KnowledgeBase Article 2501

Security Policies

Many Guardian clients have Certification and Audit requirements to meet the demands of their customers. This document has been developed to help clarify and understand some of these requirements. The majority of the requirements are procedural and system/company-wide policies not applicable to software.

Guardian Software Systems is dedicated to meeting the standards required of our clients and strives to develop software that will provide our clients with the tools they require to meet those standards and pass their audits. To that end, we have retained the services of an AS 9100 auditor, CMMC and DFARS advisors. We also maintain a consultation relationship with SQFI for Food Service certifications.

There are a number of accreditations and certificates available to our clients to show their compliance for manufacturing and safety standards as well as procedures and documentation. Software has no such accrediting authority. There are NO certifications available to software that apply to these requirements…Software cannot be AS9100 certified, ISO Certified or anything else certified.

Source Identification and Definitions 1
Guardian ERP and MES Software Compliance 4
Guardian Software Systems, Inc. Compliance 5
AS9100 Compliance 6
Guardian Cloud Solution (Hosted) 6
Guardian Government Cloud Solution (Hosted) 7

I. Source Identification and Definitions

There are numerous abbreviations and acronyms for agencies providing auditing and accreditation. This list attempts to identify the leading players.

a. **AS 9100**: *Quality Management Systems requirements for Aviation, Space and Defense Organizations*
   i. established 1994 by SAE International (Society of Automotive Engineers)
   ii. Incorporates all of ISO 9001
   iii. Current revision is AS 9100D
   iv. revised 2016
   v. Incorporates all of ISO 9001:2015
   vi. Incorporates AS 9110 and AS 9120

b. **CUI:** *Controlled Unclassified Information (identified in CMMC)*

c. **CMMC**: *Cybersecurity Maturity Model Certification*

   i. The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.

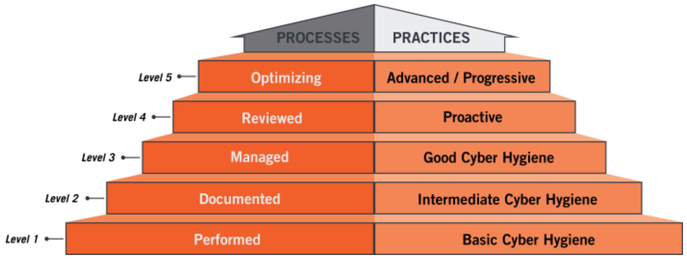
   ii. The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.

   iii. The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.

   iv. The intent is for certified independent 3rd party organizations to conduct audits and inform risk.

   v. 5 levels of Maturity

CMMC Maturity Level Descriptions



	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

d. **DFARS**: *Defense Federal Acquisition Regulations System*

   i. The defense acquisition system, as defined in 10 U.S.C 2545, exists to manage the investments of the United States in technologies, programs, and product support necessary to achieve the national security strategy prescribed by the President pursuant to section 108 of the National Security Act of 1947 (50 U.S.C. 3043) and to support the United States Armed Forces.

   ii. The investment strategy of DoD shall be postured to support not only the current United States armed forces, but also future armed forces of the United States.

   iii. The primary objective of DoD acquisition is to acquire quality supplies and services that satisfy user needs with measurable improvements to mission capability and operational support at a fair and reasonable price.

   iv. In accordance with 41 U.S.C. 1304, a new requirement for a certification by a contractor or offeror may not be included in the DFARS unless required by Statute or by approval from the Secretary of Defense

e. **DHS**: *Department of Homeland Security*

f. **DoD**: *Department of Defense*

g. **FFIEC**: *Federal Financial Institutions Examination Council*

h. **FIPS**: *Federal Information Processing Standards*

i. **FISMA**: *Federal Information Security Management Act*
   i. Act of Congress in 2002 to task government agencies to access risk and take action accordingly

j. **GLBA**: *Gramm-Leach-Bliley Act (Financial Services Modernization Act 1999)*

k. **HIPAA**: *Health Insurance Portability and Accountability Act (1996)*

l. **ISO 9001**: *Quality Management Standards*
   i. established 1987 by International Organization for Standardization
   ii. Current standard is ISO 9001:2015

