ACRMS™ Automation of NIST 800-30 Cybersecurity Risk Assessment A Force Multiplier for Management of Multiple Federal Contractor Sites

Regulatory Situation: 2024

Cybersecurity for non-public federal information has become a major issue in federal contracting, particularly for the majority of federal contractors who are small. The Department of Defense proposed draft CMMC 2.0 regulation imposes significant new liabilities on the estimated 163,987 small DoD contractors. NASA and GSA have proposed similar regulations in an effort to "standardize cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems".

Both the GSA and DoD efforts reference a variety of NIST 800 series protocols. However, two NIST publications are key to all of these efforts. NIST Special Publication 800-30 details the procedures for conducting a semi quantitative risk assessment, scoring cybersecurity risks from 1 (low) to 100 (high). NIST 800-53 describes the "Recommended Safeguards for Federal Information Systems". This sets out the answer to "How much security is enough?"

History and Technology

The 2002 publication of NIST 800-30 was a major event for consultants and contractors handling protected financial, legal, design or medical information. The NIST 800-30 protocol provided a consensus procedure for any organization relying on the NIST for cybersecurity guidance.

The 2005 publication of NIST 800-53 "Recommended Security Controls…" was another watershed event. For the first time there was a definitive answer to the eternal question of "how much security is enough?" Or at least enough to meet federal standards.

In 2006 cybersecurity consultant Robert Peterson, PE created an expert system computer model combining the 800-30 and 800-53 protocols to provide a rapid and consistent procedure to assess cybersecurity risks. In October of 2006 he recruited firewall expert Jack Kolk to jointly incorporate ACR 2 Solutions, Inc. in Lilburn, Georgia.

Application of Automated Assessment Technology

The primary advantage of an automated cybersecurity risk assessment procedure over an expert led assessment is not so much the **quality** of the assessment, but the **consistency**. Using the automated protocol organizations may be assessed on a consistent "apples to apples" basis. This has allowed remote management of dozens of locations with consistent results.

The cybersecurity requirements for different types of information are managed by different subsets of the 1186 cybersecurity safety controls in the current revision 5 of NIST Special Publication 800-53. The NIST 80-30 risk assessment protocol is more precisely a compliance protocol, assuming that compliance with the applicable regulation will provide an appropriate

level of security. ACR 2 Solutions, Inc. has successfully applied the ACR 2 Cybersecurity Risk Management System to organizations managed under the following regulations.

1. Gramm Leach Bliley Act (GLBA).
2. Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
3. Defense Federal Acquisition Regulation Supplement (DFARS) 252.24-7012.
4. NIST Cyber Security Framework (CSF).
5. Federal Contract Information FAR 52.2204-21

More than 400 contractor sites using the expert system computer model ACRMS™ risk assessment procedure have been audited since 2006.

No ACRMS™ risk assessment client has ever failed a cybersecurity audit!

The systematic and consistent application of the ACRMS™ instantiation of the NIST 800-30 protocol has been universally accepted by auditors to date.

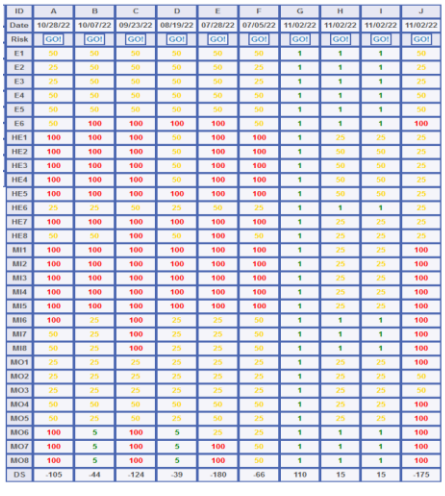
Appendix A has a summary procedure for calculating risks using the NIST 800-30 protocol. The concept is straightforward, although time-consuming for the initial calculation. “Risk” is defined by the NIST as the “net negative effect of exploitation of a vulnerability by a threat source, taking into account likelihood and impact”.

