CMMC Level 2 Blumira Checklist

Blumira is committed to supporting our manufacturing customers and making sure they have the visibility, reporting, and indelible historical record of security activity needed to meet compliance. This is why Blumira doesn't limit the number of log sources you need to monitor, or charge additional fees based on the volume of data necessary to maintain that complete record.

To help prepare for the immediate deadline of self-assessment and fast-approaching deadline in 2026 for third-party assessment, we've prepared the following checklist of specific objectives requiring the use of a monitoring solution like the SIEM integrated within the Blumira platform and questions you should ask to determine if your environment is CMMC-ready. Let's get started!

CMMC Level 2 2025/2026 Deadlines

The Department of Defense is rolling out the Cybersecurity Maturity Model Certification (CMMC) to strengthen protection of Controlled Unclassified Information (CUI). Starting November 10, 2025, all DoD contractors and subcontractors must complete a self-assessment for CMMC Level 1 or 2 to be eligible to bid on new contracts. By November 10, 2026, most organizations handling CUI are required to pass a Level 2 assessment conducted by a Certified Third-Party Assessment Organization (C3PAO) to bid on contracts.

Why You Need to Start Now

Demand for CMMC assessors far exceeds supply. With only a few dozen assessors available to serve more than 100,000 organizations seeking Level 2 certification, scheduling delays are unavoidable. Preparation can take up to six months, and there is already a 6-month waiting list to secure an assessment, which is likely to increase as the deadlines near. Organizations that postpone getting started risk missing their certification window and losing contract eligibility.

How Scoring Works

CMMC Level 2 scoring is based on the 110 cybersecurity controls outlined in NIST 800-171. Each control is weighted by importance:

- 1, 3, or 5 points per control
- 110 points total
- 110 points needed to pass
- 88 points required for a provisional pass

Failing any 3- or 5-point control means an automatic failure. If you miss smaller 1-point items, you can get a provisional pass and submit a Plan of Action and Milestones (POA&M) to fix them within 180 days.

CMMC Audit & Accountability Preparation Checklist

AU.L2-3.3.1
5-point objective (mandatory)

- [ ] Does your SIEM collect all the logs that are required for routine auditing as well as incident response? Many SIEMs selectively retain logs, or drop logs after they are received
  - [ ] 3.3.1[a] - Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified
  - [ ] 3.3.1[b] - The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.
- [ ] Does your SIEM retain all logs for your defined retention period, and for a period of time that enables both routine auditing as well as incident response?
  - [ ] 3.3.1[f] - Audit records are retained as defined.

Blumira centralized logging through our platform's cloud-based SIEM and gives you the ability to track user activity, allowing you to trace actions uniquely back to certain users and hold them accountable.

AU.L2-3.3.2
3-point objective (mandatory)

- [ ] Are all your endpoints and systems where CUI is stored or processed generating audit logs that are sent to your SIEM?*
  - [ ] 3.3.2[a] - The content of the audit records needed to support the ability to uniquely trace users to their actions is defined.

Blumira retains all ingested logs for 1 full year, and offers pre-built reports for CMMC audit log preparation which can be scheduled and delivered to your inbox.

AU.L2-3.3.5 (5-point) and AU.L2-3.3.6 (1-point)

- ☐ Are your audit logs easily accessible and searchable in a centralized repository?
  - ☐ 3.3.5[a] - Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.
  - ☐ 3.3.6[a] - An audit record reduction capability that supports on-demand analysis is provided.
  - ☐ 3.3.6[b] - A report generation capability that supports on-demand reporting is provided.

In addition to templated reports, Blumira provides on-demand reporting and analysis through our custom report builder, as well as the ability to build reports on-the-fly using Blumira Investigate on supported editions.

AU.L2-3.3.8
1-point objective (must meet 88-point pass minimum)

- ☐ Are your logs stored in such a way that modification or deletion is prevented? Many self-hosted SIEM solutions do not have sufficient auditing or protection for log modification and deletion.
  - ☐ 3.3.8[b] - Audit information is protected from unauthorized modification. - 1 point
  - ☐ 3.3.8[c] - Audit information is protected from unauthorized deletion. - 1 point

Blumira separates logging and audit tools from customers' production environments to prevent unauthorized access, modification, and deletion, and our platform limits the management of audit logging functionality to only a subset of privileged users with role-based administration.

TL;DR: Meeting the Audit & Accountability (AU) objectives for Level 2 certification requires having a centralized, searchable, permanent source of aggregated logs. Our integrated SIEM in the Blumira platform helps you meet all 9 AU objectives, including several mandatory 3- and 5-point requirements.

If you're feeling overwhelmed by the long list of resources and documentation required for CMMC preparation, Blumira has good news: in addition to the time and care built into our platform to provide you with the visibility and capabilities you need for compliance, we're launching a new CMMC support program as part of our Automate edition. This includes access to the Blumira Shared Responsibility Matrix and Customer Responsibility Matrix (SRM/CRM), along with supporting documents such as System Security Plan (SSP) templates, process and procedure documentation, and support during your assessment. Want to find out more? Visit our CMMC program page at blumira.com/cmmc to get started today!