i2ACT CMMC | NIST 800-171 Software Features

May 26 | V8

Features	i2ACT CMMC L1 | FAR	i2ACT CMMC L2 | NIST 800-171
CMMC | NIST | FAR	**FAR | CMMC Level 1**	**NIST 800-171 | CMMC Level 2**
Cyber Security Standards	**FOUNDATIONAL**	**ADVANCED**
DOD CMMC version 2.0	Level 1 – 17 Practices	Level 2 – 110 Practices
NIST 800-171 Rev 2	17 Requirements	110 Requirements
NIST 800-172	No	No
NIST 800-53 Rev 4, Non-Federal Organizations (NFO) only	61 NFO controls	61 NFO controls
NIST 800-53 Rev 5	No	No
FAR/DFARS Compliance	FAR 52.204-21 and DFARS 252-204-7012	DFARS 252-204-7012
Capabilities | Functionality		
Assessments at Practice and Objective Levels (1)	Yes	Yes
Supplier Performance Risk System (SPRS) Scoring (2)	N/A	Yes
Standard Assessment Guides at your Fingertips	CMMC AG, NIST 800-171A	CMMC AG, NIST 800-171A
Ability to Create Custom List of Remediation Actions (3)	Yes	Yes
i2 Suggested Remediation Actions as an Upgrade (over 400) (3)	Yes	Yes
Evidentiary Artifact Capture, Linking and Storing (4)	Yes	Yes
Plan of Actions & Milestones (POA&M) Excel Export (5)	Yes	Yes
Baseline Selection and Tailoring	No	No
i2 Organization Defined Parameters (ODPs) Identified at the Practice Level (6)	Yes	Yes
Educational Resources (7)	Yes	Yes
Reporting | Progress Status Notification		
Assessment Reports with Options to Select Controls & Objective Conformity	Yes	Yes
DoD SPRS Scoring Report	Yes	Yes
Remediation Action Report	Yes	Yes

Features	i2ACT CMMC L1 | FAR	i2ACT CMMC L2 | NIST 800-171
CMMC | NIST | FAR	**FAR | CMMC Level 1**	**NIST 800-171 CMMC Level 2**
Reporting | Progress Status Notification (Cont)		
Plans, Policies and Procedures Report	Yes	Yes
Book of Evidence Report with Option to Export Report with Embedded Links to Evidentiary Artifact Files (for Reviewer)	Yes	Yes
Configuration Item Report with Customizable Categories	Yes	Yes
POA&M Support Reports | Excel Export	Yes	Yes
Document Traceability Matrix (DTM) Report (8)	Yes	Yes
Document Export & Indexing (9)	Yes	Yes
Integrated Policies, Procedures & Plans Report | Document Export (10)	Yes	Yes
Objective Conformity Status Indicators, Tracking & Reporting (11)	Yes	Yes
ODP Value Definition Indicators, Tracking & Reporting (12)	Yes	Yes
Organization Defined Parameter (ODP) Report	Yes	Yes
Network Environment | DoD Document Support		
Ability to Sort Selected Assessment Notes (Assessor or Organizational) (13)	Yes	Yes
Documentation Support for DOD Assessments	Annual Self-Assessment	Triennial 3rd-Party Assessment or Annual for Select Programs
Computing Environment – Recommended (14)	Windows 11 RAM: 8GB Required 16GB	Windows 11 RAM: 8GB Required 16GB
Monitor Size – Optimum Size to View Full Pages (15)	1920 x 1080 HD Monitor	1920 x 1080 HD Monitor
Operates on Client Network (16)	Yes	Yes
CUI, Sensitive Data Controlled & Stored on Client Network	Yes	Yes

i2ACT Software for CMMC L3 \| NIST 800-172 will be available at a future date.

Notes:

1. **Assessment At Objective Level:** The i2ACT Software is designed to perform conformity assessments for both NIST 800-171 and CMMC and systematically moves through the practices, requirements, and objectives. A common format is used to capture assessment evaluations and conformity statements.

Discussions, clarifications, and examples are provided in pop-up windows for easy use while completing conformity assessments and statements. The CMMC and NIST 800-171 Assessment Guides and full versions of NIST 800-171 Rev 2 and CMMC Version 2 Levels 1-2, plus the NIST 800-53 catalogues are all searchable and retrievable at the assessor's fingertips. The i2ACT CMMC Level 3 is slated for future development.

2. **SPRS Score:** Contracting Officials use the Supplier Performance Risk System (SPRS) Supplier Risk Scores and contractor-entered SPRS score to identify "high risk" suppliers and assess the likelihood of the non-fulfillment of terms of contract, unsuccessful performance, or delivery delay.

   The i2ACT software tool prepares this SPRS Cyber Scoring Report required by the DoD Interim Rule. It should be noted that the submission of an SPRS Score also requires a completed Plan of Actions and Milestones (POA&M) with title, version, date of last revision, and estimated date to complete along with a System Security Plan (SSP).

3. **Remediation Actions (RAs):** During the Assessment process, remediation actions will need to be identified for each objective that is not fully met. The i2ACT tool offers two options:

   - **User Customized List of Remediation Actions:** Often a remediation task will apply to multiple cybersecurity controls and remediation for a given control may involve multiple tasks. In the new i2ACT tool, a given remediation task can be defined once and associated with multiple controls. The software allows the user to create a custom list of Remediation Actions (RAs) which will be stored in a database using a specific numbering system. These custom RAs will be accessible by the user at any point during the assessment process.

   - **I2 Suggested Remediation Actions:** i2 also offers a set of "Best Practice" RAs (over 400) that have been developed over the course of the last 10 years of Assessment and Compliance engagements. The RAs can be purchased with the i2ACT Tool or can be purchased as an UPGRADE at any time after the initial purchase of the tool.