The calculation algorithm for the risk assessment is given on page 25 of NIST Special Publication 800-30. Low, Medium, and High likelihoods of adverse events are scored at 0.1, 0.5 or 1.0, respectively. In the same manner, Low, Medium, and High impacts are scored at 10, 50 and 100 respectively. By multiplying the likelihood score and the impact score, a risk score from 1 (low) to 100 (high) is calculated.

Likelihoods and impacts are a function of the presence or absence of assigned safeguards. For example, the impact of a facility fire when all data is backed up hourly to a cloud server on the other side of the Rockies can fairly be listed as “low”. However, if backup tapes are stacked on top of the server (true example) a server fire impact could be “high”.

As noted in Appendix A there are more than 5,000 calculations involved in a NIST 800-30 risk calculation. Initial creation and validation of the 800-30 expert system computer model was time consuming and expensive. Subsequent uses are quick and very low cost.

Multi-site Management using the ACRMS™ Management Edition



ID	A	B	C	D	E	F	G	H	I	J
Date	10/28/22	10/07/22	09/23/22	08/19/22	07/28/22	07/05/22	11/02/22	11/02/22	11/02/22	11/02/22
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	50	50	50	50	50	50	1	1	1	50
E2	25	50	50	50	50	25	1	1	1	25
E3	25	50	50	50	50	25	1	1	1	25
E4	50	50	50	50	50	50	1	1	1	50
E5	50	50	50	50	50	50	1	1	1	50
E6	50	100	100	100	100	50	1	1	1	100
HE1	100	100	100	50	100	100	1	25	25	25
HE2	100	100	100	50	100	100	1	50	50	25
HE3	100	100	100	50	100	100	1	50	50	25
HE4	100	100	100	50	100	100	1	50	50	25
HE5	100	100	100	100	100	100	1	50	50	25
HE6	25	25	50	25	50	25	1	1	1	25
HE7	100	100	100	100	100	100	1	25	25	25
HE8	50	50	100	50	100	50	1	25	25	25
MI1	100	100	100	100	100	100	1	25	25	100
MI2	100	100	100	100	100	100	1	25	25	100
MI3	100	100	100	100	100	100	1	25	25	100
MI4	100	100	100	100	100	100	1	25	25	100
MI5	100	100	100	100	100	100	1	25	25	100
MI6	100	25	100	25	25	50	1	1	1	100
MI7	50	25	100	25	25	50	1	1	1	100
MI8	50	25	100	25	25	50	1	1	1	100
MO1	25	25	25	25	25	25	1	25	25	100
MO2	25	25	25	25	25	25	1	25	25	50
MO3	25	25	25	25	25	25	1	25	25	50
MO4	50	50	50	50	50	50	1	25	25	100
MO5	50	25	50	25	50	25	1	25	25	100
MO6	100	5	100	5	25	25	1	1	1	100
MO7	100	5	100	5	100	50	1	1	1	100
MO8	100	5	100	5	100	50	1	1	1	100
DS	-105	-44	-124	-39	-180	-66	110	15	15	-175

Using the automated version of the NIST 800-30 risk assessment protocol to supervise multiple sites is practical even with organizations regulated under different regulations such as GLBA and HIPAA. One client was able to manage cybersecurity concerns for 103 locations across 16 states from a single location outside of Detroit. This should be attractive to APEX consultants who often provide support services to hundreds of small contractors.

Currently the most common combination is FAR 52.204-21 for organizations handling only Federal Contract Information (FCI)

and DFARS 252.204-7012 for contractors handling both FCI and Controlled Unclassified Information (CUI).

ACR 2 clients working with APEX Accelerator (APEX) or Manufacturing Extension Partnership (MEP) consultants receive a discount on their ACRMS™ software. ACR 2 provides this discount because clients working with a MEP or APEX consultant are easier for ACR 2 to manage. MEP and APEX offices can provide “boots on the ground” services anywhere in the USA.

To facilitate MEP and APEX collaboration between MEP or APEX consultants, ACR 2 provides free ACRMS training to MEP and APEX staff about once a month. Training sessions are listed on our website at https://cuicybersecuritycompliance.com/events. This free training session includes ACRMS FAR-21, ACRMS DFARS-7012 and ACRMS Enterprise software for each MEP or APEX participant. The morning session ends with preparation of a CMMC Level 1 Annual Assessment. The afternoon session ends with creation and scoring of a CMMC Level 2 System Security Plan. Training is free, but sessions are limited to 10 participants.

