Quality Partner Newsletter September 2021

Issue date: September 2021

Firstly, I hope you are all safe and well.

Welcome to the twenty third edition of the Quality Partner newsletter. The newsletter is designed to keep readers up to date with developments in Quality Management Systems, in particular related to the Automotive Quality Management Standard IATF 16949: 2016

For this edition I again sought ideas and inspiration from the IATF 16949 LinkedIn group. The group is a great forum to share and discuss issues with IATF 16949 and the associated scheme, with over 56000 members. Considering ideas from the group, this issue focuses on:

- Contingency planning
  - Sanctioned interpretations
- Cyber security
  - Outsourcing
  - Manufacturing processes
  - Non-manufacturing processes
- Risk based audit days
- Questions from LinkedIn colleagues and answers

If you have any questions or topics for future editions, please feel free to mail to: paul.hardiman@qualitypartner.co.uk

Despite the ongoing situation with Covid 19, the number of organizations certified to IATF 16949 remains stable with 80,620 IATF 16949 certified sites at end of August 2021.

Many third-party audits continue to be done remotely where auditors cannot get to the client's site or remote support functions.

The top 3 countries continue to be China (40657 sites), India (6212 sites) and Republic of Korea (5068 sites) .

I hope you enjoy this edition of the newsletter. Let us continue to network and learn together!

It is great to get so much positive feedback on the newsletter, which inspires me to continue writing!

For more information on Quality Partner onsite and remote courses related to IATF 16949, best practice auditing, effective implementation of the automotive core tools contact: paul.hardiman@qualitypartner.co.uk

For More Information Visit www.qualitypartner.co.uk

Author: Paul Hardiman

qualitypartner
delivering quality as standard

An IATF 16949 requirement that has become an area of focus in audits is 6.1.2.3 Contingency planning.

Before we study the detail of the requirement, we also need to review sanctioned interpretations SI 3 (which incorporated SI 17)

Considering this SI, the current requirement is (changes in red):

"The organization shall:

a) identify and evaluate internal and external risks to all manufacturing processes and infrastructure equipment essential to maintain production output and to ensure that customer requirements are met;

b) define contingency plans according to risk and impact to the customer;

c) SI 3. prepare contingency plans for continuity of supply in the event of any of the following, but not limited to: key equipment failures (also see Section 8.5.6.1.1); interruption from externally provided products, processes, and services; recurring natural disasters; fire, pandemics; utility interruptions; cyber-attacks on information technology systems; labour shortages; or infrastructure disruptions;

d) include, as a supplement to the contingency plans, a notification process to the customer and other interested parties for the extent and duration of any situation impacting customer operations;

e) periodically test the contingency plans for effectiveness (e.g., simulations, as appropriate);
SI 3 For cybersecurity testing may include a simulation of a cyber-attack, regular monitoring for specific threats, identification of dependencies and prioritization of vulnerabilities. The testing is appropriate to the risk of associated customer disruption; Note: cybersecurity testing may be managed internally by the organization or subcontracted as appropriate

f) conduct contingency plan reviews (at a minimum annually) using a multidisciplinary team including top management, and update as required;

g) document the contingency plans and retain documented information describing any revision(s), including the person(s) who authorized the change(s).

h) include in contingency plans the development and implementation of appropriate employee training and awareness"

Not surprisingly the SI added requirement related to areas of high risk, including pandemics and cyber security. The requirement "interruption from externally provided products, processes, and services" was already included, which covers the management of supply chain shortages (semiconductor chips etc.).

Before we study the additions, it is worth reminding ourselves on the purpose of contingency plans. The requirement is to ensure that whatever circumstances an organization faces, they are still able to supply to meet customer requirements.

It is less important what the organization call the plan (there is no requirement to call any documented information a contingency plan, it can be called disaster recovery plan, emergency response plan etc.), or whether all the information is in one document, but more important what is the content!

Let's look at some of the changes:

Cyber security

Cybersecurity is a growing risk to manufacturing sustainability in all manufacturing facilities, including automotive. Organizations need to address the possibility of a cyber-attack that could disable the organization's manufacturing and logistics operations, including ransomware. Organizations need to ensure they are prepared in case of a cyber-attack.

