IMPACT
PRESENTED BY DQS INC.
Quarter 3, 2021

CMMC & Cybersecurity Risk Mitigations

In this issue:

"Cybersecurity can be a complex topic - but it doesn't have to be."

As a certification body, our business reputation is key to our on-going success. And as we began working on our activities to add the new Department of Defense (DoD) – Cybersecurity Maturity Model Certification (CMMC) to our offerings, we were well on our way through our gap assessment. However, along the way to understanding and implementing the requirements for CMMC – our focus is and continues to be eliminating or reducing business risk first with the goal of achieving CMMC as an affirmation to mitigating risk and supporting our customer's needs.

Data security is key, but demonstrating continual improvement, proactive risk mitigation and cybersecurity certification may be part of customer contractual requirements and can be a market differentiator. If your company is reviewing your cybersecurity controls and risk assessment, hopefully sharing our journey may lend some perspective for your consideration of next steps.

The DQS journey began in August 2020 with that all important self-assessment. Gaps were identified and the process for gap closure began. In January 2021, DQS Cyber Security Inc. was incorporated to lay the foundation for CMMC standard certification.

As gap actions were progressing, we received a Zero-Day Exploit notification from Microsoft on March 2nd. DQS installed the critical patches on March 3rd and performed a scan. The scan showed the exchange server was targeted by the Exploit and IOCs were found in the logs. With immediate support from a cybersecurity firm, no traces of malicious activity or footholds or compromise were found. The cybersecurity firm did provide risked-based feedback for consideration based on review of our network.

Having this third party, unbiased set of eyes widened the team's perspective beyond the gap assessment. Through this assessment, additional actions were added to the gap closure plan.

Throughout the process, several technical and administrative controls were implemented. Examples include: multi-factor authentication, enhanced password policies, increased physical security, adding additional layers of firewalls and expanding the use of VPN, moving to cloud based exchange, and on-going monthly risk mitigation and ISMS Management Reviews with top management.

Then came the Kaysea event in June. DQS does use the Kaysea tool. However, since March many layers of protection and controls have been added to the network. Our cybersecurity partner identified the threat early on and was able to take all assets off-line and without incident. This was a true test of the risk mitigation activities done to date.

It has been almost six months since the Zero-Day Exploit event, and as we look back to where we were, to where we are it is amazing what has been accomplished in the past year.

Cybersecurity can be a complex topic – but it does not have to be. Yes it requires specialized and technical experts, but it also requires all stakeholders – including employees, process owners, suppliers, and customers to build a strong Information Security Management System.

Continued on page 2

AT PRECISION

AT Precision has been continuously ISO 9001 certified since May 18, 2000. To celebrate this milestone, DQS Inc. President and CEO Brad McGuire and Regional Sales Manager Mike Curry presented a plaque to the Chuck Thudium and Rich Hauser at AT Precision in June for their commitment to quality.

AT Precision was founded in 1990 and provides highly accurate machined components to a wide variety of customers for various industries. Their commitment to quality has resulted in many of their new customers referred to them by satisfied existing customers.

Congratulations, AT Precision!

Continued from page 1

To begin – a good approach may include starting with understanding the context of the organization, who the interested parties are in your business and what are the needs and expectations of those interested parties. Then understanding your current state and current risk to meeting those needs, helps to put things in perspective and help the organization prioritize highest risk items first. Some actions take longer than others to implement, while others may be quick things to accomplish, but it helps to understand the runway as you work on hardening your environment. Understanding the total tasks and timing helps with resource planning, whether those resources are internal or external. Having a reoccurring cadence, with strong leadership participation that is focused on these resources on these priorities can help the organization eliminate or reduce risk over time.

Once an organization has done their self-assessment, having an independent, impartial "fresh set of eyes" review your cybersecurity program can provide validation of the activities, areas for improvement or understanding any additional gaps that may still need to be addressed.