ACRMS™ Management Edition Details

The ACR 2 Cybersecurity Risk Management System or ACRMS™ program consists of several interlocking elements, all based on NIST guidance documents.

1. Policy creation. The ACRMS™ utilizes the NIST 800-series of cybersecurity safety controls. The approximately 40,000 pages of guidance are well written and comprehensive. Typically written in PhD level 18th grade English, they are far from user friendly. The ACRMS policy templates extract relevant information, translating key items into 10th grade English. A partial set of NIST guidance documents is shown at right. A sample ACRMS™ template is in Appendix B.
2. Procedure creation. Who is going to achieve which tasks on what schedule? ACR 2 has created typical small contractor sites for various regulated groups. For FAR 52.204-21 regulated contractors ACR 2 has created the fictional 5 person Jim Bob Uniforms, or JBU. The larger fabricator Bobby Lee Welding (BLW) is a composite of about 50 small DFARS 252.204-7012 contractors cybersecured by ACR 2 since 2017. Sample tasks are pretty consistent for small contractors. The median federal manufacturing contractor has five staff. Site Data Forms are in Appendix C.
3. Artifact creation providing documentation that the assigned task was completed on schedule and was successful in meeting the policy objectives. Artifact examples are integrated with the policy templates in Appendix B.
4. NIST 800-30 risk assessment tracking the degree of completion of assigned tasks and the subsequent effect on risk scores. Tasks not completed on schedule will affect risk scores. An excerpt of typical tasks for a DFARS -7012 clients is in Appendix D.

At present most small DOD contractors will be regulated under some combination of FAR 52.204-21 and DFARS 252,204-70121. Both regulations are linked to revision 2 of NIST Special Publication 800-171. Contractors handling only nonpublic Federal Contract Information (FCI) such as price and delivery details only need to meet 17 of the 110 requirements. Manufacturing contractors handling Controlled Unclassified Information (CUI), typically drawings and specifications, need to meet 110 requirements, including the17 for FCI.

The use of color-coding red (high risk) to green (low risk) was added at the request of clients back in 2007. Recent NIST protocols have adopted a similar scoring procedure. The red/yellow/green makes it very easy to see trends. A typical NIST Special Publication 800-30 summary report is shown below.

	Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
E1	Wind	Roof damage	M	M	25
E2	Fire	Smoke damage	M	M	25
E3	Flood	Facility damage	M	M	25
E4	Power loss	Loss of operations	M	M	25
E5	Power loss	Damage to building	M	M	25
E6	Vehicle collision	Facility damage	M	M	25
HE1	Human error	Data acquisition	M	M	25
HE2	Human error	Data storage	M	M	25
HE3	Human error	Data retrieval	M	M	25
HE4	Human error	Data modification	M	M	25
HE5	Human error	Data transmission	M	L	25
HE6	Human error	System design	M	M	5
HE7	Human error	Procedure implementation	M	M	25
HE8	Human error	Internal controls	M	M	25
MI1	Malicious insider	Data acquisition	M	M	25
MI2	Malicious insider	Data storage	M	M	25
M13	Malicious insider	Data retrieval	M	M	25
M14	Malicious insider	Data modification	M	M	25
M15	Malicious insider	Data transmission	M	H	25
M16	Malicious insider	System design	M	M	50
M17	Malicious insider	Procedure implementation	M	M	25
M18	Malicious insider	Internal controls	M	H	25
MO1	Malicious outsider	Data acquisition	M	H	50
MO2	Malicious outsider	Data storage	M	H	50
MO3	Malicious outsider	Data retrieval	M	H	50
MO4	Malicious outsider	Data modification	M	H	50
MO5	Malicious outsider	Data transmission	M	H	50
MO6	Malicious outsider	System design	M	L	50
MO7	Malicious outsider	Procedure implementation	M	L	5
MO8	Malicious outsider	Internal controls	L	L	1

The ACRMS™ risk calculation engine is mounted on a FEDRAMP medium server and accessed using HTTPS. Data is heavily encrypted using the 256 bit AES protocol.