It is important to point out that IATF 16949 is not a cyber security standard, it is an automotive quality management system standard and that IATF auditors will not be cyber security experts.

There are already dedicated standards related to IT and security including:

ISO 20000: IT Service Management

ISO 20000 is the international ITSM (IT service management) standard. It enables people responsible for IT processes to ensure that their ITSM processes are aligned with the business's needs and international best practices. The ISO 20000 standard helps organisations benchmark how they deliver managed services, measure service levels, and assess their performance.

ISO/IEC 20000-1:2018 Service management system requirements is the standard for certification while ISO/IEC 20000-2:2012 Guidance on the application of service management systems is for guidance.

ISO 27001: Information Security Management System

ISO 27001:2013 is the international standard for information security. It sets out the specification for an information security management system (ISMS). The information security management system standard's best-practice approach helps organisations manage their information security by addressing people, processes, and technology.

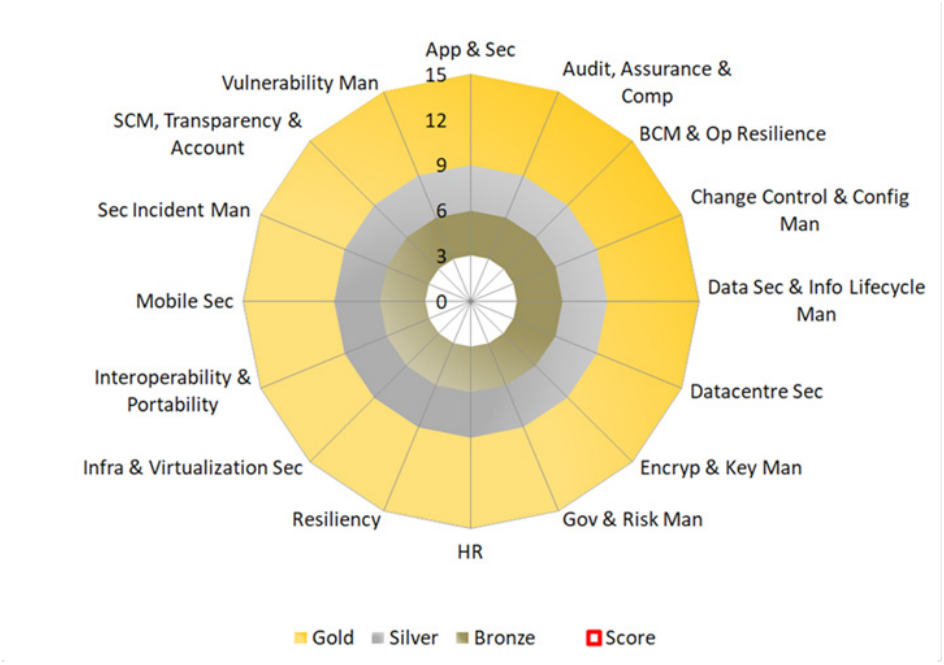
STAR

The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM). Publishing to the registry allows organizations to show current and potential customers their security and compliance posture, including the regulations, standards, and frameworks they adhere to. It ultimately reduces complexity and helps alleviate the need to fill out multiple customer questionnaires.

STAR level 1 is a self-assessment, while STAR level 2 is a third-party certification.

The third-party audit gives organizations a maturity scale to the security and service delivery that they offer. A spiderweb graph, called a medallion, identifies whether a set of controls and sub-controls are within a specification of No Formal Approach, Reactive, Proactive, Improving, or Innovating.

Based upon the result of the assessment organizations are awarded bronze, silver or gold level based on the medallion below.



TISAX

Trusted Information Security Assessment Exchange (TISAX) is a common assessment and exchange mechanism in the automotive industry. It is an inter-company test and exchange mechanism based on the VDA Information Security Assessment (ISA). TISAX has been developed under the guidance of the VDA to ensure a unified level of information security. TISAX brings standardisation, quality assurance and mutual recognition of audits. TISAX provides for information security assessments by audit providers in accordance with VDA standards and helps avoid redundant audits.

