Defence Cyber
Protection Partnership

Defence Cyber Protection Partnership

Cyber Security Model

Guidance for adopting other standards to meet requirements of DefStan 05-138

July 2019

Executive Summary

1. There has been a desire from the industry for adopting internationally recognised standards such as ISO27001, NIST 800-171, NIST 800-53, CCM and others as alternatives to DCPP's Cyber Security Model (CSM). This is due to some organisations having to comply with other standards to meet regulatory, industry or legal requirements or having already adopted them as part of their Governance, Risk and Compliance (GRC) programmes.

2. A mapping exercise of ISO 27001 and NIST 800-171 against DefStan 05-138 has concluded:

a. Standards and frameworks vary in terms of requirements they address: Some address organisational governance, some specify technical controls while others cover mixture of the two.

b. The scope of coverage and application of the standards vary, and organisations are free to apply them from a limited scope to the entire organisation. ISO 27001 is a very good example of this approach.

c. The standards and frameworks take generic approach to applying controls, whereas DefStan 05-138 takes a risk-based approach.

d. There are controls from other standards that will meet requirements of DefStan 05-138 controls even if the entire standard cannot be substituted as an alternative.

3. Therefore, adopting a standard such ISO 27001 or NIST 800-171 will assist in achieving elements of requirements within DefStan 05-138. A security professional should be able interpret the intention of DefStan 05-138 requirements and identify the controls from other standards that would meet those and address the remaining controls separately.

4. This approach applies to Low, Moderate and High Risk Profiles that include extra controls building on the baseline requirement of Cyber Essentials Plus. The Very Low Profile still requires Cyber Essentials scheme.

The **recommendation** for Contracting Authorities is to continue to request responses to Suppliers Assurance Questionnaire (SAQ) to assess the compliance of a supplier against a risk profile. A supplier who has adopted other standards should be able to meet varying levels of DefStan 05-138's requirements depending on the scope and nature of the adopted standard. They will still be required to address the remaining controls of DefStan.

Key documents

5. The key MOD policy document which support CSM process is DEFSTAN 05-138[1]. Key to the CSM is DEFCON 658 which is a contract condition.

Background

6. There is an industry wish for mapping widely adopted, internationally recognised standards such as ISO20071 as a substitute for DefStan 05-138.

7. The DefStan 05-138 under Cyber Security Model (CSM) within DCPP takes a risk-based approach by defining applicable controls. Many of the standards and frameworks take a generic approach to specifying requirements and controls for information and cyber security. Some standards cover more governance aspects of information security while others concentrate on technical controls. Some are very prescriptive while others outline high level requirements. Several standards have attestation process to declare compliance through independent assessors whereas many others do not have an assessment process. Many standards are applied with varying scope

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652597/20171016-Defence_Standard_05-138_Iss_2.gov.uk.pdf

and the adopting organisations are free to apply them to the entire organisation or a small department.

8. Therefore, although it is possible that controls from one standard will map to those within DefStan 05-138, there is not a one for one equivalence. We will illustrate this by using a standard, that has received a high level of interest for mapping within the industry, namely, The NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems.*

Comparison of DefStan 05-138 and NIST 800-171

9. The result of our mapping of DefStan 05-138 requirements to NIST 800-171 is outlined in the following table:

DEFSTAN 05-138 Control	NIST 800-171 Mapping	Adopt without significant impact?
L.09	3.8.7	Yes
L.10	3.12.4	Yes
L.11	3.4.1	Yes
L.13	3.5.2	Yes
L.16	3.6.1 and 3.6.2	Yes
M.01	3.6.2 and 3.11.1	No
M.03	3.11.1 and 3.12.1	Yes
M.05	3.13.1 and 4.13.4	No
M.07	3.14.1 and 3.14.3	Yes
M.12	3.13.6 and 3.14.6	No
M.13	3.5.10	Yes
M.14	3.9.1	Yes
H.07	3.13.6 and 3.14.6	Yes
H.08	3.5.3 and 3.7.5	No
H.09	3.13.2	Yes
H.12	3.6.1	Yes

10. In order to illustrate the mapping challenge, we will use some examples that can be easily adopted and other examples that do not map:

DefStan 05-138 Requirement	Requirement	Required Response	NIST 800-171 control	NIST Control Description	Conclusion
L.09	Does your organisation have a policy to control the exchange of information via removable media?	We assess the risks of the use of removable media and are managing it with a Policy that is documented and maintained.	3.8.7	Control the use of removable media on information system components	Adopting this control would make no significant difference to DefStan 05-

					138
L..10	Does your organisation have an approved Information Security Policy in place?	We have a documented and maintained policy that considers as a minimum the following areas: Information Risk Management Regime, Network Security, User Education and Awareness, Malware Prevention, Removable Media Controls, Secure Configuration, Managing User Privileges, Incident Management, Monitoring and Home & Mobile Working (and physical security).	3.12.4 (110th requirement)	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Adopting the NIST control may require the Supplier Cyber Protection tool guidance to be modified a little but could be adopted as there is no significant difference
M.01	Does your Organisation have a policy to ensure regular, formal information security related reporting?	Yes, regular formal reporting arrangements are in place at board level.	3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization	Adopting these two controls in place of M.01 would not be sensible as 3.11.1 is mapped to a 'High' control (H.11) so adopting would increase the 'difficulty' of the DefStan 'Moderate' level. However, it is technically possible to adopt the NIST controls so long as a control that is part of "High" profile is moved to "Moderate".
			3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	

