POST-WEBINAR DOSSIER

Navigating the Changing

Compliance Landscape in 2020 & Beyond

Updates to PCI-DSS, ISO 27001, NIST 800-53,
NIST 800-171 & the new CMMC

NNT™
SECURITY THROUGH SYSTEM INTEGRITY

Table of Contents

One hour long, power-packed webinar, with insights from 2 eminent speakers from New Net Technologies and Compliance Forge

This webinar was centered around the latest updates in the compliance landscape - PCI-DSS, NIST 800-171, ISO 27001, and the CMMC. We explored compliance standards that impact organizations and introduced security and compliance solutions that enable businesses to be more proactive in their responses.

This webinar also highlights the concept of moving towards a data-centric security model and discusses leading security frameworks and recent changes businesses need to be aware of. Furthermore, it also discusses seven steps towards building an audit-ready CMMC program as well as relevant frameworks that will be important for most businesses in the coming years.

Agenda:

- **Understanding important updates to PCI-DSS, NIST 800-53, NIST 800-171, ISO 27001 and the introduction of CMMC**
- **Receiving guidelines on what businesses should be doing now to be better prepared**
- **Practical tools to help accelerate compliance readiness**
- **Case studies on how NNT achieves compliance**

Tom Cornelius, Senior Partner at **Compliance Forge** & Founder & Contributor at Secure Controls Framework (SCF)

Mark Kedgley is Chief Technical Officer at **New Net Technologies** (NNT)

Expected new versions in 2020/2021 that will significantly impact cybersecurity/privacy programs:

NIST 800-53 R5:

The new version is already in final draft format, and features new sections with a focus on resiliency and will offer guidance to companies looking to recover from cyberattacks that affect the availability of IT assets, such as ransomware or DDoS attacks.

NIST 800-171 R3:

Once the NIST 800-53 R5 comes out, it is expected to cascade down to cause a third, updated release of NIST800-171. It will be tied to NIST 800-171 R5 and will also impact the **Cybersecurity Maturity Model Certification** (CMMC). Right now, it's on version 1.02, which was released in January.

CMMC v1.x (based on NIST 800-171 R3 changes):

The **Department of Defense** (DoD) is set to launch the PathFinder Project, which is essentially a proof of concept to see how well the CMMC is going to be rolled out. It's expected to cause various changes, and it's essential to note that CMMC is missing different components. While there is talk of having reciprocity with NIST 800-171 or Fedramp or other leading frameworks out there, this is not possible in its current state. CMMC covers 110 core Controlled Unclassified Information (CUI) controls but completely neglects non-Federal organizational controls that are a requirement in NIST 800-171.

ISO 27001 / 27002:

The new version is likely to be launched in 2021 and is expected to be updated with a modern risk approach to integrity, safety, confidentiality and availability.

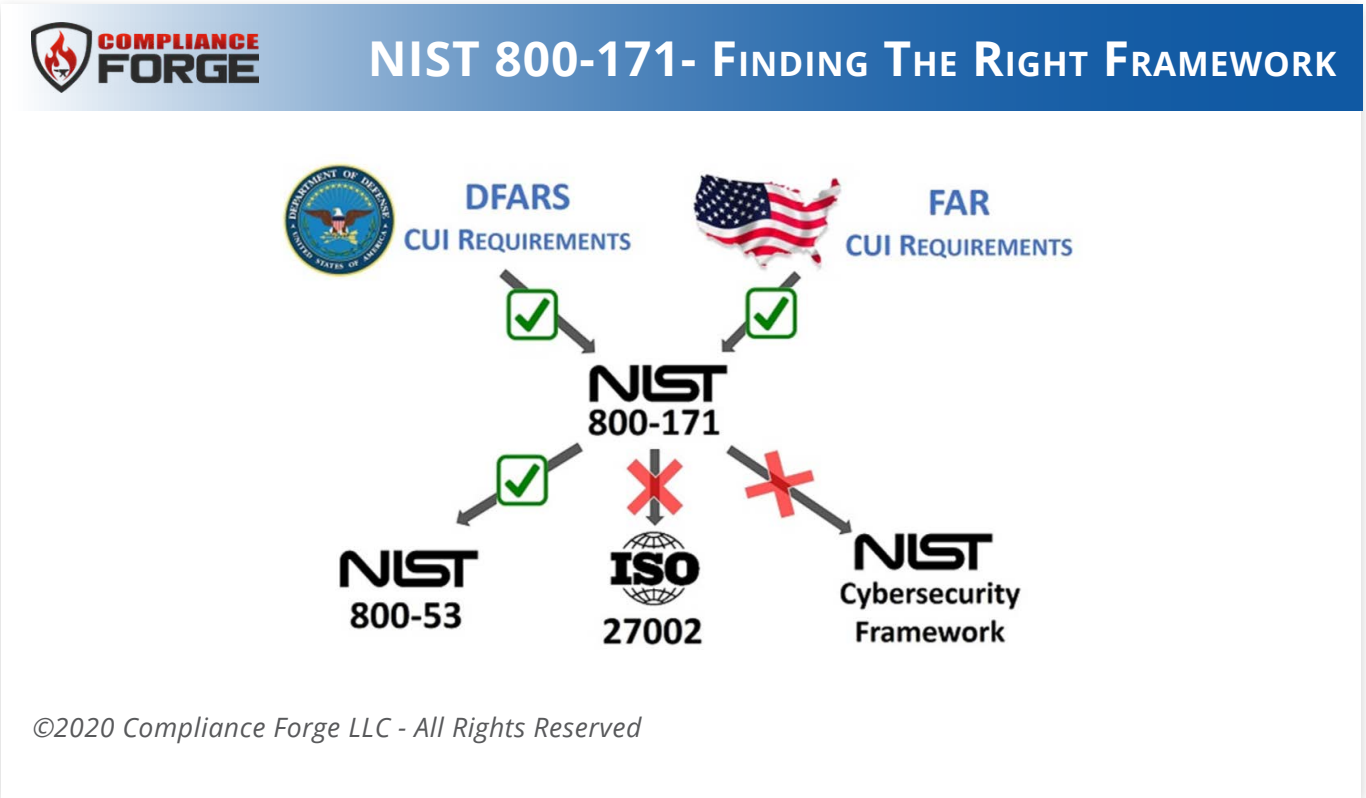
California Consumer Privacy Act (CCPA):