At DQS, our core business is to perform the assessments of management systems for client organizations. DQS is a certification body for companies to more than 100 national and international standards and sector- or customer-specific requirements. Currently, we have more than 2,500 leading industry experts with the knowledge and expertise to help in achieving business objectives. We serve a wide spectrum of industry sectors, including automotive, electrical, engine construction, the metal and chemicals industries, services, food, health care, the aviation and aerospace industries and telecommunications. DQS certificates have been issued for more than 65,000 customer sites from more than 85 offices.

DQS has IT Service Sector with a wide range of industry experience across several standards that can offer Gap Assessments/Certifications in the following:

- CMMC – Level 1 and Level 3 (Gap Assessment)
- NIST 800-171 – Letter of Conformance
- NIST 800-53 – Letter of Conformance
- ISO 27001 – Information Security Management System (accredited certification) (Gap assessment)
- ISO 27701 – Privacy Information Management System (accredited certification) (Gap assessment)
- ISO 27017 – Cloud Services for PII - Letter of Conformance
- ISO 27018 – Protection of PII - Letter of Conformance
- ISO 22301 – Business Continuity - Letter of Conformance
- TISAX - Certification
- Cloud Security Alliance STAR (certified audit firm)
- CMMi Appraisal (licensed partner)

With regards to CMMC specifically – DQS has Provisional Assessors who can assist in Gap Assessments while we are awaiting next steps in our C3PAO application.

Let us know how we can help along your cybersecurity journey.

Regards,

Laura Flanagan

Lead Auditor and CMMC Project Manager

DQS Inc.

Mobile: 231-350-1136

Email: Laura.Flanagan@dqsus.com

REGISTERED FIRM MARK USE

The DQS Use of the Registered Firm Mark document has been updated. It can be found at https://dqsus.com/requirements-and-regulations/ and below is a summary of the changes.

- A.2.2 – Registered Firm Mark can no longer be used on our client's quotes as that can imply product certification. Further explanation about not using on calibration certificates, certificates of analysis, etc. is provided.

- A.2.3 – Clarification regarding bulk packaging use and not implying product certification.

- A.2.5 – Addition that use of statements of conformance must also be removed upon withdrawal.

- A.5 – New section on restrictions on ISO logo is added and allowances on using statements of conformance is updated.

Initial Audit Process Introduction

The first step in the certification journey will be an initial (sometimes called Registration) audit. The initial audit is made up of two steps – the first step is called the Stage 1 audit, and the second step is called the Stage 2 audit. The Stage 1 audit is a readiness review, and the Stage 2 is a full audit of the system.

Prior to the Stage 1 audit, you will want to make sure that your organization has defined and implemented the Management System, completed a complete cycle of internal audits, and conducted a management review after the internal audits are complete. It is essential that a complete cycle of internal audits, covering all processes and requirements, and a subsequent management review be conducted prior to the Stage 1 audit occurring. Failure to complete these activities prior to the Stage 1 audit will result in an immediate recommendation of 'not ready' during the Stage 1, and another Stage 1 must be conducted, increasing costs and adding delays. If any of these items are not complete prior to the Stage 1, please contact your DQS Customer Service Representative as soon as possible to delay the Stage 1.

During the Stage 1 audit, the auditor will review the system to see that most, if not all, processes have been defined. There will also be a tour of the facility to help ensure we understand the organization and to help in planning the Stage 2 audit.

At the conclusion of the Stage 1 audit there are a few possible outcomes/recommendations.

- The first is that the organization is ready to proceed to the Stage 2 audit.

- The second is that the organization is not ready. This would then require that the Stage 1 audit is repeated to ensure that the organization is ready before proceeding.

- The third possible outcome is that the organization is ready with concerns. This would allow the organization to proceed with the Stage 2 while noting there are some risks that it would be best to address prior to the Stage 2. Note that this outcome is not allowed for the Aerospace standards.

As there is the possibility, if the system does not show to be ready, that the Stage 2 audit would need to be postponed, it is recommended that the Stage 1 and Stage 2 audits are scheduled more than 1 month apart. Nonconformities are not issued as a result of a Stage 1 audit. There could however be areas of concern that are noted. It is best that these are resolved prior to the Stage 2 audit. In some cases, evidence that they have been addressed may be required. This then provides the best chance of a positive outcome from the Stage 2 audit.