ACRMS™ Levels of Management

The ACRMS user program monitors cybersecurity for a single site or network, typically with fewer than 50 users. The monitoring focus is on the changed in standardized risk scores over time.

There are a large number of available monitoring and management reports, as shown at right.

Groups of sites are managed using an ACRMS™ Enterprise account. The focus is on differences in standardized risk profiles between different locations. A muti-site summary status report is shown on the following page.

Groups of Enterprise sites are managed using a Megaprize account.

Example Report: Multi-site Enterprise risk score summary.

ID	Enterprise Nickname	Hide
A	BLW1222DEMO	☐
B	BLW0926demo	☐
C	BLWdemo0815	☐
D	BLW0613DEMO	☐
E	BLW2021update	☐
F	BLWdemo102422	☐
G	BLWdemo0919	☐

ID	A	B	C	D	E	F	G
Date	03/27/24	01/25/24	08/19/22	07/05/22	02/24/23	02/29/24	09/23/22
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	1	50	50	50	50	50	50
E2	1	50	50	25	50	25	50
E3	1	50	50	25	50	25	50
E4	1	50	50	50	50	50	50
E5	1	50	50	50	50	50	50
E6	1	100	100	50	100	100	100
HE1	25	100	50	100	100	100	100
HE2	25	100	50	100	100	100	100
HE3	25	100	50	100	100	100	100
HE4	25	100	50	100	100	100	100
HE5	25	100	100	100	100	100	100
HE6	50	100	25	25	50	100	50
HE7	25	100	100	100	100	100	100
HE8	25	100	50	50	100	100	100
MI1	100	100	100	100	100	100	100
MI2	100	100	100	100	100	100	100
MI3	100	100	100	100	100	100	100
MI4	100	100	100	100	100	100	100
MI5	100	100	100	100	100	100	100
MI6	25	25	25	50	100	100	100
MI7	5	50	25	50	50	100	100
MI8	5	50	25	50	50	100	100
MO1	50	50	25	25	100	100	25
MO2	50	50	25	25	100	100	25
MO3	50	50	25	25	100	100	25
MO4	100	100	50	50	100	100	50
MO5	50	50	25	25	100	100	50
MO6	25	25	5	25	100	100	100
MO7	50	100	5	50	100	100	100
MO8	50	100	5	50	100	100	100
DS	-197	-201	-39	-66	-149	-201	-124

Note that all the BLW or Bobby Lee Welding sites have only fictional data.

Updating and version control.

“Cybersecurity is a moving target” is a quote from sources as wide ranging as Duke University and industrial cybersecurity consultant Arete. As Duke cybersecurity professor Michael Reiter puts it “As new technologies emerge, security has to catch up.”

NIST 800-53 is the key document for “Recommended Security Controls...” The last major update was 2020, with minor changes in November 2023. This version is more than twice as long as the 2005 original.

Updates announced for 2024 or 2025 include changes to NIST 800-66, affecting the HIPAA Security Rule, major changes to the NIST Cybersecurity Framework (CSF) and significant changes to NIST 800-171. The 800-171 changes will affect both DFARS -7012 compliance and the FAR-21 requirements.

NIST documents may change significantly after initial draft publication. A case in point is NIST 800-171. The initial public draft includes a CUI 3.12.5 requirement for independent assessment of cybersecurity controls effectiveness, as shown below.

3.12.5. Independent Assessment

Use independent assessors or assessment teams to assess controls.

DISCUSSION

Independent assessors or assessment teams are individuals or groups who conduct impartial security assessments of the system. Impartiality means that assessors are free from perceived or actual conflicts of interest…

This requirement could have had a major impact on APEX Accelerator offices, who had been proposed as the likely source of assessment teams. After more than 1600 comments CUI 3.12.5 was removed from the final public draft of NIST 800-171 rev 3.

Typically, there will be a time period, up to a year, between publication and implementation of new NIST requirements. It is tempting to make no improvements until regulatory changes are final. However, last minute process changes can end up being avoidably expensive.

Appendix A: Automating NIST 800-30 Risk Assessment

On July 13, 2010, HHS published the final "meaningful use" requirements for receiving subsidy payments under the American Recovery and Reinvestment Act (ARRA). Along with transaction requirements, page 44372 requires both hospitals and Eligible Providers (EPs) to "Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process."