The CCPA went into law on January 1st, but it is under revision for future versions.

The biggest impact is going to be on NIST 800-53, with a more moderate impact on ISO. An interesting implication is that NIST 800-171 and the CMMC will also be affected. Right now, these are focused on DoD contractors and its supply chain, but it is widely expected to roll out more to the federal government. Once this does happen over the next couple of years, it should then turn into a US national standard, a minimum set of requirements that has to be addressed.

PCI DSS v4

PCI DSS has been around the longest and is probably the most widely implemented. It is a truly global and truly enforced standard. While PCI DSS 4.0 is being billed as a major version change, the 12 core requirements and the sub-requirements we know and love remain. The update is determined to be more flexible and more open to new technologies.



DFARS and FAR drive requirements

DFARS and FAR contractual clauses define compliance requirements, which mostly comprises cybersecurity controls that federal contractors have to meet in order to get and keep the contract. While DFARS (**Defense Federal Acquisition Regulations**) is focused on defense contractors, FAR (**Federal Acquisition Regulations**) focuses on any US government contractor.

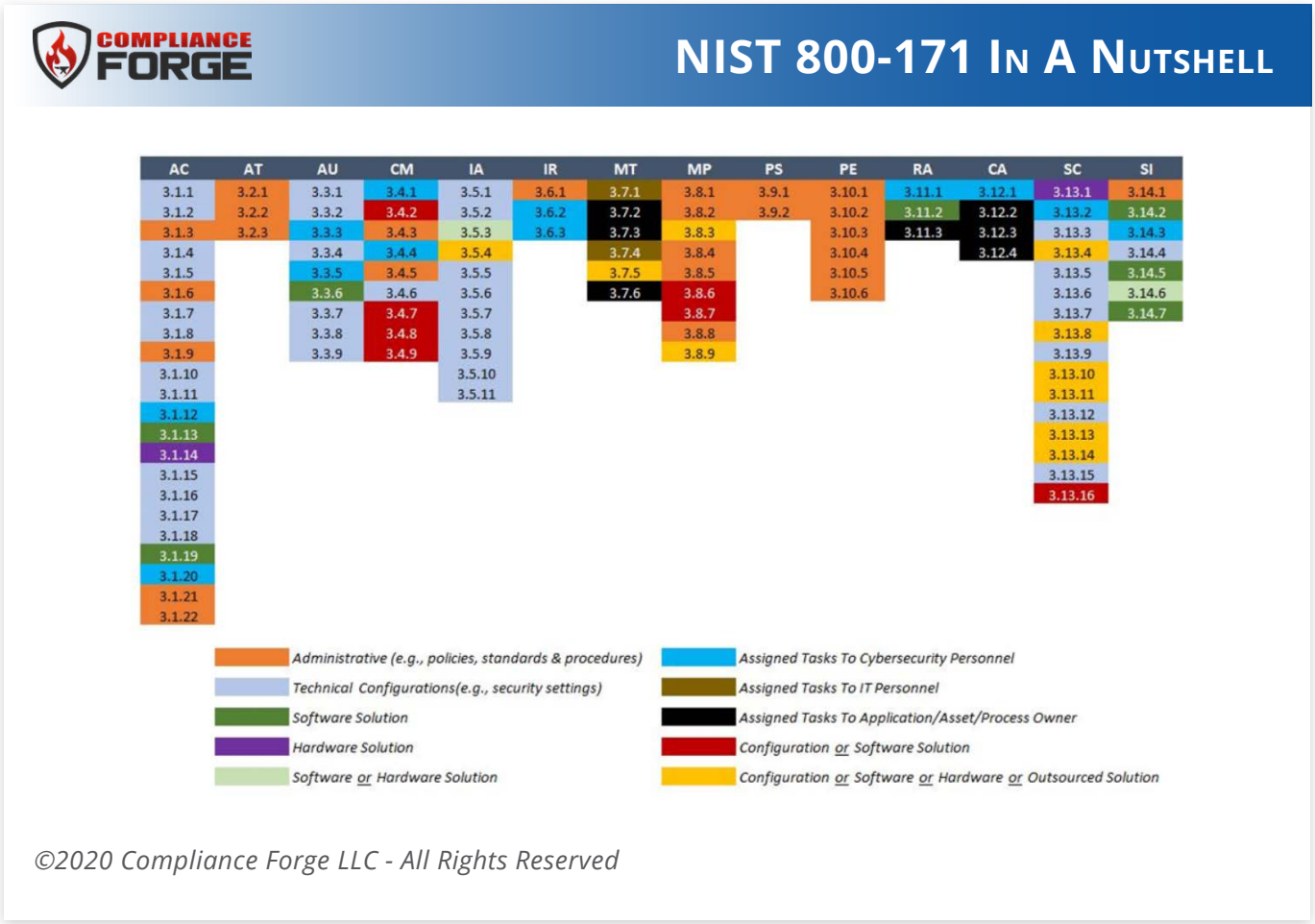