m. **NADCAP**: *National Aerospace and Defense Contractors Accreditation Program*
   i. established 1990 by SAE International (Society of Automotive Engineers)
   ii. Administered by the Performance Review Institute (PRI)
   iii. Accrediting administrator for special processes in Aerospace and Defense
      1. Aerospace Quality Systems (AQS)
      2. Aero Structure Assembly (ASA)
      3. Chemical Processing (CP)
      4. Coatings (CT)
      5. Composites (COMP)
      6. Conventional Machining as a Special Process (CMSP)
      7. Elastomer Seals (SEAL)
      8. Electronics (ETG)
      9. Fluids Distribution (FLU)
      10. Heat Treating (HT)
      11. Materials Testing Laboratories (MTL)
      12. Measurement & Inspection (M&I)
      13. Metallic Materials Manufacturing (MMM)
      14. Nonconventional Machining and Surface Enhancement (NMSE)
      15. Nondestructive Testing (NDT)
      16. Non-Metallic Materials Manufacturing (NMMM)
      17. Non-Metallic Materials Testing (NMMT)
      18. Sealants (SLT)
      19. Welding (WLD)

n. **NIST**: *National Institute of Standards and Technology*
   i. formerly the National Bureau of Standards (1901-1988)
   ii. Physical Sciences Laboratory and Non-Regulatory Agency
   iii. U.S. Department of Commerce
   iv. SP prefix documents: “Special Purpose”

o. **SOC**: *Security Operations Center*
   i. Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy.

p. **SQF**: *Safe Quality Food*

i. SQFI (Safe Quality Food Institute) in association with Global Food Safety Initiative (GFSI) to regulate industry standards and regulations for all sectors of the food supply chain – from the farm to the consumer.

II. Guardian ERP and MES Software Compliance

As stated in the introduction of this document, the Guardian ERP Solution with MES is not eligible for any certification as none exists. The software does provide capabilities to assist you, the end-user, to meet compliance requirements as follows:

a. Access Control: NIST SP 800-171r2 3.1

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.11 MES: Terminate (automatically) a user session after a defined time (5 seconds).

b. Access Control: NIST FIPS 200 3

3 Minimum Security Requirements

1. The Guardian ERP and MES are in full compliance with NIST FIPS 200 meeting or exceeding the Minimum Security Requirements as identified in section 3
2. Guardian is fully FIPS Compatible (users may utilize FIPS encryption throughout their environment)
3. Guardian uses encrypted usernames and passwords for access authentication.

c. Awareness and Training: NIST SP 800-53r5 AT

AT-3 NIST SP 800-53r5 AT-3 “Role-Based Training”

1. Guardian Training can provide role-based security and privacy training to personnel with the following roles and responsibilities: Guardian Super-User, Guardian Administrator.

AT-4 NIST SP 800-53r5 AT-4 “Training Records”

2. Guardian ERP Employee Training Record can document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training and Retain individual training records for indefinitely.

d. Audit and Accountability: NIST SP 800-171r2 3.3

i. NIST SP 800-53r5 AU-2 “Event Logging”

1. Control: Pervasive AuditMaster
   a. Pervasive AuditMaster is an optional add-on to the Pervasive SQL database engine to monitor and log user definable or all events including additions, changes and views to the database.

ii. NIST SP 800-53r5 AU-8 “Time Stamps”

1. Control: Guardian ERP and MES
2. Guardian uses the company’s Guardian database server as the time source. This server should be synchronized with all other systems on the network.

III. Guardian Software Systems, Inc. Compliance

Guardian Software Systems, Inc. is currently creating written internal policies to reach compliance with NIST SP 800-53r5 and NIST SP 800-171r2 – both of which are the basis for CMMC.

When accessing client data, Guardian is in full compliance with NIST, DFARS and CMMC requirements as far as the client’s environment complies. Internally, Guardian treats client data as sensitive information, restricting access and following the requirements of NIST CMMC. Test data is deleted immediately upon completion of testing.

