Updates to Standards

AEROSPACE | AUTOMOTIVE | ENVIRONMENTAL | FOOD SAFETY | IT SERVICES | MEDICAL DEVICES

Quarter 2, 2018

Topics covered in this issue:

ISO 45001:2018 Transition Plan, GDPR Compliance FAQ, Summary of CMMI 2.0 Changes, & Updates to IAF Mandatory Documents

ISO 45001:2018 - New Registration and Upgrade Policy

DQS Inc. is pleased to announce our registration and transition policy for both new clients and clients registered to BS OHSAS 18001:2007.

- The BS OHSAS 18001:2007 standard will be withdrawn in favor of ISO 45001:2018 standard, and there will be a three year transition period for customers to upgrade to the new standard.
- For existing customers already registered to BS OHSAS 18001:2007, all certificates renewed after March 12, 2018, will expire no later than March 12, 2021.
- New client certificates to BS OHSAS 18001:2007 will be valid for a period of less than three years, to expire no longer than March 12, 2021.
- Readiness review or Stage 1 policy
  - If the client has an existing DQS registration to ISO 14001:2015 or RC 14001:2015 with integrated processes, a separate readiness review for ISO 45001 upgrade is a client option but not required.
  - A client or auditor may request a readiness review, gap assessment, or upgrade audit at any time.
  - An off site readiness review or optional on site readiness review is required for a standalone BS OHSAS 18001, or non-integrated system upgrade to ISO 45001:2018.
  - An on site stage 1 is required for a new registration to ISO 45001:2018.
- Existing BS OHSAS 18001 clients must complete their upgrade assessment before December 31, 2020. Upgrade audits will be conducted as a recertification audit. We recommend scheduling it to coincide with the next scheduled recertification audit as the most cost-efficient method.
- New registrations to BS OHSAS 18001 will not be conducted after March 12, 2020
- Gap assessments are available from DQS starting immediately.

DQS Inc. is in the final stages of the ANAB application process in order to be able to provide accredited ISO 45001 certificates.

Would you like to learn more information about ISO 45001:2018 - New Registration and Upgrade Policy? You can gain access to DQS Inc.'s recorded webinar by going to https://dqsus.com/information-center/recorded-webinars/.

Candace Orbaugh, Sustainability Programs Manager

GDPR Compliance - What You Need to Know

The General Data Protection Regulation (GDPR) of the European Union went into effect on May 25, 2018. This regulation will protect the personal information of EU nationals. Any organization regardless of their geographic location will be subjected to this regulation if they are handling personal data of EU nationals.

While GDPR provides elaborate requirements for data privacy, there are very few data protection and data security requirements. Organizations have implemented security controls from other standards like ISO 27001 or NIST 800-53. ISO 27001 allows the adoption of privacy requirements in the Statement of Applicability (SOA). Advantages of ISO 27001 over other security standards is it provides an accredited certification as evidence of compliance.

To help answer any confusion about GDPR you might have, we have compiled some of the questions asked during our GDPR Compliance Webinar.

Q: Is GDPR certification a voluntary or mandatory certification for organizations?
A: According to GDPR Regulation, GDPR Certification is a voluntary certification. However, if you are a processor working for a controller, the controller may require GDPR certification from your company proving its' compliance with GDPR requirements.

Q: Is there a comprehensive to-do list for US-based companies that only have a web presence but no offices in Europe?
A: Currently, there isn't a specific list available; although, one may become available in the future.

Q: If a company credit card is used without any direct reference to an individual, does this come under GDPR?
A: A company credit card number is not private information and does not fall under GDPR unless the company card is attached to an individual.

Q: Does a US company need to have a Data Protection Officer (DPO) located in Europe, if they have a customer located there?
A: No, but if you have an office in Europe then you will need to designate someone to act as the DPO or as the point of contact for complaints directed towards the company.

Q: If my company is ISO 27001:2013 certified, touches Personally Identifiable Information (PII), and has a field office in Europe, what is the impact on my certification audits? What might customers require beyond our ISO certificate?
A: There will be no impact on your certification audits, but you may need to show your customers GDPR Compliance for your European Employees. However, you do have to include the GDPR related privacy requirements into the scope of your Statement of Applicability (SOA), and you will have to be audited against that.

Q: Where can I find the list of authorized countries?
A: Go to https://ec.europa.eu/info/law/ select "Laws by Topic," select "Data Protection" select "Data Transfers Outside of the EU," finally select "Adequacy of the protection of personal data in non-EU countries.

Q: If my company uses remote access but data is not pulled/transferred to a country outside of the EU, will my company still fall under GDPR?
A: If you are accessing data remotely then it is not considered as a transfer. However, the data within EU is still covered under GDPR, so the body storing the EU country's data is still responsible for managing and safeguarding this data. If you are only accessing data remotely and you are not processing this data, we need to see about doing a risk assessment. If it is proof that there is no chance of data breach, then you can claim exemption from GDPR.

