Updates to Standards

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

Quarter 1, 2019

Topics covered in this issue:

Aerospace, NIST, TISAX, BRC Issue 8, and ISO 45001 Courses

Aerospace Transition Lessons Learned

Congratulations to all who have successfully completed the transition process for the 2009 versions of the AS standards to the 2016 versions! With the completion of this first year we have all continued to learn and grow as well as receive further clarifications and expectations form the Aviation, Space, and Defense (AS&D) industry. We wanted to take a few minutes to share what we have learned with you!

In the past year, the highest number of NCRs issued globally has been against clause 8.4.3 Information for External Providers. The industry has been sharing the importance of making sure that requirements are flowed down to the sub-tier suppliers. It is critical to make sure that the customer specific requirements typically found in the T and Cs or Quality Clauses of the customers POs are reviewed and flowed down as required/appropriate. If the items listed in the standard are not required to be flowed down to the sub-tier suppliers by the customer, it is the organization's responsibility to review them and determine their requirements in regards to these items.

When completing the AS Basic Data that is sent to you prior to the audit, it is critical to make sure the headcount is accurate. The determination of audit days begins with the number that is provided, and if it is inaccurate, the determined audit duration could also be incorrect ,which often results in additional travel costs. When determining the headcount full-time, temporary, and part-time employees must be included. All individuals that provide support to the system that is covered in the scope of certification must be included. This would include people in support service such as maintenance, calibration, human resources, contract, purchasing, and such. If your AS scope is limited to applications only for the AS&D industry, the headcount must include not just the people who work on the AS&D product but also all support people and management.

OASIS Next Generation provides increased visibility to those who the organization's OASIS Administrator has granted access to their tier 2 data. An aspect that they are looking closely at is the NCRs. They are looking for good robust corrective actions. Evidence of all the actions taken must be loaded into OASIS. If the audit is a recertification or initial audit, evidence of the effectiveness of the corrective action is also needed. It is also important to make sure all timing requirements that are identified in the audit report and the NCRs are met as this information is also visible and the organizations certificate can be suspended if not met.

As we continue to become more familiar with the new standard, the industry has provided a clarification document that includes a lot of helpful information. It is a resource that auditors and certification bodies refer to for guidance on the intent of the industry and the standard. It is available at https://www.sae.org/iaqg/projects/9100-2016_clarification_table.pdf . I encourage you to take a few minutes to review this document and hope you find it as helpful as we do.

NIST Cybersecurity Framework and ISO/IEC 27001:2013

The National Institute of Standard and Technology (NIST) has developed this framework under executive order 13636 for improving critical infrastructure cybersecurity. The framework was initially released in February 2013 and updated in April 2018. All government agencies are mandated to use this framework. As a result, all agencies are expecting compliance to this framework from their major contractors.

An important point to remember is that this is a framework for risk assessment, not a security standard like NIST 800-53 and ISO IEC 27001, so the work compliance can be misleading. This framework was not developed to replace or upgrade existing security standards from NIST. It is a tool for assessing an organization's current risk portfolio and provide them with a roadmap for improving Cybersecurity resiliency.

NIST Cybersecurity Framework has three elements (a) Framework Core, (b) Framework Implementation Tiers, and (c) Framework Profile.

The Framework's core provides essential functions, categories (security domains,) sub-categories (controls,) and references to the international standards where those controls can be found. This has provided references to COBIT, NIST, and ISO 27001 standards.

The second element of the framework is the Implementation Tiers. Based on the maturity of the security posture, four implementation tiers have been defined. The below table shows two dimensions of the framework.

History:

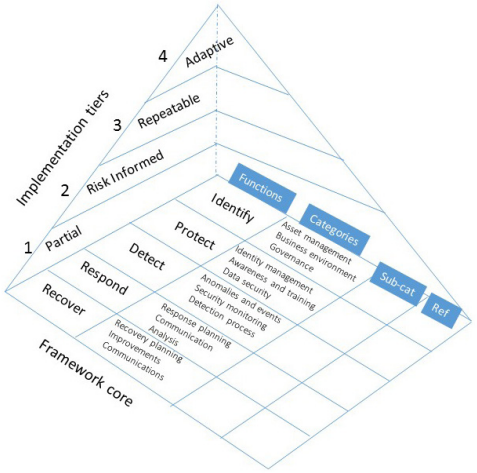
The company has built upon its rich history in this framework is equivalent to "Domain" of ISO 27001 controls or "Family" of NIST 800-53. Sub-category provides control statements, and the next column provides reference to some international standards where details of the control statement can be found.

One example of the complete framework text is in the table to the right:

It is evident that the framework core is providing the requirements but does not provide actual controls. Organizations are free to choose controls from one or more of the international standards from the reference.