The scope of TASAX assessments is broken down into 4 modules,

1. Information security management system (ISMS): which is a module that is mandatory and contains 52 controls
2. Data protection: this module is required when the supplier processes personal data of customers (4 controls)
3. Connecting with third parties: which is required when the supplier is connected to an IT network or similar technical exchange of confidential data where the manufacturer is established (4 controls)
4. Prototype protection: which is required when the supplier works with strictly confidential information about prototypes (22 controls)

The IATF contingency planning requirement is not only focused on being reactive if a cyber attack occurs, but being proactive by testing contingencies:

e) periodically test the contingency plans for effectiveness (e.g., simulations, as appropriate);

SI 3 For cybersecurity testing may include a simulation of a cyber-attack, regular monitoring for specific threats, identification of dependencies and prioritization of vulnerabilities. The testing is appropriate to the risk of associated customer disruption.

Note: cybersecurity testing may be managed internally by the organization or subcontracted as appropriate Also, the newly issued SI 22 against requirement 7.2.1 states

To reduce or eliminate risks to the organization, the training and awareness shall also include information about prevention relevant for the organization's working environments and employees' responsibilities, such

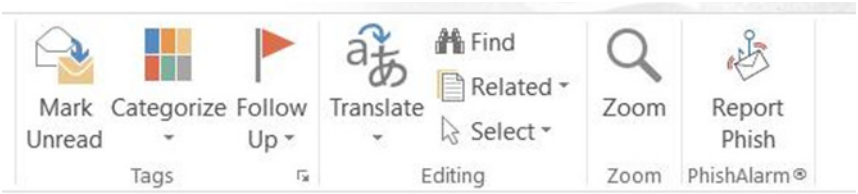
as recognizing the symptoms of pending equipment failure and/or attempted cyber-attacks."

What should an IATF auditor look for in auditing these requirements?

Firstly, these requirements and SI's state "may" and "such as" and not a shall, and that any testing of cyber security systems should be based on risk to customer disruption.

An auditor can challenge the process owner responsible for IT security on how employees are trained in being aware of the dangers of opening "fishing" e-mails and their attachments.

An example of possible evidence is shown below:



Approximately once a month employees get a "fake/phish mail" from their IT team to train/alert them of suspicious e-mails. A "phishing button" on top of each mail is clicked if the employee believes the mail is fake/fishing.

IT can then monitor how many/which people are opening a mail while they should not, and then trigger appropriate retraining.

SI 3 also adds to 6.1.2.3 e) a note (which is guidance only):

"Note: cybersecurity testing may be managed internally by the organization or subcontracted as appropriate".

In bigger organizations the testing may be managed by the internal IT processes, but for smaller organizations the activity may be outsourced. This itself can bring possible threats if the organization does not select a competent service provider.

An IATF auditor can challenge an organization on how any IT service provider is selected, including what valid certifications (which may include the standards outlined above), and then who is responsible in the organization for interacting with the service provider, including analysis of any results of penetration testing. Finally, cyber security gets a mention in 7.1.3.1 Plant, facility, and equipment planning through SI 18, which adds

"c) implement cyber protection of equipment and systems supporting manufacturing."

An auditor can challenge an organization on how cyber protection is ensured for any manufacturing equipment, or supporting systems, especially if the equipment is connected to internal systems and to the internet, for example to receive software updates from equipment manufacturers. This poses a potential risk which people responsible for the IT process should be aware of and managing.

A particular risk for an auditor to focus on is where new equipment is introduced where IT may not be informed.

Summary

IATF auditors, whether internal, second or third party do not need to be IT experts but do need to have the confidence to challenge the relevant personnel on how IT security risks are being managed, and how effectiveness of this is measured.

7.2.3 Internal auditor competency states:

c) understanding of applicable ISO 9001 and IATF 16949 requirements related to the scope of the audit;

The requirements discussed above, including those introduced through SI's, are part of the IATF requirements and therefore auditors auditing any aspects of the organizations management of IT security, including contingency planning, need to be understood.

Contingency planning awareness and training

Now let's look at the requirement in 6.1.2.3, and SI 3:

"h) include in contingency plans the development and implementation of appropriate employee training and awareness"

The contingency plan should be created by a multidisciplinary team, although we all know in many companies it is created by an individual! Sometimes, the relevant process owners are not even aware of it.

Rather than it just be a theoretical pile of paper, the requirement is now clear that all the relevant employees that would have to react in a situation that could impact supply to the customer know how to react, including short term actions, communication with the customer etc.