Right now, FAR only has 15 basic cybersecurity requirements but it is clear that in the future FAR will also adopt NIST 800-171. This means that eventually, the DOD and US federal government will have a common cybersecurity playbook, instead of operating with two different sets of requirements.

To understand the relationship between NIST 800-53 and 171, Appendix E of 800-171 provides a complete listing of the 'Moderate Baseline' from 800-53 and the rationale for how this has been tailored to produce the 800-171 control set.

The tailoring rationale tags each of the 800-53 controls as either

NCO	Not directly related to protecting the confidentiality of CUI
FED	Uniquely federal, primarily the responsibility of the federal government
NFO	Expected to be routinely satisfied by non-federal organizations without specification
CUI	The CUI basic or derived security requirement is reflected in and is traceable to the security control, control enhancement, or specific elements of the control/enhancement

There are 110 CUI requirements and 62 NFO requirements. NFO requirements include policies, training records, and other required elements that must be in place before shifting focus to more pertinent security requirements that will help protect this controlled and classified information.

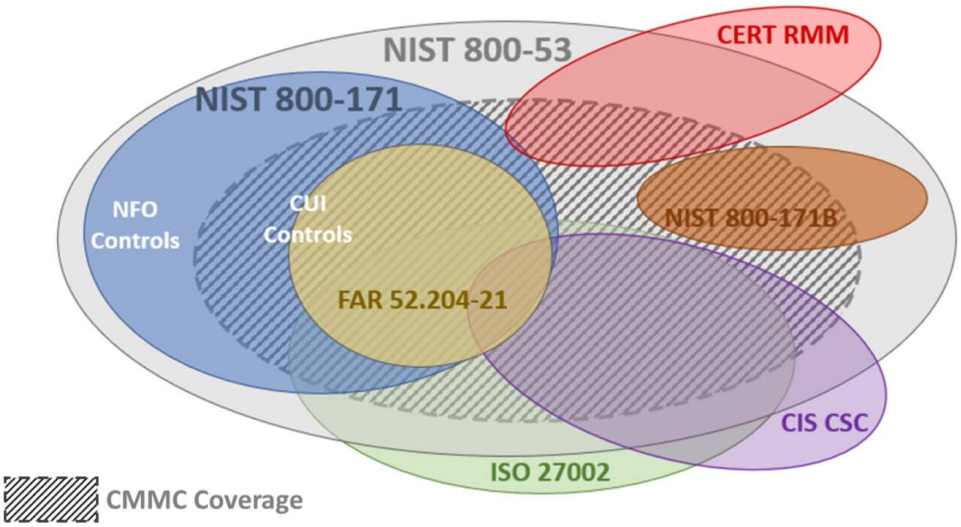


NIST 800-171 in a nutshell

While NIST 800-171 is expected to be a hardcore set of cybersecurity requirements and is generally considered to be a very big roadblock, it really is just a set of good IT hygiene practices, comprising change control, access control and vulnerability management/ patching.

