seem to be reasonably prepared.

The survey indicates that many organisation's plan to implement a structured or semi-structured approach, rather than a more un-structured and mental (non-documented) approach. In our view this is encouraging as we believe this to be a beneficial way to achieve an effective process.

The new version of ISO 9001 does not put forth an explicit requirement for a formal and documented risk management process. It is up to the organisation to select the method it will use to determine and address its risks and opportunities. The depth and complexity of the approach will largely depend upon the size and complexity of the organisation, in addition to factors like the complexity of external regulations, requirements for public reporting, shareholder interests, public profile, numbers and types of customers, and range and types of suppliers, for example.

Hence there will be a range of approaches, from a simple qualitative process to a full quantitative assessment, depending upon the size and type of company and their respective contexts. Whatever approach is selected, however, it should be a recurring process to reflect changes in the internal and external context. It is therefore recommended that at minimum the outputs of determination are documented to secure a reasonably consistent and repeatable process.

In determining the risk, however, there must be a conscious decision on how to approach it: is action required? Options for dealing with risk can vary and include: avoiding the risk, taking the risk to pursue an opportunity, eliminating the risk source, changing the likelihood or consequence, sharing the risk (e.g. through insurance) or retaining the risk by an informed decision. Where there is a risk that that could impact on conformity of products or service the action taken should be sufficient to address the risk i.e. remove, eliminate or change the likelihood or consequence. And indeed priority should be given to risks that impact on conformity of goods and services.

SURVEY METHODOLOGY

1206 qualified quality management system experts completed the online survey between September 28 to October 4, 2015.

Respondents were drawn from ISO 9001 companies certified by DNV GL. Experts surveyed span around 40 countries and all industrial sectors

- 1.6% Primary
- 64.7% Secondary
- 33.7% Tertiary

DEMOGRAPHIES & RESPONDENTS

IN TOTAL

1206

AMERICAS	220
ASIA	372
EUROPE	608
OTHERS	6

RISK DETERMINATION IN ISO 14001

While ISO 14001 certified companies were not part of this Espresso Survey, we would like to provide some insight into how risk determination is included in the new version.

For 6.1 in ISO 14001:2015 there are extensive amendments compared with 6.1 in the High Level Structure and the clause is divided in the following sub-chapters:

- 6.1.1 General
- 6.1.2 Environmental aspects
- 6.1.3 Compliance obligations
- 6.1.4 Planning actions

Chapters *Environmental aspects (6.1.2)* and *Compliance obligations (6.1.3)* incorporate most of the requirements that are found in the comparable chapters of the 2004 edition, i.e. 4.3.1 and 4.3.2. Thus they remain key pillars while also introducing new elements. Chapter *General (6.1.1)* introduces some new requirements compared to the 2004-edition, as well.

WHAT IS CHANGED OR NEW?

6.1.1 General

In short, this sub-chapter seeks to identify "high potential" risks and opportunities, i.e. issues that has a certain (high) level of impact, whether adverse or beneficial.

The overall intent of the process(es) required from 6.1.1 is to *ensure that the organisation is able to achieve the intended outcomes* of its environmental management system (EMS) in order to prevent or reduce undesired effects and to achieve continual improvement. This can be achieved by determining its risks and opportunities and planning actions to address them. These risks and opportunities can be related to:

- environmental aspects,
- compliance obligations, and/or
- other issues (4.1) and requirements (4.2) .

Environmental aspects can create risks and opportunities associated with adverse or beneficial environmental impacts and other effects on the organisation. The risks and opportunities related to environmental aspects can be determined as part of the significance evaluation or determined separately.

Compliance obligations can create risks and opportunities, such as failing to comply (which can damage the organisation's reputation or result in legal action) or performing beyond its compliance obligations (which can enhance the organisation's reputation).

The organisation can also have risks and opportunities related to other issues (ref. 4.1), including environmental conditions, or needs and expectations of interested parties (ref. 4.2), which can affect the organisation's ability to achieve the intended outcomes of its EMS.

Some potential examples of "high potential" risks related to external/internal issues (4.1) or needs and expectations of interested parties (4.2):

- Own waste disposal site soon reaching its limits and there is a need for alternative solutions.
- Need for a metal producer to source ore from new mines, which potentially may affect air emission levels of heavy metals from own operations.
- Consumers and NGOs ban use of certain ingredients in food products, which puts a company's own products at market and brand risk.

Risks may also be related to environmental conditions that can affect the organisation's ability to achieve the intended outcomes for the EMS.

For example:

- Increased flooding that may affect premises and equipment.
- Water scarcity in drought periods limiting availability to use water for own operations, including emissions control equipment.

6.1.2 Environmental aspects

A significant change for the environmental aspects process is the explicit requirement to consider more strongly the *life cycle perspective*. What does this mean? The organisation may obtain relevant information directly or seek it through the supplier of relevant products and/or services. Information already developed for regulatory or other purposes may also be used. Typical stages of a product life cycle that one should consider could be extraction of raw materials, design, production, transportation, use, and end-of-life treatment. The life cycle stages that are applicable will vary depending on the activity, product or service. It should be noted that a detailed life cycle assessment is not required. Carefully evaluating the life cycle stages that can be controlled or influenced by the organisation may be sufficient.

Another significant change is the explicit requirement to take into account "... *abnormal and potential emergency situations*" when determining the environmental aspect and not solely to focus on "normal" operations.

SAFER, SMARTER, GREENER

TOR GUNNAR TOLLEFSEN
Global Service Manager – Management Systems
Tor Gunnar Tollefsen is national expert delegate to ISO committee TC 207/SC1 WG5, which is responsible for the ISO 14001 revision.

BASTIAAN POLDERMANS
Global Service Responsible – ISO 9001
Bastiaan Poldermans is member of ISO committee TC 176/SC2 WG24, which is responsible for the ISO 9001 revision.

ViewPoint ESPRESSO

viewpoint@dnvgl.com
dnvgl.com/assurance/viewpoint