Q: Where can I learn more about GDPR?
A: You can go to https://dqsus.com/information-center/recorded-webinars/ and watch a free webinar covering the basics of GDPR.

DQS Inc. provides assessments to the GDPR. Our audit is conducted to the GDPR requirements and a letter report is provided identifying any areas for action. Our recommendation is to combine it with an ISO 27001 audit for the best result.

Subrate Guha, Director of IT Services

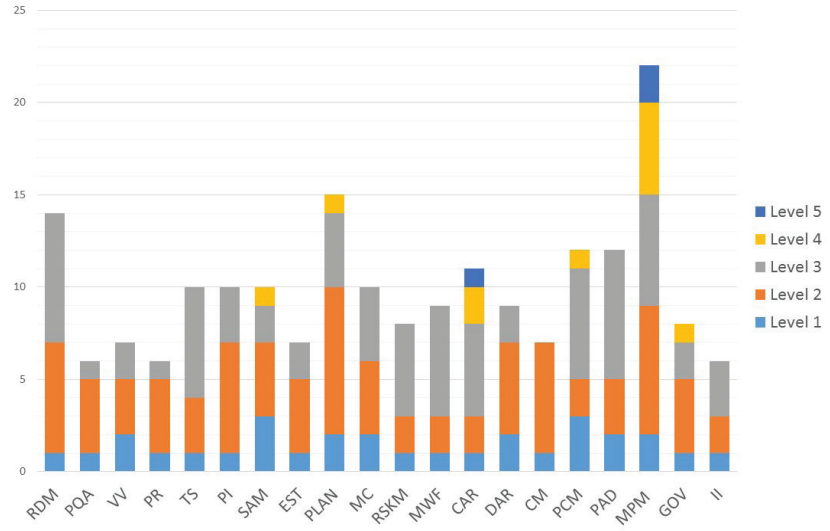
CMMI 2.0 - Summary of Changes

The CMMI Institute released a CMMI rewrite for development 2.0 on March 28.

Structural change in 2.0:

- Practice areas reduced to 20 – Goals and sub-practices removed
- Generic practices removed from each practice areas and moved to a new practice area
- Each Practice Areas have practices for different maturity levels
- Practices assigned to Level 1

The graph below shows the distribution of the practices in various practice areas and maturity levels.



There are a few of nomenclature changes like Process Areas are now called Practice Areas, and practice areas have been reorganized into the following sections.

Requirements Development and Maintenance (RDM): Equivalent to Requirement Development (RD) process area.

Process Quality Assurance (PQA): Simplified from Process and Product Quality Assurance (PPQA) addressing only process QA.

Verification and Validation (VV): Used to be two separate process area.

Peer Review (PR): Peer review was part of PPQA process area.

Requirements Development and Maintenance (RDM): Equivalent to Requirement Development (RD) process area.

Requirements Development and Maintenance (RDM): Equivalent to Requirement Development (RD) process area.

Technical Solution (TS) and Product Integration (PI): Editorial changes.

Supplier and Agreement Management (SAM): These practice areas have added some level 3 and level 4 practices.

Requirements Development and Maintenance (RDM): Equivalent to Requirement Development (RD) process area.

Estimating (EST): Used to be part of Project Planning (PP) process area and has been simplified. Only size estimation is required. Effort, cost, and schedule are derived measures based on the size estimate.

Planning (PLAN): Equivalent to Project Planning (PP) process area. No requirement to plan for data management. Some new practices added including one level 4 practice.

Monitoring and Control (MC): Equivalent to Project Monitoring and Control (PMC) process area.

Risk Management (RSK): Equivalent to Risk Management (RSKM) process area. Requirements have been simplified.

Organizational Training (OT): No major changes.

Causal Analysis and Resolution (CAR): This was a level 5 process area. Version 2.0 requires organizations to do causal analysis from level 1. Requirements grow with the maturity levels. Level 5 requires the use of the statistical method.

Decision Analysis and Resolution (DAR) and Configuration Management (CM): No major changes

Process Management (PCM): Equivalent to Organizational Process Focus (OPF) process area. Requirements expanded to identify business case for improvement and validation of outcome against the expectation.

Process Asset Development (PAD): Equivalent to Organizational Process Definition (OPD) process area. Requirements simplified. Tailoring requirements removed.

Managing Performance and Measurement (MPM): Equivalent to Measurement and Analysis (MA) process area. New and high maturity practices added to elevate scope of this area.

Governance (GOV): This is a new practice area specifically for the senior management. Role of senior management was not explicitly addressed in the previous version except few requirements in the Generic Practices. This is one of the major updates in version 2.0.