M.05	Does your organisation have a policy for data loss prevention?	We have policy that defines what information may be released and implement controls and monitoring to control the flow of data within the network and detect the unauthorised release of sensitive information.	3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	The two NIST controls referenced include elements of controls from DefStan 'High' (H.07, H.09 and H.10) so adopting would increase the difficulty of the 'Moderate' level
			3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	
M.07	Does your organisation manage vulnerabilities for which there are no countermeasures?	We subscribe to a vulnerability alerting service, formally review alerts and mitigate as a matter of priority).	3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	The NIST controls could be adopted without any significant impact to the DefStan other than increasing the control count.
			3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	

11. From the above selected examples, it is evident that there are a few possibilities:

a. Some DefStan 05-138 requirements have equivalent NIST 800-171 controls.

b. Some DefStan 05-138 requirements require more than one NIST 800-171 control.

c. Trying to adopt some controls from NIST 800-171 to address DefStan 05-138's requirements for a certain profile may exceed the requirements of that profile and thereby increasing the difficulty unnecessarily.

d. Some DefStan 05-138 requirements do not have equivalent control or combination of controls within NIST 800-171.

12. In conclusion, it is not possible to directly map NIST 800-171 controls to DefStan 05-138 in its entirety to satisfy the full DefStan 05-138 requirements.

Guidance and Recommendation

13. The previous section has concluded that it is hard to point to an alternative standard is equivalent to DefStan 05-138. Some of the individual controls are roughly equivalent and some are

not. However, we recognise that organisations may have invested in meeting other standards and should not have to start from scratch.

14. For example, if an organisation has implemented the following NIST 800-171 controls:

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

and

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote sessions.

it would then meet the H.08 requirement within High profile of DefStan 05-138:

H.08 Undertake administration access over secure protocols, using multifactor authentication.

As the combination of those NIST controls 3.5.3 and 3.1.13 will meet the requirements of H.08.

15. Using another example, DefStan 05-138 for Moderate profile requires:

M.12 Define and implement a policy to control remote access to networks and systems.

There are no equivalent control(s) within NIST 800-171. However, if the controls

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

and

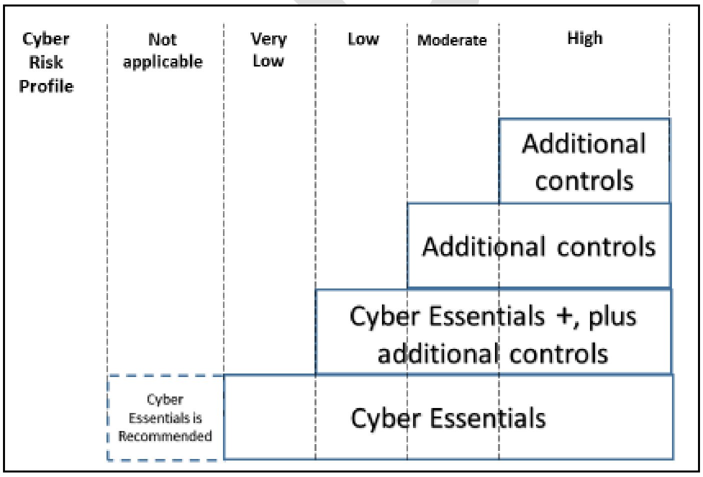
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

are implemented, they would meet the requirement M.12 even if the combination exceeds the intention of M.12 and may even address requirements of DefStan's High profile. However, neither control by itself would meet the intention of M.12.

16. There are many more examples like the ones illustrated here. Therefore, it is possible for a security professional to interpret the intention of DefStan's requirements and identify already applied controls from other standards that would meet the intention. This will enable them to select the appropriate response with the Supplier Assurance Questionnaire (SAQ). Many DefStan 05-138 requirements can be met using this approach. Any remaining requirements should be addressed.

Recommendations

17. The risk profile Very Low requires Cyber Essentials. Other risk profiles require Cyber Essentials Plus, as a baseline, plus other controls where these recommendations are applicable.



Contracting Authorities

18. MOD or higher tier suppliers should continue to use Supplier Assurance Questionnaire (SAQ) for assessing a supplier against a risk profile.

19. They should encourage their suppliers to avoid quoting a standard they follow within a CIP (Cyber Implementation Plan) without attempting to answer SAQs.

Suppliers

20. The suppliers who have adopted (or planning to adopt) other standards should interpret the intention of DefStan 05-138's requirements and could respond positively within the SAQ when there are equivalent controls or combinations of controls as described above, ensuring the scope is applicable.

21. Suppliers should avoid simply stating that they have implemented another standard within a Cyber Implementation Plan (CIP) without answering the SAQ. This will save time and effort for the contracting authority and will also enable the suppliers to reuse SAQ for future contracts.

END