Guardian may, on occasion, be required to make onsite visits to clients for evaluation, discovery and/or consultation. Guardian’s personnel are screened and required to comply with **NIST SP 800-53r5**, **NIST SP 800-171r2**, **CMMC**, **SQF Code 9.1-2.3.3.1**. While onsite, Guardian personnel are required to follow all protocols outlined by the client as visitors to their facilities.

Personnel at Guardian are trained and certified in their use of the Guardian ERP and MES Software and must meet proficiency standards before contact with clients – subject to annual review.

IV. AS9100

While no software can be certified for AS9100, the Guardian ERP Solution with MES assists in AS9100 Certification by:

1. Documentation required for NADCAP Accreditation
2. Industry-standard certification documents
   a. Certificate of Conformance
   b. Chemical Certifications
   c. Mechanical Certifications
   d. NDT Certifications
3. Traceability through production, including split work orders and rework
   a. Material Lots
   b. Required Quality Checks in MES
   c. Serialization
   d. Supplier Approvals
   e. Scrap Tracking
4. Detailed Process Instructions available to worker on MES
5. Instant access to SDS documentation
6. Record of Engineering Change Notices

V. Guardian Cloud Solution (hosted)

a. The Guardian Cloud Solution is provided by OFFSITE, LLC and is in full compliance with **NIST SP 800-171r2** and **DFARS PGI 239**. OFFSITE, LLC is not a US Government certified hosting service.

b. The Cloud service is located in Kenosha, Wisconsin as a **SOC 2 Type 2 Audited Data Center**. The **SOC 2 Type 2** Report covers the AICPA's Trust Services Principles and Criteria for Security, Availability, Confidentiality, and Privacy. The report also includes a mapping of the controls tested to ISO/IEC 27001:2013 Annex A / ISO/IEC 27002:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, HIPAA security requirements, and FFIEC's examination guidelines for GLBA Information Security. Current report is for the period August 1, 2019 – July 31, 2020.

c. The Guardian Cloud Solution utilizes a secure environment for hosted services including the Guardian Database Server as well as Remote Desktop Services and IIS Services for the use of the Guardian ERP Solution with MES.

d. Built on the industry leading Cisco Unified Computing System (UCS) platform to provide customizable, scalable, reliable and secure environment.

e. The Guardian Cloud Solution utilizes a central data center in Kenosha, Wisconsin with Tier III Backup and Replication services in Chicago, Illinois and Tier III Disaster Recovery services in Denver, Colorado.

VI. GUARDIAN GOVERNMENT CLOUD SOLUTION (HOSTED)

a. Guardian utilizes the **AWS GovCloud Solution** as an option for those clients requiring the added security and auditing provided for some Government contracts. The new **CMMC** (**Cybersercurity Maturity Model Certification**) requires higher level security standards than those currently certified by the SOC 2 Type 2 Report.

b. DoD contracts will require CMMC levels;

   i. Level 1 - safeguard Federal Contract Information (FCI)

   ii. Level 2 - transition to protect Controlled Unclassified Information (CUI)

   iii. Level 3 - protect CUI

   iv. Levels 4 and 5 - protect CUI and reduce risk of Advanced Persistent Threats (APTs)

c. The AWS GovCloud Solution is in full compliance with **CMMC Level 3**.

US Government Compliance

CJIS
Criminal Justice
Information Services

DoD SRG
Department of
Defense
Data Processing

FedRAMP

FedRAMP
Government Data
Standards

FERPA
Educational Privacy
Act

FIPS
Government Security
Standards

FISMA
Federal Information
Security
Management

GxP
Quality Guidelines
and Regulations

HIPAA
Protected Health
Information

HITRUST CSF
Health Information
Trust Alliance
Common Security
Framework

ITAR
International Arms
Regulations

MPAA
Protected Media
Content

NIST
National Institute of
Standards and
Technology

PIPEDA
Canada's Federal
Private Sector
Privacy Legislation

SEC Rule 17a-4(f)
Financial Data
Standards

VPAT / Section 508
Accessibility
Standards