4. **Evidentiary Artifacts:** Thousands of artifacts of evidence will need to be collected, stored, organized, and made available to the C3PAO assessors to demonstrate conformance with requirements, practices, and assessment objectives. For ease of editing and management, Imprimis offers a unique "Evidence Citation Viewer" feature that streamlines this process in a single pop-up viewer. Storing and Linking features include:

   - Storing and linking artifacts of evidence to multiple requirements and practices.
   - Linking artifacts at the practice or assessment objective level to support conformity statements.
   - Managing and storing artifacts within the tool for retention in the database for future reference.

5. **POA&M Support, Excel Export:** At the completion of the Assessment, 3 documents will be available for use in preparing the POA&M – the Remediation Action Report, a separate RA Title Report and a RA Description Report. The RA Title Report will be organized into 3 sections – Physical, Logical and Procedural, and is to be used in a GANT type Project Plan like MS Project to develop the top-level POA&M with the implementation schedule. The RA Description Report can be exported into MS Excel for use as the reference document for the detail of the POA&M and will be used for implementation of detailed the tasks in each remediation action. Once exported, both reports can be used in multiple ways to meet each individual customer's needs.

6. **Imprimis Organization Defined Parameters (ODPs) Identified at the Practice Level:** ODPs are critical to both security and compliance. They define the values that are part of the system configuration and the decisions used in the management of the network or system. In NIST 800-171 Rev 2, the Organization Seeking Compliance (OSC) must derive the ODPs from the requirements themselves. Imprimis has provided these in the Imprimis ODP Catalog. In later versions such as NIST 800-171 Rev 3 and NIST 800-53 Rev 5 catalog of controls, NIST defines the minimum set of ODPs which must be defined, and the OSC should identify and define any other ODPs they consider important to the operation of their system. Imprimis will provide updated lists of ODPs as required. An ODP Report is available from the tool.

7. **Educational Resources:** All compliance references are available via tabs for each control so the user can 'learn as they go'. The remediation actions also have explanatory material available for each one.

8. **Document Traceability Matrix (DTM) Report:** The official government or C3PAO assessors will require documentation showing which documents apply to individual requirements or security controls. Reviewing the applicability and adequacy of these documents is an arduous task. The DTM is designed to show which documents (policies, procedures, plans, standards, and catalogs) apply to each task as a minimum and allows for any desired specific citations to applicable parts of these documents to be identified.

9. **Document Export and Indexing:** When undergoing an official assessment, the assessor(s) will require that all documents be sent to them one or two weeks prior to conducting the assessment so that they can review them in advance. The i2ACT allows all documents to be stored in the database. The user can then establish a folder of their choosing and export all of the documents into this folder, along with a report that indexes the documents either by listing each category or linking each document to the specific controls to which it has been mapped. This folder can then be easily zipped, compressed, and encrypted with a password and sent to the requesting assessor. The assessor can then easily review them in a browser or PDF form by clicking the links to each document.

10. **Integrated Policies, Procedures and Plans Report and Document Export:** As part of the export capability described above, all Policies, Procedures, Plans and Catalogs can be separated from other artifacts included in the assessment when required.

11. **Objective Conformity Status Indicators, Tracking, and Reporting:** NIST 800-171 and CMMC Level 2 currently have 110 requirements/practices but have 320 Assessment Objectives or AOs. The complexity of the assessment is significantly increased by addressing every AO. The i2ACT helps to manage this complexity by giving clear indications of the status of each AO as implemented or planned, and which AOs are not applicable or not addressed. The tool also provides easy navigation to any AO. The i2ACT provides the same visibility, tracking and navigation to ODPs as well. Reports including AOs are available in the tool.

12. **ODP Value Definition Indicators, Tracking, and Reporting:** There are a large number of ODPs that need to be specified and tracked, further increasing the complexity of compliance. The i2ACT provides the status of each ODP, and easy tracking, access or navigation of each OCP. ODP reports are also available in the tool.

13. **Internal Notations**: Assessment, compliance and remediation notes can be added to any compliance statement. The entry of separate notes may be used to document any desired aspect of the assessment – for the benefit of the company or for the benefit of the Assessor. These company specific notes can be saved in the database and be either printed or not printed at report development time.

14. **Computing Environment:** The suggested computing platform to be used with the i2ACT software is a 64-Bit computer with Windows 11 Operating System, with 8GB RAM required, and 16GB RAM recommended. Because Microsoft no longer supports Windows 8 installations and Windows 10 support is ending soon, if you decide to run i2ACT on an unsupported operating system, we cannot guarantee the software will perform properly. In addition, Imprimis supports only “Click-to-Run” 64-bit and 32-bit installations and will not support MSI based installations for Access. For a full user interface experience (full form functionality or a wider desktop for multiple simultaneous screens), a 1920 x 1080 HD Monitor is recommended.

15. **Monitor Size:** For a full user interface experience (full form functionality or a wider desktop for multiple simultaneous screens), a 1920 x 1080 HD Monitor is recommended.

16. **Operates on Client Network:** The i2ACT Software operates on the client’s network and must be stored in a protected data share. If Assessments are provided to, stored on, or accessible by another organization, that organization must accept the full DFARS cybersecurity clause flow-downs and must also comply with NIST 800-171 and /or CMMC at the appropriate level. If the outside organization is a cloud service or managed service provider with access to, or potential access to, Controlled Unclassified Information (CUI), they must not only be certified at the FedRAMP Moderate baseline, but also must accept paragraphs c-g of the DFARS 204.73 regulations subsection. Ensuring this is true is the contractor’s responsibility.