This could be personnel working in production, supply chain, HR, IT, maintenance etc. An organization should have evidence the relevant people are aware of the plan and know how to react, this could be very short awareness sessions, does not need to be days of training!

What is Outsourcing?

The word "outsource" is mentioned in the IATF definitions, and then the word is used 6 times in the auditable requirements, including in 4.4.1.1, 7.5.1.1, 8.3.4.3 (twice), 8.4.2.1 and 8.5.1.6.

The definition of outsource in ISO9000 is *"make an arrangement where an external organization performs part of an organization's function or process"*

whereas in IATF the definition is *"portion of an organization's function (or processes) that is performed by an external organization"*

I think there is a lot of confusion on what outsource really means, amongst organizations and auditors, and how this should be audited in internal and external audits.

Let's explore this by asking the following questions:

1. Are the IATF requirements just applicable to outsourcing manufacturing processes (e.g., heat treatment), or any QMS related process?

My view both.

I propose we need to divide the discussion into two sections, namely outsource of an aspect of a manufacturing process, and then any other process that may affect the effective implementation of a Quality Management System (QMS)

Outsourced manufacturing processes

Firstly, we need to make clear that outsourcing is not the procurement of components or materials that are an input into the manufacturing process. The management of this procurement activity is covered by ISO9001 and IATF 16949 requirements in 8.4 Control of externally provided processes, products, and services.

Many organizations elect to outsource aspects of their value-added manufacturing process to an external provider, and in the context of IATF this is considered outsourcing.

Under the requirement 8.4.2.1 Type and extent of control — supplemental

*"The organization shall have a **documented process** to identify **outsourced processes** and to select the types and extent of controls used to verify conformity of externally provided products, processes, and services to internal (organizational) and external customer requirements.*

The process shall include the criteria and actions to escalate or reduce the types and extent of controls

and development activities based on supplier performance and assessment of product, material, or service risks…."

For a new product, the need for outsourcing would be determined in the new product introduction process, and as well as the selection of an external provider who has, at minimum, ISO9001 certification (as defined in 8.4.2.3 Supplier quality management system development). When developing the process flow, PFMEA and control plan for the manufacturing process the interactions between the site and the outsourced process would have to be considered.

The organization would not be responsible for developing the process flow, PFMEA and control plan for the outsourced process, but as part of requirement 8.3.4.4 Product approval process they would need to *"approve externally provided products and services per ISO 9001, Section 8.4.3, prior to submission of their part approval to the customer".*

The following IATF 16949 requirements also need to be met:

4.4.1.1 Conformance of products and processes

The organization shall ensure conformance of all products and processes, including service parts and those that are ***outsourced****, to all applicable customer, statutory, and regulatory requirements (see Section 8.4.2.2).*

Once approval is gained for a new product from the customer, the organization then needs to implement the "types and extent of controls" decided on based on risk, which could include a combination of supplier audits/development and receiving verification and/or inspection as defined in the PFMEA and control plan.

Let's look at an example. An organization manufacturers cam shafts, for which the raw forging is bought in, machined, then sent to an external provider (outsourced) for heat treatment, and then ground to final size before sending to the customer. The heat treatment supplier is ISO9001 approved and historically had given good quality and delivery performance. There have historically been no customer complaints related to heat treatment.

In this example the organization has the following information available for audit:

- The part approval documentation for the relevant part, including the heat treatment supplier submission, in any customer prescribed format, approved by the customer. (8.3.4.4)
- A process flow, PFMEA and control plan, showing the interfaces and risks between the site and the outsourced heat treatment process, and the monitoring strategy for the receipt of the product from the heat treatment supplier (receiving inspection) (8.3.5.2)
- A documented process for managing outsourced suppliers (8.4.2.1)

- A purchase contract with the heat treatment supplier, including communication of customer and any legal and regulatory requirements, as well as requirements for product batch traceability (8.4.3.1)
- Records of the heat treatment suppliers ISO9001: 2015 accredited certificate (8.4.2.3), and data on their quality and delivery performance. (8.4.2.5)
- A supplier development plan to move towards IATF 16949 certification (8.4.2.3)
- Records of receiving inspection, done at a frequency defined in the control plan (8.6.4)

In my view, if the above is effectively implemented, this is meeting the intent of the requirements in IATF 16949 related to the management of manufacturing outsourced processes.