The third element of the framework is the framework profile. Organizations can use the framework core to do an assessment to determine status of implementation of the controls as "Fully implemented," "Partially implemented," or "Not implemented." Using this data, the organization can determine their current implementation tier. The Organization can then decide their target implementation tier and develop roadmap for improvements.

The underlining principle of this framework is continuous improvement of security practices. ISO 27001 will be very useful for this purpose, as among the standards referred in the framework only ISO 27001 provides a management system that drives continuous improvement. ISO 27001 requires a repeatable method for conducting risk assessment. NIST cybersecurity framework can be used for risk management. An ISO 27001 certified organization can use the framework as a roadmap for improving maturity of their ISMS.



Function	Category	Sub-category	Reference
Identify	Asset Management	• Physical device and systems are inventoried • Software platforms and applications are inventoried • Communicational communications and data flows are mapped • ----	NIST 800-53 CM8, PM5 ISO 27001 A.8.1.1, A.8.1.2 COBIT 5 BAI09.01, BAI09.02 ....

Did you know?

DQS offers a couple ISO 45001 courses that you can host at your organization to prepare for the transition. Contact your Customer Service Professional, Regional Sales Manager, or sales@dqsus.com.

In addition, we have added a public course that we will host in Research Triangle Park, NC on March 12-13. You can learn more and sign up at dqsus.com/standard/ohsas-18001/iso-45001.

White Paper on TISAX- Information Security in the Automotive Industry

The newest edition of requirements to the Automotive family is TISAX. TISAX is an information security standard created specifically for the automotive industry. Currently the OEMs requiring TISAX are Volkswagen and Daimler. The standard that TISAX is based on is 27001 and is readily available. DQS continues to be engaged in the latest requirements and is one of 6 certification bodies globally that are qualified to audit TISAX compliance. Please contact your customer to see where they stand on TISAX and see the below whitepaper put together by DQS Holding GmbH for more information.

So far, information security in the automotive industry has been strongly influenced by individual approaches - that is about to change. Service providers and suppliers must regularly prove to their customers that they meet the high security requirements for data provided. So far, such assessments have been carried out mainly by the manufacturers themselves, which in the past repeatedly led to unnecessary multiplication.

With TISAX (Trusted Information Security Assessment Exchange), there will be a joint assessment and exchange procedure in the future.

Why TISAX?

Are you a supplier or service provider for the automotive industry? If so, you need only one thing to assure customers that you are keeping their information secure – participation in the TISAX Exchange. All it takes is one assessment every 3 years.

Imagine your partners. They have confidential information they need to share with their supplier – you. The cooperation between you and your partners creates value. The information your partners share with you is an important part of this value creation. Thus, they need to protect it appropriately. And they want to be sure that you are handling this information with the same due care. But how can they be sure that this information is in good hands? They can't just "believe" you. Your partner needs to see some proof.

The participants in TISAX share information via a common online platform on the information security status of another participant, in the form of the results of assessments performed. Important to know: not every TISAX participant automatically has access to the assessment results of another participant. Who receives which information in the TISAX network is something the audited company itself decides by explicit release from case to case.

The advantages of TISAX

- Cross-company recognition of the assessment results among all TISAX participants
- Greater confidence in certified service providers and suppliers
- Avoids the need for multiple checks
- Fewer misunderstandings due to the harmonized VDA-ISA test catalog
- Mutual recognition in the TISAX network saves time and cost
- Only one TISAX assessment every three years

Becoming a Participant – Exchanging Information

Access to TISAX is via a subscriber registration, which takes place online on the TISAX portal. Registration is the prerequisite for being able to select a TISAX accredited audit service provider. Registered participants will receive a list of accredited providers from which they can freely choose. An organization may also register several locations and have a group assessment carried out. After an assessment based on VDA-ISA, information can be provided or obtained in TISAX.

Who is behind TISAX?

TISAX uses the ISA questionnaire compiled by the German Automotive Industry Association VDA based on essential aspects of ISO / IEC 27001. Recently, the VDA developed this into a common assessment and exchange procedure called TISAX, which is operated by ENX, an association of European car manufacturers, suppliers and associations.

ENX monitors adherence to the TISAX procedure, which includes general requirements for audit service providers and specific requirements for ENX TISAX audit service providers, and safeguards the quality of implementation and assessment results. To this end, ENX concludes contracts with all authorized audit service providers as well as with the participants. Standardization and quality control will ensure common recognition of test results among all TISAX participants.

Conducting a TISAX assessment by DQS as a TISAX Accredited Audit Provider (XAP)

Customer submits scope and and assessment level, e. g. with or without prototype protection.