The HIPAA Security Rule was published in 2003 as 45 CFR 164. Quoting from page 8377 of the regulation, 45 CFR 164.308 requires the user to "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." This risk analysis is further defined on page 8346 where it states "This standard and its component implementation specifications form the foundation upon which an entity's necessary security activities are built. See NIST SP 800–30, ''Risk Management Guide for Information Technology Systems,'' chapters 3 and 4, January 2002."

Since the Clinger-Cohen Act of 1996, the National Institute of Standards and Technology has been required to set the standards for information security throughout the federal government. The publication of the NIST 800-30 risk assessment procedure in 2002 both eased and complicated the burden on organizations required to complete risk assessments. Although it established the procedures for assessing risk, the procedures are both voluminous and complex. Conducting a NIST compliant risk assessment remains problematic for many organizations. A single copy of the applicable NIST risk assessment references as of mid-2007 is shown at right.

Page 1 of the most recent HHS guidance on risk assessment, published in July of 2010, states that the NIST protocols "represent the industry standard for good business practices with respect to standards for securing e-PHI."

The NIST 800-30 documentation, while detailed, is well written. On page 8, the protocol states that "The risk assessment methodology encompasses nine primary steps…

Step 1 System Characterization (Section 3.1)

Step 2 Threat Identification (Section 3.2)

Step 3 Vulnerability Identification (Section 3.3)

Step 4 Control Analysis (Section 3.4)

Step 5 Likelihood Determination (Section 3.5)

Step 6 Impact Analysis (Section 3.6)

Step 7 Risk Determination (Section 3.7)

Step 8 Control Recommendations (Section 3.8)

Step 9 Results Documentation (Section 3.9)."

These steps can be automated using standard expert system computer simulation methods well known to persons skilled in the field. The process for automating the risk assessment protocol is similar to that for automating tax return preparation and similar complex procedures.

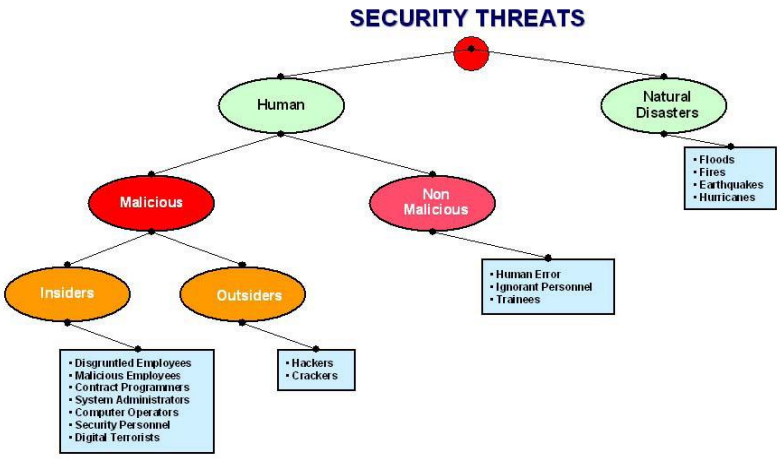
The ACR 2 Solutions risk assessment software was first published in 2006. The use of this expert system software package for preparation of a 45 CFR 164.308 risk assessment reduces the time required from 40+ hours to less than 4 hours, with even more time saved in the updating process.

Recent advances in using SCAP scanner technology have reduced the time for creating a Stage 1 meaningful use 45 CFR 164.308 risk assessment to less than 30 minutes during an office visit.

1. **System Characterization (3.1)**
   Page 12 of 800-30 requires questionnaires, document review, and automated scanning tools for system characterization. The Automated Risk Management program from ACR is compatible with a variety of network scanning engines, including the SCAP validated scanners developed under the auspices of the Department of Homeland Security. An extensive policy questionnaire is also used, keyed to the requirements of NIST 800-53.

2. **Threat Identification (3.2)**
   Page 13 of 800-30 lists natural threats, human threats, and environmental threats. An early 2000 information security paper by Jaisingh and Rees refers to the Microsoft classification of threats as being divided into natural disasters, Human Error, Malicious Insiders and Malicious Outsiders. Later papers, by Mintaka (2003) and Altoros (2007), include a more elaborate version of the Rees diagram.