Most of these activities are assigned to IT teams rather than the core cybersecurity team. Of course, this depends on the maturity level of your organization and whether you have a dedicated IT and security team or even specializations within these.

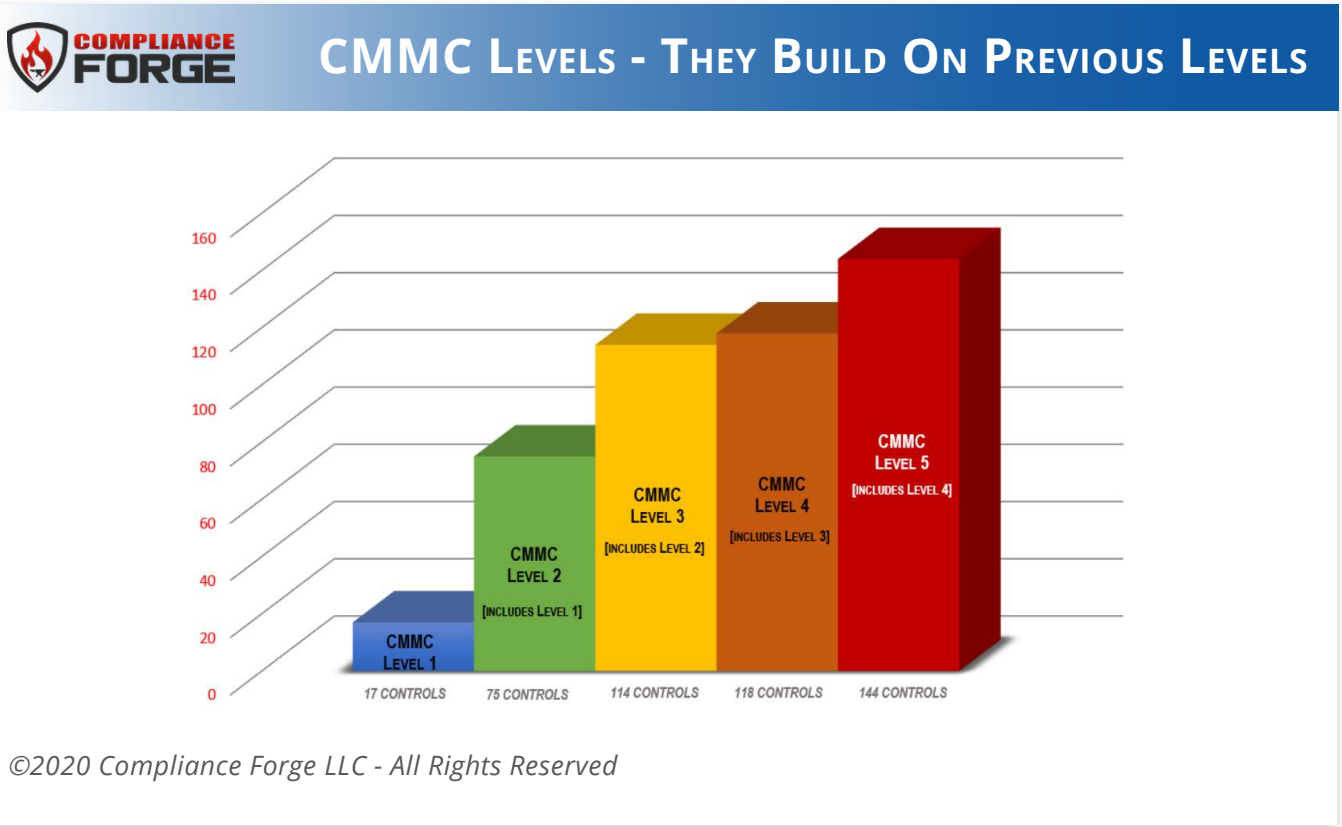
CMMC Is Far More Than NIST 800-171



CMMC is far more than NIST 800-171

CMMC is essentially a hodgepodge of various frameworks.

For the average company that stores transparency processes, they have 130 requirements. 110 of those are directly out of NIST 800-171, but when you start looking at data requirements that are out there, you've got FAR, which is basically Level 1. You've got ISO 27022, CIS CSC, NIST 800-171 Bravo (which is essentially a high baseline from NIST 853). There is also CERT RMM which is a resiliency type of requirement.



CMMC Levels – How do they build on previous Levels?

There are currently five different levels within the Maturity Model. Each incremental level builds on the previous levels. In other words, every control in Level 1 is included in all the other levels, with more controls added for each progression to the next level.