Once it is determined that the system is ready, we will conduct the Stage 2 audit. The Stage 2 audit will be a full system audit which looks at all processes. The processes will be assessed for being defined, implemented, and effective. We will also audit all of the shifts that work is performed on. It is important that all of the processes have been running for some period of time such that there is objective evidence of their implementation to support a registration decision. Having process and procedures without evidence can only result in a failed outcome for the Stage 2 audit. The more evidence in hand, the greater the chances for success during the Stage 2.

At the conclusion of the Stage 2 audit there are a few possible outcomes/recommendation.

- The first is a recommendation for certification. This would be the recommendation if no nonconformities were identified during the audit.

- The second is a recommendation for certification upon successful closure of any nonconformities issued during the audit.

- The third is a recommendation that the system is not ready for certification.

If nonconformities are identified, the audit team will notify you at the time identified and review with you at the closing meeting with a request for corrective action. Upon acceptable responses, the audit will then be sent to the technical review team where an independent decision will be made based on the recommendation of the audit team. We typically are able to complete this review within two weeks of the closure of the nonconformities however, there are times that it could take up to four weeks to complete. Once complete, if the decision is positive, then a certificate is issued and sent to you and you can share that you are a certified organization.

Remote Auditing Tips

Over the past 18 months we have had a lot of experience with remote auditing, and we have learned many things. Some things went right, and some things went not so right. What I want to do in this white paper is make you aware of these things so that you are better prepared for your upcoming virtual / remote audit. I will break them down into office processes and manufacturing processes, as each audit type has its own challenges.

Office processes

Many office processes are easily managed and audited remotely using screen sharing applications, such as: MS Teams, GoToMeeting, Webex, Zoom, etc. All of these applications function similarly, but your team needs to know how to use them. What we have learned is that the management rep has taken the time to know how to use the tool, but many auditees may not have had that much experience with them, especially if they have not been working from home.

Some key points to know:

- The web versions of these tools do not have the same capabilities as the downloaded application. For instance, the web version may not allow the user to share his/her screen. This is critical during an audit.
- The web version may not support sharing control of the keyboard and mouse. It is easier for the auditee to just let the auditor scroll the document on his own than to listen to his/her commands ("scroll up, not so far, scroll down, make it bigger", etc.)
- If you have multiple people in a conference room environment and all are logged into the meeting, only one microphone can be active, otherwise you will have some very annoying interference.
- Also, if you have a group of people in a conference room, they may all be wearing masks due to company policy and some masks really play havoc with the microphone. We may not be able to hear that person at all. Practice this first if that is the plan for the audit.
- If someone plans to use two monitors, they should practice knowing which one is being shared.
- Personnel who will be sharing a variety of documents should "share screen" vs. "share document". This way they can easily toggle back and forth between different documents. If they choose "share document", they have to "un-share" before "re-sharing" to display the next document.

Manufacturing processes

Some of the same apps can be used for the manufacturing portion of the audit, as they all interface with the computer's camera or with an external camera. The audio is probably the biggest challenge with mfg. audits.

Some key points to know:

- For video stability, having the camera on wheels is much better than hand carrying the computer or external camera. Many people will put their computer on a cart and push it to the mfg. area. I have seen others mount an iPad on a rolling tripod. Either method brings stability to the image that the auditor is seeing.
- I have personally experienced body mounted cameras, but those would be fine, as well. Just practice with them. Your local electronics store has many options for you and many price ranges.
- Having the computer on wheels also saves wear and tear on the person holding it. When an auditor goes to the mfg. floor it is usually for an extended time. While the computer only weighs a couple of pounds, it gets really heavy within 20 minutes or so.
- Audio is the big challenge, but a little technology goes a long way. Noise cancellation is the key. Microphones with noise cancellation on your end makes the auditor's life pretty easy. Noise canceling headsets make life easy on the auditee. The full over-ear headsets are the best for noise cancellation in very noisy areas. If mfg. is relatively quiet, there are puck mic/speaker combos with noise cancellation which work nicely and everyone can then hear the conversation.
- WIFI signal strength should be tested in all areas of the plant and signal boosters added as needed.
- The auditor will likely be viewing some records on the mfg. floor. If these are hard copies, practice viewing these with the camera to see how clear it will be.