   While there are other acceptable ways to identify threats, the dominance of Microsoft products in the Federal space indicates that the use of the Microsoft division of threats into Environmental, Human Error, Malicious Insiders and Malicious Outsiders is both useful and widely acceptable. The Rees diagram is shown below.



3. **Vulnerability Sources (3.3)**
   In 2005, the NIST created the National Vulnerability Database (NVD), which superseded the I-CAT database referred to on page 16 of 800-30. The NVD is incorporated into the SCAP validated scanners that are an integrated part of the Automated Risk Management program from

   Page 18 of 800-30 notes that vulnerabilities in management, operational, and technical areas all need to be considered.

   The Automated Risk Management program from ACR system further divides vulnerable areas into management (Procedure implementation and Internal controls), operational (Data acquisition, Data storage, Data retrieval, Data modification, Data transmission) and technical (System design). In addition, the environmental vulnerabilities of Wind (roof damage), Fire (and smoke) damage, Flood, Power loss (loss of operations), Power loss (Damage to building), and Vehicle collision (including car bombs) are included. It is believed that this division was taken from an early 800-30 risk assessment draft, but the original source has been lost.

   Other division of areas of vulnerability could be made, but these are reasonably comprehensive and are easily assigned to particular 800-53 safeguards.

4. **Control analysis (3.4)**

The utility of the 800-30 risk assessment process was greatly enhanced by the 2005 publication of 800-53, “Recommended Security Controls for Federal Systems.” For the first time, a listing of adequate safeguards to achieve an acceptable level of risk was made explicit by an authoritative source.

This frequently updated list, in conjunction with the SCAP validated scan engine, is the basis for much of the Automated Risk Management program from ACR process.

Two key elements in control analysis are anti-virus protection and intrusion protection. Both are highly important precautions, and the volume of virus and intrusion traffic is closely associated with the current security level of a network. A badly infected network will be both compromised and slow, as more and more network resources are misapplied by unauthorized uses.

Likelihood determination (3.5)

For an 800-30 risk assessment, likelihood has a specific legal meaning, as follows;

> *High* - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
>
> *Medium* - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
>
> *Low* - The threat-source lacks motivation or capability, or controls are in place to
>
> prevent, or at least significantly impede, the vulnerability from being exercised.

Since the publication of 800-30 in 2002, cybercrime has exceeded illegal drugs as the leading criminal activity worldwide. Threat source motivation and capability can reasonably be assumed.

The Automated Risk Management program from ACR features approximately 105 of the safeguards of NIST 800-53. Mapping of these safeguards to the four threat sources (Environmental, Human error, Malicious insider and Malicious outsider) is done by inspection. For each threat source, the vulnerable areas of management (Procedure implementation and Internal controls), operations (Data acquisition, Data storage, Data retrieval, Data modification, Data transmission), and technology (System Design) are also fairly obvious. With over 5,000 entries, this mapping is complex and time consuming, but fairly rigorous.

The translation of the safeguards map into an expert system computer program was done

by observing experienced risk assessment consultants and tweaking the calculation

engine to produce the same results using either a human expert or the expert system computer program. The development team had access to federally audited risk assessments, which greatly facilitated the validation process.

Information security risk assessments produced with this automated system have been audited by both OCC and FDIC experts.

5. **Impact analysis (3.6)**

Impact levels under 800-30 have very specific definitions.

> *High* - Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
>
> *Medium* - Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
>
> *Low* - Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

The calculation of impact levels is also mapped to 800-53 safeguards in a fairly obvious fashion. For example, a system that does not meet the requirements of safeguard CP-9, Information System Backup, will be much more impacted by Fire than a system which is compliant with CP-9 and has a well written contingency plan (CP-2) that includes training (CP-3) and testing (CP-4).

6. Risk determination (3.7)

The calculation algorithm for the risk assessment is given on page 25 of 800-30. Low, Medium, and High likelihoods of adverse events are scored at 0.1, 0.5 or 1.0, respectively. In the same manner, Low, Medium, and High impacts are scored at 10, 50 and 100 respectively. By multiplying the likelihood score and the impact score, a risk score from 1 (low) to 100 (high) is calculated.