Implementation Infrastructure (II): Generic Practices simplified.

CMMI Institute is going to change the appraisal method from SCAMPI A to the Benchmark Appraisal Process and will require less data collection effort and eventually reduce appraisal time and cost. However, the new appraisal process will require annual sustainment appraisals with reduced scope. After the initial benchmark appraisal, organizations have to go through two sustainment appraisals in the following years then it will need another benchmark appraisal. This is very similar to ISO certification cycle.

Please contact us if you are interested in an integrated ISO 9001 and CMMI 2.0 audit.

Subrate Guha, Director of IT Services

IAF Publications Update

Have you wondered how DQS determines the number of audit days required or sampling plans? Or why we ask for your updated information before every audit? Most of our accredited certifications must not only be conducted under the requirements of ISO 17021-1 or ISO 17065 requirements, but also the IAF Mandatory documents.

Who is the IAF? The IAF is the global association of Conformity Assessment Accreditation Bodies in the fields of management systems, products, services, & personnel. Its function is to develop single worldwide program of conformity assessment which reduces risk for business & its customers by assuring that accredited certificates may be relied upon. Accreditation assures users of the competence and impartiality of the body accredited.

The following are some of the IAF Mandatory document numbers/ topics that DQS must meet that directly impact how we conduct management system audits.

IAF MD 1: 2018 – Audit and Certification of Multi-site Organizations
IAF MD 2: 2017 – Transfer of Accredited Certificates
IAF MD 3: 2008 – Advanced Surveillance and Recertification Procedure (ASRP)
IAF MD 4: 2008 – Computer Assisted Auditing Techniques (CAAT)
IAF MD 5:2015 – Audit Time
IAF MD 9:2017 – ISO 13485 Audits
IAF MD 11: 2013 – Integrated Management System Audits
IAF MD 18:2015 – ISO 20000-1 Audits
IAF MD 21:2018 – Migration from OHSAS 18001 to ISO 45001
IAF MD 22:2018 – Occupational Health and Safety Audits

Other IAF documents are published that indirectly impact our audits as they address accreditation body assessment of Certification bodies.

All the mandatory documents are available here for further details: https://www.iaf.nu/articles/Mandatory_Documents_/38

Several of the IAF MD's have been published or revised within the last year: IAF MD 1, 2, 9, 21 & 22. In additional IAF MD 4, 5 and 11 are in the revision process, soon to be published.

Highlights of the recent revisions are:

IAF MD 1 – (Effective January 2018)

Previously IAF MD 1 addressed only audit of multi-site organizations eligible for a site sampling scheme. As such it still includes eligibility requirements for sampling, minimum sample sizes of each group of sites, site selection, and audit methodology at the central office and sites. The revision now incorporates what was in IAF MD 19 to include other multi-site organizations with a single management system but not eligible for sampling or where the client does not want site sampling or the standard scheme does not allow sampling. For these organizations, sampling is limited to the surveillance years where a minimum of 30% of the sites must be audited. The revision reflects that organizations may have a combination of sites eligible for sampling and others that are not.

In addition, some of the new definitions added include:

- Virtual site - "Virtual location where a client organization performs work or provides a service using an on-line environment allowing persons from different physical locations to execute processes."
- Sub-Scope – "The scope of a single-site."

The definition of virtual site has been added to multiple IAF MD's in the last few years and recognizes the increase in design and development organizations that operate fully or partially in an on-line environment.

The definition of sub-scope makes it clear that the activities of each individual site must be listed on the certificate and not just encompassed on the main certificate scope. The use of the sub-scope also helps to enable site groupings for sampling selections.

IAF MD 2 (Effective June 2018)

The most significant change in the certificate transfer requirements is in regard to cooperation between the issuing CB and the accepting CB. The accepting CB is required to contact the issuing CB to verify certificate validity, completeness of documentation and status of nonconformities from the last audit. This cooperation includes communication of the accepting CB's transfer timing so that the issuing CB does not prematurely suspend or withdraw the certificate until the process is complete. If there is a case of non-cooperation in regard to information, the accreditation body of the CB is to be informed.

DQS has operated under requirement similar to this for several years as ANAB issued requirements about this cooperation. It gives full transparency in the process enabling a smooth handover and continued certificate coverage. Without this at times, organizations have been afraid to tell their CB about initiating the transfer process for fear of a lapse between certificates. This communication was difficult initially but works quite smoothly now.

The revision also addresses the allowance for the certificate of the accepting CB to list the prior certificate issuance date of the issuing CB as well as the issue date of the accepting CB. This allows for the organization to show the longevity of continuous certification.

In our next addition, we will highlight other IAF MD revisions. Please contact us with any questions about our multi-site certificate approach or to find out about the process of transferring certificates to DQS.

Lisa Brandon, Vice President of Business Development