However, this also gives rise to a certain level of misunderstanding - often leading businesses to think that if they're Level 1 now, they will be Level 2 next year and so on and so forth.

In fact, the different levels are aligned to match business practices. For example, if you're saying, a janitorial services company or a landscaper, who happens to have some type of federal contract information as a part of that contract, you're likely to be at Level 1. Going forwards, if your business model continues unchanged, and you still won't be processing, transmitting or handling any more CUI, your Level 1 maturity will still be just as relevant going forwards too.

In fact, most businesses that are Level 1 will stay Level 1.

There is conflicting guidance from DoD and CMMC

A Level 2 is supposed to be a stepping stone to a step 3. However, there is no clear definition as to what Level 2 and Level 4 look like at the moment.

A Level 3 is essentially the middle and comprises businesses that store, transmit or process CUI or MSPs that work on behalf of a client and have access to admin rights.

There is no clear guidance so far from the AB or DoD on what will constitute an organization to be a Level 4 or Level 5. But when you look at the different practice requirements, it's progressing into protection against advanced persistent threats.

Level 5 will most likely comprise major defense contractors, for example, Lockheed Martin or Boeing.

Out of approximately 300,000 companies that are supposedly going to be in scope for CMMC, the vast majority will be Level 1. The rest are going to be Level three with a small minority at Level 4 or Level 5.

COMPLIANCE FORGE

CMMC Level 1

CMMC LEVEL 1 = Federal Acquisition Regulation (FAR) 52.204-21

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

These controls are primarily FAR Cybersecurity requirements. While practices are expected to be performed, process maturity is not addressed at CMMC Level 1.

CMMC LEVEL 1

Level 1 is essentially a baseline for any US government contractor. The DoD took the 15 cybersecurity requirements from FAR and translated those into 17 requirements that already directly link into NIST 800-171.

COMPLIANCE FORGE

CMMC Level 2

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

For process maturity, a CMMC Level 2 organization is expected to establish and document standard operating procedures, policies, and strategic plans to guide the implementation of their cybersecurity program.

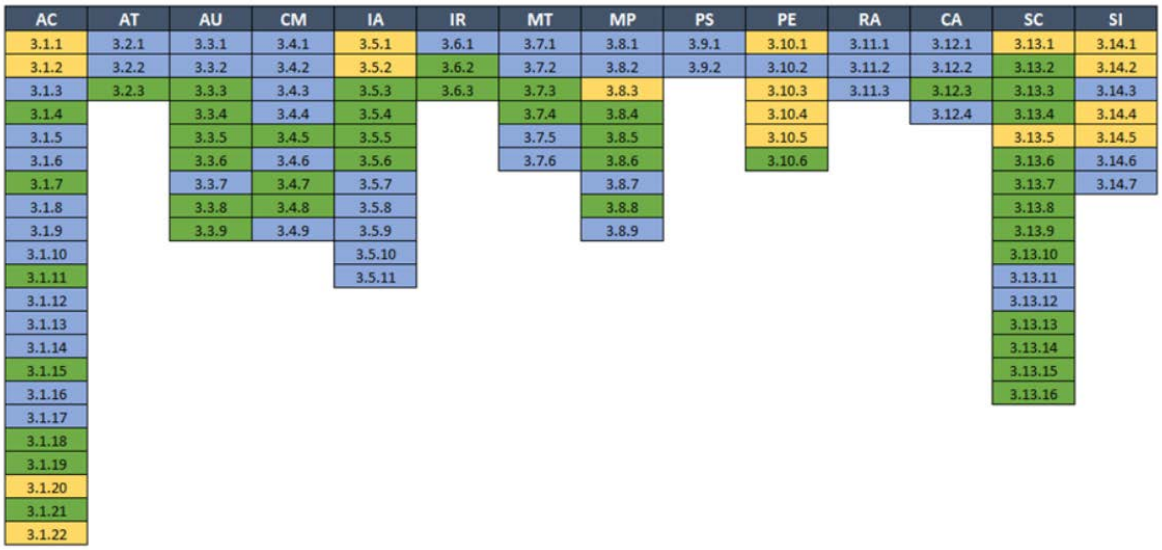
CMMC LEVEL 2

CMMC Level 2 is a little more than half of NIST 800-171 with 75 controls. Interestingly, for process maturity, a CMMC Level 2 organization is expected to establish and document standard operating procedures, policies, and strategic plans to guide the implementation of their cybersecurity program.

While Level 2 is slightly more mature, it is not the entire set of requirements, because Level 1 and Level 2 are focused on companies that only store, transfer, process federal contract information, not CUI. CUI is in-scope only when you get to Level 3, 4, and 5

COMPLIANCE FORGE

CMMC Level 3



AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

For process maturity, a CMMC Level 3 organization is expected to adequately resource and review activities adherence to policy and procedures, demonstrating management of practice implementation.