A requirement that often causes discussion is 7.5.1.1 Quality management system documentation (Quality Manual) especially:

c) the organization's processes and their sequence and interactions (inputs and outputs), including type and extent of control of any ***outsourced*** *processes;*

To address this requirement organizations often develop a high-level process map to show the process sequence and interaction and include this in the Quality Manual. But, in this, the high-level manufacturing process may just be shown as "production", and not broken down into the manufacturing sub-processes, so therefore in the case above, heat treatment would not be shown as an outsourced process.

Is this compliant?

The requirement clearly states the quality manual does not have to be a single document "The organization's quality management system shall be documented and include a quality manual, which can be a series of documents"

In my view it is ok, if the process flow diagram, which is part of the QMS, and the documented process on outsourcing are available, and define the relevant sequence and interaction between the site and the outsourced heat treatment process.

For any third party audit, the auditor would not visit the heat treatment supplier, but should verify the effective management of the outsourced process, including the information outlined above.

Outsourced non-manufacturing processes

As well as outsourcing manufacturing processes, many organizations in the automotive supply chain may decide to outsource other processes that can have an impact on the effectiveness of the QMS. Examples could be:

- IT services such as cyber security
- Site services including site security
- Facility of equipment maintenance services
- External calibration
- Provision of human resources (e.g., recruitment or temporary resource agencies)

A question that often arises from this is:

Is this outsourcing or is it covered by the requirements in 8.4 Control of externally provided processes, products, and services?

In my view it does matter, if the activity is effectively managed by the organization within the scope of the QMS, and evidence can be provided that all the relevant IATF 16949 requirements have been effectively addressed within the relevant QMS processes.

For all the above there should be:

- Evidence on how the external providers were selected to ensure they can provide the relevant services, and meet any relevant IATF 16949 or customer specific requirements (8.4.1, 8.4.1.2)
- Documented information related to 8.4.3 Information for external providers, which could include purchase orders, contracts, or service level agreements (8.4.3)
- Defined roles, responsibilities, and authorities for ensuring the relevant external providers performance is monitored, acceptable, and meets the relevant IATF 16949 requirements (5.3.1)
- Evidence that the external providers have provided the services provided in the above (8.4.3)
- Evidence of external provider performance as an input to management review (9.3.1)
- Evidence that any issues with external provider performance are dealt with effectively (10.2.1)

If an organization makes the decision to outsource a complete process (for example an organization may outsource their entire IT Management process), they must still have somebody defined to manage the interaction with any outsourced process and ensure that documented information is available to ensure all the relevant IATF 16949 requirements are met.

Summary

Whether an organization outsources part of its manufacturing process, or all or one aspect of another QMS process, the key thing is they must show control, ownership and have documented information available to demonstrate the outsourced processes are providing the correct services and at the same time meeting all the relevant requirements of IATF 16949.

The complete manufacturing process cannot be outsourced, as the organization would not meet the eligibility criteria defined in the IATF rules.

Risk based audit days

Many of you will be aware that IATF established a set of rules titled “Rules for achieving and maintaining IATF recognition, currently at the 5th Edition.

If IATF want to change a requirement in the Rules this is done through sanctioned interpretations (SI’s).

One sanctioned interpretation issued in February 2021, effective June 2021, was SI 26 related to audit day calculations for third party audits. In the SI it states:

“When the client does not meet the IATF OEM quality and/or delivery targets specified in the IATF OEM scorecard(s), the certification body shall increase the total audit days by the hours listed in the table below. The increased audit time shall be used to review the corrective actions associated with the IATF OEM quality and/or delivery targets not being met and the associated risk to similar processes / products……”

Firstly, this will only apply to first tier suppliers who supply directly to an IATF member with a supplier code issued by the relevant OEM, including its subsidiaries, affiliated brands and joint ventures as defined in the IATF member quick reference guides, available at: https://www.iatfglobaloversight.org/oem-requirements/quick-reference-guides/

For these IATF 16949 certified organizations, the 3rd party auditor will ask them to provide customer scorecard data prior to any surveillance, transfer, or recertification audits. Based on the scorecard review, and any supporting information, the auditor will make the decision if additional audit time is needed.