General

- Testing is key. This is easily done internally and then validated with the auditor. Several standards require a test, but it is a great idea no matter if it is required or not.
- Please have cameras on as much as possible to make the audit feel like an in-person audit.
- At times, WIFI strength may drive you to turn the camera off to conserve bandwidth and that is okay.
- There are two ways to set up the web meetings. Either one day long session or individual sessions. The one long session has flexibility. The individual ones keep the audit on schedule. Personally, I like the flexibility, but either is fine.
- Remember to take breaks to stretch your legs and give your eyes a break from the screen.

CMMC WEBINAR

Our recent webinar discusses the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC,) that will be required throughout the entire supply base. This webinar will help you:

- Understand the background of the CMMC
- Understand the CMMC requirements
- Review examples evidence needed for CMMC audits
- Understand the current status of the CMMC Process soon

The webinar can be found on our website at the link below under the webinars portion of the page.

https://dqsus.com/standard/cmmc/

ISO/IEC 27701:2019 Security Techniques

Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management

In the ISO 27001 series, ISO 27701 standard is for the Privacy Information Management Systems (PIMS). This standard adds additional privacy processing controls to ISO 27001 to create a framework for data protection and privacy.

It is noteworthy that Information Security Management System (ISMS) helps an organization keep their information confidential, accurate and available to those who are authorized to access it. Information security provides the necessary basis for PIMS, which enables an organization to protect the privacy of personal information and prevent unauthorized use or disclosure of such information, in compliance with the regulatory, statutory, and contractual requirements. ISO 27701 certification provides the internationally accepted mark of assurance to an organization that they have taken all the steps to conform to data protection privacy requirements in addition to achieving organization-wide information security.

Why consider ISO 27701 certification? Having certifications for ISO 27001 and 27701 demonstrates to your clients that you have taken the steps to ensure information security and data privacy. These certifications will open opportunities with business partners and show your capabilities regarding the protection of privacy to all stakeholders. There are many benefits to airing this certification.

- Demonstrated Security and Privacy: Compliance with ISO 27701 requires compliance with ISO 27001 first. Together these certifications demonstrate a very rigorous approach to information security and data privacy
- Global recognition: This is a global certification
- Third party Audit: Certification of compliance by a third-party auditor is a trustworthy attestation. GDPR does not have an accredited certification process

DQS Inc. is accredited to provide third-party audits for ISO 27001. Our auditors have experience in auditing this rigorous standards for multiple clients.

The terms used in ISO 27701 standard are defined in ISO 29100. Some of these are listed below since this is relevant to understanding the value added to the organization by certifying to this standard. The tables below show important distinctions regarding the two standards discussed in this article.

PII principal: A natural person to whom the personally identifiable information PII relates. (Clause 2.11)

Personally Identifiable information (PII): Information that can be used to identify the PII principal or is directly or indirectly related to the PII principal. (Clause 2.9)

PII processor: Privacy stakeholder that processes PII on behalf of, and in accordance with the instructions of, a PII Controller. (Clause 2.12)

PII Controller: Privacy stakeholder(s) that determines the purposes and means for processing PII other than natural persons that use the data for personal purposes. (Clause 2.10)

ISO 27701 terminology	GDPR terminology
PII principal	Data subject
PII	Personal data
PII processor	Data processor
PII controller	Data controller

ISO 27001	ISO 27701 Additions
Clauses	Privacy requirements added to ISO 27001 clauses
Annex A controls	Modification of ISO 27001 Annex A controls. Also, additional controls created for privacy
Guidance in ISO 27002	Information added to the ISO 27002 guidance regarding data controllers and data processors

Controller Responsibility	Processor Responsibility
Create Privacy Notices	Processing limitations
Implement mechanisms so PII principals can exercise their privacy rights	Assist with individual rights
Create processor contract requirements	Transfers and disclosures
Privacy by design and default	Subcontractors