CMMC LEVEL 3

CMMC 3 is supposed to cover all 110 CUI controls from NIST 800-171, but the control count is 114, so it is a little more than just NIST 800-171.

For process maturity, a CMMC Level 3 organization is expected to adequately resource and review activities adherence to policy and procedures, demonstrating management of practice implementation.

Of the 110 controls, everything is addressed from the perspective of NIST 800-171. But there are an additional 20 controls that are linked back to NIST 800-53.

So, it is essentially NIST 800-171 CUI controls + 20 additional controls.

COMPLIANCE FORGE

CMMC Crosswalk

DoD Cybersecurity Maturity Model Certification (CMMC) v0.6 *[note - this version focuses on CMMC Levels 1-3]*				CMMC Level Requirement					Crosswalk / Mapping							
Domain	Capacity	#	Practice						FAR 52.20	NIST 800	NIST 800-	CERT RMM	ISO 270	NIST CS	CIS v7	Secure Contro
Access Control (AC)	**C001** Establish system access requirements	AC-C001-P1001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	x	x	x	x	x	(b)(1)(i)	3.1.1	AC-2 AC-3 AC-17		6.2.1 6.2.2 9.1.2 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 9.4.4 9.4.5 13.1.1 13.2.1 14.1.2 14.1.3 18.1.3			IAC-15 IAC-20 NET-14
		AC-C001-P1005	Provide privacy and security notices consistent with applicable Federal Contract Information (CFI) rules.	N/A	x	x	x	x		3.1.9	AC-8		9.4.2			SEA-18
		AC-C001-P1006	Limit use of portable storage devices on external systems.	N/A	x	x	x	x		3.1.21	AC-20(2)					DCH-13.2
	C002 Control internal system access	AC-C002-P1002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	x	x	x	x	x	(b)(1)(ii)	3.1.2	AC-2 AC-3 AC-17		6.2.1 6.2.2 9.1.2 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 9.4.4 9.4.5 13.1.1 13.2.1 14.1.2 14.1.3 18.1.3			IAC-15 IAC-20 NET-14
		AC-C002-P1007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	N/A	x	x	x	x		3.1.5	AC-6 AC-6(1) AC-6(5)		9.1.2 9.2.3 9.4.4 9.4.5			IAC-21 IAC-21.1 IAC-21.3
		AC-C002-P1008	Use non-privileged accounts or roles when accessing nonsecurity	N/A	x	x	x	x		3.1.6	AC-6(2)					IAC-21.2
		AC-C002-P1009	Limit unsuccessful logon attempts.	N/A	x	x	x	x		3.1.8	AC-7		9.4.2			IAC-22
		AC-C002-P1010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	N/A	x	x	x	x		3.1.10	AC-11 AC-11(1)		11.2.8 11.2.9			IAC-24 IAC-24.1

FREE DOWNLOAD = www.cmmc-compliance.com

CMMC Crosswalk

This covers the domains, capacities, and practices from CMMC v0.6 that was released earlier this month, which focuses on CMMC Levels 1-3. The next version will fill in details around CMMC Levels 4-5.

Compliance Forge built a framework where all practices can be seen and what processes are mapped into different frameworks.

FREE DOWNLOAD

This CMMC crosswalk is available at CMMC-Compliance.com.

Navigating PCI DSS 4.0 with Mark Kedgley, CTO, New Net Technologies

PCI DSS 4.0 - Objectives

The PCI DSS 4.0 update is determined to be more flexible and more open to new technologies. There is new language and intent around the concept of 'Customized Validation' which gives organizations greater license to meet the intent of the requirements. If your business is a heavy user of cardholder data then you will already have years of being involved with QSA's and getting reports on compliance.

- The PCI DSS is presented using 12 different requirements and compared to something like NIST 800-53, is a relatively succinct security controls mandate
- It is focused primarily on protecting cardholder data, unlike the more comprehensive coverage of the CIS Controls
- The current 3.2.1 version of the standard enables businesses to leverage advances in technology, embrace the updated controls, and be better equipped to handle new threats
- Another major shift for PCI DSS 4.0 is a far greater emphasis on operating security controls continuously, an approach squarely in line with the NNT SecureOps™ approach. The concept of continuous change control is always a foundational security control that features in all security standards and frameworks.

PCI DSS 4.0 - 18-month transition period

It takes a long time to go through an update – at least two rounds of Request for Comment and discussion, then the supporting materials need to be produced.

