PIM Form Scoring

Page Contents

Jump to...

M Form Scoring

e

Once a form is submitted by a Supplier in PIM, form feedback is generated based on the Supplier's responses. For most forms, a score or other quantitative results are returned as part of the feedback. These scores, or feedback, can be seen:

- In the right-hand section of the **Form Detail** page for the submitted form
- In the **Feedback Report,** available to download as a PDF via the **Reports** drop down menu on the Form Detail page

The sections below provide additional information on scoring or feedback provided for each PIM form.

NIST SP 800-171 Scoring

There are two main percentage values reported as feedback for a submitted NIST form:

- **Implemented + Approved**: This is the percentage of the controls marked as **Implemented** or **Approved Exception by DoD)** by the Supplier.
- **Implemented + Approved + Addressed**: This is the percentage of the controls marked as **Implemented**, **Approved Exception (by DoD)**, and **A ddressed with SSP & POAM** by the Supplier. It is the percentage of all controls that did not have a response of **Not Implemented**.

In addition, for each separate control family, the count for each response categories displays: Implemented; Addressed with SSP & POAM; Approved Exception (by DoD); Not Implemented. Also, if the supplier has met 100% of the controls in that family, a progress bar displays as green for the control family, otherwise anything below 100% is shown as red.

An **Estimated Completion Date (ECD)** value also displays on the Form Detail page of a completed form, if the date exists. This is the date in which the organization input it would implement all controls for which it currently has **Addressed with SPP & POAM**, and therefore has not yet implemented.

Cyber Security Questionnaire Scoring

A submitted Cybersecurity Questionnaire provides two main scores:

- **Overall Score**: The score is a simple average of all control activities across all capability levels and gives credit for implementing individual control activities within each control family.
- **Capability Score**: This score indicates the current Capability Level (0-5), and also shows how many of the controls to obtain the next level have been met. The Capability Score's last two digits (after the decimal point) indicate how close in percentage the Supplier is to achieving the next Capability Level.

The table below shows each Capability Level that exists for the Cybersecurity Questionnaire, as well as the score range and description for each of level.

Capability Level	Score Criteria	Description
Level 5	5.00	Cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented and optimized on an ongoing basis
Level 4	4.00-4.99	Cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented
Level 3	3.00-3.99	Solid performing cyber risk management program; strong protections have been implemented; Advanced threats are understood and taking steps to address with specific controls; Additional risk mitigations are likely needed to protect against advanced attacks
Level 2	2.00-2.99	Moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information.
Level 1	1.00-1.99	Basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented.
Level 0	0-0.99	Red No or minimal cyber risk management program; significant cyber protections are lacking

---

Conflict Minerals Reporting

Though this form does not have a numerical score or any derived counts or percentages as part of the form's feedback response, the Feedback Report for this form does contain all responses to the questions within the report.

Cyber Supply Chain Risk Management (C-SCRM) Scoring

The score for this form is derived as a sum of the points given for each question's selected response per the following point values:

- Yes - Fully = 10 points
- Yes - Partially = 5 points
- No = 0 points.

The total (maximum) possible points for this form is 180.

Concise DFARS / DFARS 252 CS

DFARS 252 CS has three values reported as feedback:

- **Compliant**: This is a Yes/No indicator of if the NIST 800-171 requirements have been implemented or not by the organization which submitted the form.
- **Sharing**: This is a Yes/No indicator of if the organization is sharing Controlled Unclassified Information (CUI)/Covered Defense Information (CDI) with its suppliers or subcontractors.
- **Flowdown**: This a Yes/No indicator of if the organization is flowing down the DFARS 252.204-7012 clause to its suppliers or subcontractors

If no CUI/CDI is handled by the organization, the feedback just indicates this as **No CUI.**
How useful was this content?

Your Rating: Results: 7 rates