The additional time added allows the certification body to dedicate more time to focus on performance issues that have posed a risk to the organization’s customers.

If the organization can provide evidence of effective implementation of the corrective actions for the quality and/or delivery performance issues at the time of supplying the planning data, then no increase is applied.

This gives the certification bodies significant challenges in the logistics of planning audits, as they will only know if additional time is required close to the audit. For organizations this will be an additional cost, which is difficult to budget for.

The solution: Provide the OEM's good quality and delivery performance!

New video discussion series on auditing

I am delighted to have teamed up with Agata Lewkowska, owner of Qualitywise.pl, Poland to film a series of videos on best practice auditing in the automotive industry.

The series will be published shortly on You Tube, more details will be published on the LinkedIn IATF 16949 group. The link to access the series on You Tube is https://www.youtube.com/watch?v=uon12HG5MmA

A video from the 10 video series will be published weekly on a Wednesday.

Ask the expert

Quality Partner's expert, Paul Hardiman

Question
I recently conducted an internal audit and found the following issue:

"The welding parameters of the welding equipment are not set according to the work instructions"
Which appropriate requirement from the IATF 16949 would suit the deviation?

Answer
Firstly, as an auditor I would want more objective evidence, for example:

- Were the weld parameters correct at the time of job set up, (Review set up records) or adjusted afterwards?
- Were the weld parameters in the control plan, and did they match those in the work instruction?
- Was there any temporary deviation in place?

The more objective evidence you collect the easier it is to identify the potential system problem, and to

allocate the most appropriate clause.

In this case the relevant requirements could be:

- 8.5.1.2 Standardised work — operator instructions and visual standards
- 8.5.1.3 Verification of job set-ups
- 8.5.6.1.1 Temporary change of process controls
- 9.1.1.1 Monitoring and measurement of manufacturing processes

The important thing to stress to the relevant process owner is that the correction should be taken to address the specific incident, but systemic corrective action should be taken, including root cause identification to prevent further instances.

Question
We recently had a nonconformity in a third-party audit related to not undertaking an attribute MSA study for visual inspection.

In reviewing the control plans, we do visual inspection of over 100 finished product part numbers, with over 100 operators doing the inspections. However, all inspections relate to surface finish of automotive trim products.

My question is do we have to do studies for each part number and for all operators? Our fear if the answer is yes, this would mean hundreds or thousands of studies, and take man-years of work.

Answer
The relevant requirement in IATF 16949 is 7.1.5.1.1 Measurement system analysis which states:

"Statistical studies shall be conducted to analyse the variation present in the results of **each type** *of inspection, measurement, and test equipment system identified in the control plan."*

In addition, IATF 16949 frequently asked question 6 which states:

A complete statistical study on each single piece of equipment is **not** required. Instruments with the same characteristics (e.g., measurement range, resolution, repeatability, etc.) can be grouped and a sample instrument (representative of the gauge family) can be used for the statistical study.

Although the FAQ is written in the context of variable equipment the same principles apply to attribute equipment (including visual inspection).

You certainly do not need to do a study for every combination of part number and operators! Firstly, before considering any MSA study, you should ensure that the IATF requirement 8.6.3 Appearance items are met, namely:

"For organizations manufacturing parts designated by the customer as "appearance items," the organization shall provide the following:

a) appropriate resources, including lighting, for evaluation;
b) masters for colour, grain, gloss, metallic brilliance, texture, distinctness of image (DOI), and haptic technology, as appropriate;
c) maintenance and control of appearance masters and evaluation equipment;
d) verification that personnel making appearance evaluations are competent and qualified to do so."

Even if the parts in question are not appearance items, you must ensure an appropriate work environment, and that all the operators are competent to make the relevant inspections (which could include eyesight and colour blindness checks).

Then you can group the types of visual inspection into groups. If all the painted products are similar with similar defined standards/requirements, then one study may be sufficient. In making this decision you should also consider customer specific requirements.

You would then select three operators at random that perform the inspections, select a minimum of 30 parts (should be a part that has the tightest inspection criteria or a part that has more historic problems). Some parts should meet the standard and some parts not, as determined by an expert.

You are then ready to perform the attribute agreement analysis. Remember the study should be done in the normal work area!