This is why the implied flexibility of the new version may prove so valuable. In the past, new innovations, like P2PE, have promised brand new technological solutions for descoping devices, but have been delayed by the need to be properly ratified, followed by a lengthy update period for the security standard.

The new flexible 'Customized Validation' should help in this respect - to look beyond the traditional compensation controls and more flexibility.

The PCI DSS v4.0 standard is scheduled for completion six months prior to the release of the supporting documentation, training, and program updates that are required to support the use of PCI DSS v4.0. The PCI DSS v4.0 standard will, therefore, be available for 2 years prior to the retirement of PCI DSS v3.2.1.

The bottom line is - there is plenty of time to get up to speed.

PCI DSS 4.0 - What do we know?

Broadly the standard remains the same because security controls are largely still the same, but the overall themes are to embrace new technologies where they improve card data security and to inspire merchants to raise the bar.

In some respects, it's no different to the NIST 800-171 and CMMC situation where you have an authority trying to empower and encourage industry to take up cybersecurity responsibility. PCI has the advantage in that there is an established auditor community with years of experience in operating the PCI DSS.

What do we know so far about PCI DSS 4.0?

- MFA (Multi-Factor Authentication) is being promoted, at least in part because it is now so readily available and a relatively straightforward add-on. Software tokens on a smartphone deliver multifactor authentication technology to the highest level of security at minimal expense.

- However, it is also a response to recent trends in breaches. A significant proportion of breaches involve the use of stolen credentials and the most common variety of malware is password dumpers. In the recent Verizon 2020 DBIR, 37% of breaches involved the use of stolen credentials. It's a serious security threat to target and one where solutions are within reach.

- Other changes are intended to give the PCI DSS longevity and stability. Every time the standard changes, it's a long and laborious process for everyone involved, and confusion reigns. Tokenization and P2PE both took years to be accepted as valid de-scoping technologies, but until the PCI SSC did so, these technologies, that seemed to be game-changers, weren't approved.

- The final point is to really advance the effectiveness of the Security Standard by getting organizations to progress their adoption of security controls – how many times have we heard 'checkbox compliance'? This cliché is still too often the reality, with gesture security being too often where the bar is set. The promotion of Business as Usual incorporation of continuous PCI Processes and procedures is the only way that cardholder data is properly protected.

PCI DSS 4.0 - BAU

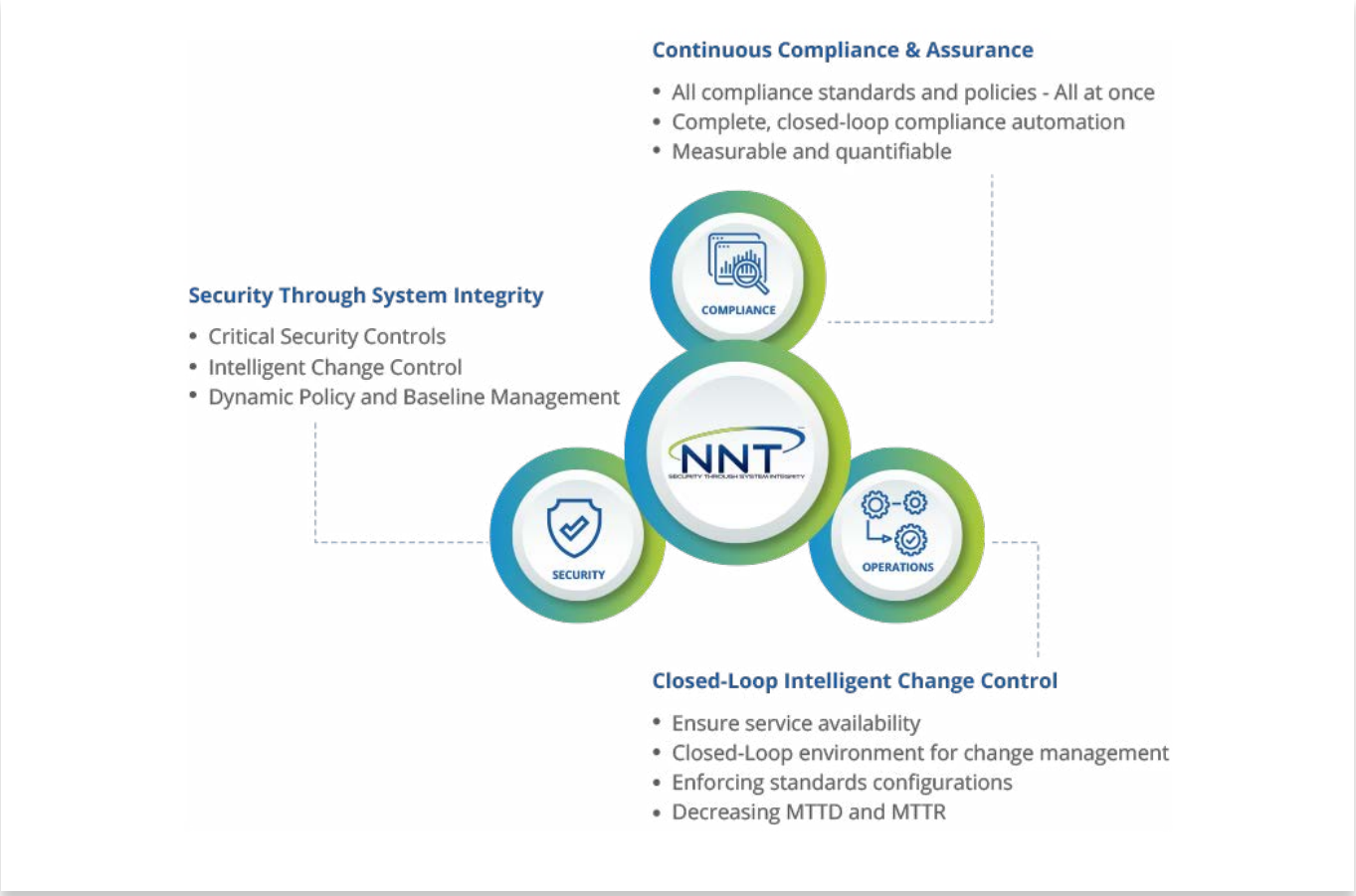
Appendix 3 requirements of the current DSS version used to only be applicable to anyone processing the largest volumes of card data. A move to make these 'advanced' requirements now the norm aligns with what was mentioned earlier about the CMMC, in that it is still necessary to beg/plead with many organizations to properly embrace and embed secure into their operational procedures as Business as Usual.