↓

Online registration as TISAX participant at www.enx.com/tisax, followed by registrations of the scope ID by ENX (annual service fee).

↓

Selection of an authorized audit service provider, then kick-off, document review (self-assessment, not on-site) and subsequent assessment (level 2: off-site, level 3: on-site)

↓

The interim report is discussed; in case of non-conformities, corrective actions are agreed upon for implementation.

↓

If necessary, implementation of actions in the agreed time period. Once the non-conformities are closed, an effectiveness check will be carried out by means of an assessment.

↓

The final report will be posted on the TISAX online platform. That done, the participant is listed with their TISAX Labels.

BRC Food Issue 8: New Clauses and Changes

After a transition phase of six months, the BRC Food Standard Issue 8 will replace Issue 7 on the 1st of February 2019. To prepare you for the new version, we have outlined the most important changes below.

What's New?

Despite being an evolution from previous versions of the standard, the BRC Global Standard for Food Safety Issue 8 introduces quite a lot of significant changes compared to its predecessor Issue 7. According to BRC, the new issue has consolidated key themes including ensuring global applicability and benchmarking to the Global Food Safety Initiative (GFSI), encouraging the development of a food safety culture and expanding the requirements for environmental monitoring. Alongside these areas of focus are the addition of new sections and clauses, which we have summarized for you below.

Removing second/split unannounced audit option

Version 7 of the BRC Food Standard offered three audit options: Full announced audit, full unannounced audit, and split unannounced audit. The last one divided the audit requirements into two separate audits, the first one unannounced and the second one announced. Reflecting that the full unannounced audit option is generally preferred because it gives extra confidence to specifiers, Issue 8 will remove the split unannounced audit option. Unannounced audits remain optional.

Food Safety Culture

Food Safety Culture is a fundamental factor in the management of product safety. Issue 8 places more emphasis on developing a Food Safety Culture. Sites shall plan to maintain and develop food safety and quality culture within the business and during objective setting. This also involves the management. As company culture is a rather subjective issue, the auditor does not evaluate the culture itself, but the documented measures with regards to the status of the culture in the organisation and the improvement measures that have been introduced.

Significant food safety issue

In Issue 7 the certification body needed to be notified when there was a product recall. Issue 8 expands this requirement to any "significant food safety issue". Situations in which the certification body should be notified include all product recalls, any situation where regulatory authority insists on action (e.g. an enforcement notice) due to product safety or legality concerns, adverse media attention relating to product safety or any food safety incident with the potential to harm a consumer. It should be noted that only the site(s) where an issue occurs is/are required to notify their certification body.

Section 8: High Risk, High Care and Ambient High Care Requirements

The requirements for production facilities who fall into the high risk, high care and ambient high care categories have been centralized and are now found in section 8. Sites are expected to demonstrate that production facilities and controls are suitable to prevent pathogen contamination of products. These clauses, previously found under section 4 and 7, need to be fulfilled in addition to all relevant requirements in sections 1 – 7.

Section 9: Requirements of the traded goods- voluntary module

This module has been incorporated as a separate section and requires the organization to operate procedures for approval to ensure that food products are safe, comply with legal requirements and are manufactured in accordance with product specifications. In a stark difference to Issue 7, any non-conformities assigned against this module will now be included in the overall grade.

The Integration of Pet Food

Found under section 5 (Clauses 5.1.5 – 5.1.7), pet food has been integrated and defined to assist manufacturers. This encompasses the procedures when dealing with products for various animal species and ensuring that products are designed for their intended use (complete diet or complementary product). Medicated food needs to be precisely labeled, materials need to be clearly identifiable and involve mechanisms to ensure that the correct concentrations are used.

Whistleblower system

It is now fundamental that a whistleblower system be integrated to ensure all concerns regarding product safety, integrity, quality and legality to senior management can be reported and handled confidentially. The method (e-mail, hotline number etc.) needs to be clearly communicated to employees. A process to handle concerns raised needs to be implemented and documented. This ties in particularly well with BRCs newly released whistleblower hotline.

The addition of Cyber Security Clauses

Under section 3, clause 3.11.1 it is a requirement that organizations implement procedures to document and handle cyber attacks or the failure of their internet security. As this topic becomes increasingly more relevant, it brings BRC Food in line with other standards and principles.

Internal Audits

According to BRC, it is clear that many sites are not effectively scheduling internal audits throughout the year, which is evident by the non-conformities being raised. To combat this, clause 3.4.1 has been amended to ensure that safety management systems are being assessed at regular intervals. This means at least 4 audit dates per year.

Transition Timeline

Starting from the 1st of Feburary 2019 the use of the new standard is compulsory. Prior to that date, it is not possible to be certified according to the new version.

By: Thijs Willaert, DQS CFS