This is precisely why NNT emphasize SecureOps™ as the only way to master security, and this is echoed in the contents of Appendix 3 regarding 'verifying PCI DSS requirements for every change, and building this into change management processes.'

SecureOps™ is short for Secure Operations. It includes a combination of the essential, foundational security controls as prescribed by all leading security frameworks such as The CIS and NIST with the operational discipline of change management and the innovation of change control pioneered by NNT.

By ensuring the basic and essential security controls are in place, combined with the ability to validate the safety of all changes, organizations can prevent and protect against cyber-attack while improving IT Service Delivery quality.

SecureOps™: Audit, Configure and Secure your entire network



NNT SecureOps™ in lockstep with BAU

The crucial difference with SecureOps™ is that there is this highly automated, comprehensive visibility, analysis, and validation of change – Change Control.

It uses the 'business as usual concept' to continually check if the basic and essential security controls are being operated. This, combined with the ability to validate the safety of all changes, enables organizations to prevent and protect against cyber-attacks while improving IT Service Delivery quality.

It's a genuinely new and effective way of automating security controls exactly in line with the true intent of the PCI DSS. NNT SecureOps™ integrates a portfolio of technologies to automate change control and correlates knowledge of planned changes with detected change activity from the estates to isolate unexpected changes and throw the spotlight onto breach activity when it does happen.

How NNT Helps with Continuous Compliance & Assurance

- Built-in compliance policies – Compliance policies and regulations change constantly. NNT has predefined policies that can be applied in a matter of seconds to determine if systems are in compliance
- Complete, Closed-Loop Compliance Automation – Automate the process of compliance validation and provide descriptive details on how to rectify if compliance drift has occurred
- Give management and auditors the confidence they need with reports that can be generated within minutes that show evidence of compliance testing, results and remediation
- Get total visibility into all changes and detect and validate changes – Track every change made across the IT environment and expose unauthorized changes through reconciliation with expected changes
- Reduce the cost of compliance with automation – Streamline the audit process by removing the need for internal audit staff to spend countless hours gathering evidence to present to external auditors with automation. By enabling workflow automation that monitors and tracks security risks, organizations know they are in compliance in real-time

Continuous Compliance and Assurance is an ongoing process of proactive risk management that delivers predictable, transparent, and cost-effective results to meet information security goals.

NNT Capabilities	PCI-DSS	NERC CIP	SOX	HIPAA	NIST 800-53	NIST 800-171	CMMC	MAS TRM	IRS 107	20 CSC	COBIT	ISO 27001
FIM (Intelligent Change Control)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Continuous Configuration Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hardware & Software Asset Inventory	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Vulnerability Assessment (Unlimited IPs)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audit Log Analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remediation	✓	✓	✓		✓	✓	✓					

Contact us

US - (844) 898-8362, UK - 01582 287310

info@nntws.com

www.newnettechnologies.com

Schedule a free consultation | **Request a Demo**