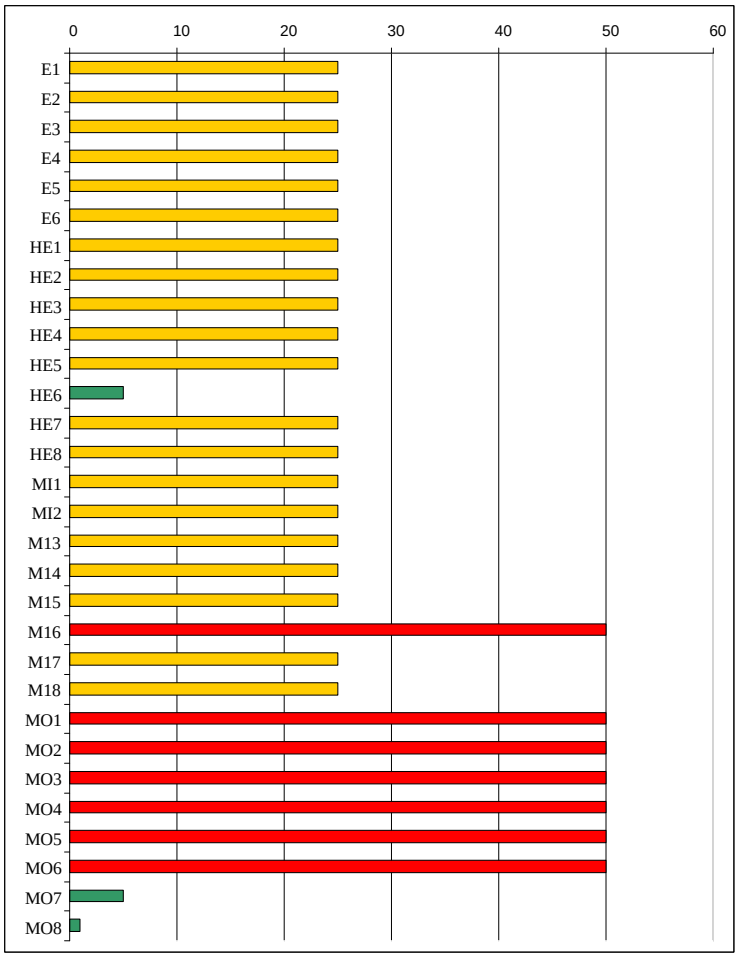
7. **Control recommendation (3.8)**

These reports give a mapping of the featured safeguards which are missing, against the identified risks in order of impact. These reports should be used to determine which safeguards need to be changed or updated.

8. Results documentation

Upon completion of the Automated Risk Management program from ACR risk assessment, the initial set of data will produce two reports, a “Baseline Report” showing the risk scores ordered by threat source and a “Risk Assessment Chart. “with the same risk scores shown in graphical form. A sample is shown below.

	Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
E1	Wind	Roof damage	M	M	25
E2	Fire	Smoke damage	M	M	25
E3	Flood	Facility damage	M	M	25
E4	Power loss	Loss of operations	M	M	25
E5	Power loss	Damage to building	M	M	25
E6	Vehicle collision	Facility damage	M	M	25
HE1	Human error	Data acquisition	M	M	25
HE2	Human error	Data storage	M	M	25
HE3	Human error	Data retrieval	M	M	25
HE4	Human error	Data modification	M	M	25
HE5	Human error	Data transmission	M	L	25
HE6	Human error	System design	M	M	5
HE7	Human error	Procedure implementation	M	M	25
HE8	Human error	Internal controls	M	M	25
MI1	Malicious insider	Data acquisition	M	M	25
MI2	Malicious insider	Data storage	M	M	25
M13	Malicious insider	Data retrieval	M	M	25
M14	Malicious insider	Data modification	M	M	25
M15	Malicious insider	Data transmission	M	H	25
M16	Malicious insider	System design	M	M	50
M17	Malicious insider	Procedure implementation	M	M	25
M18	Malicious insider	Internal controls	M	H	25
MO1	Malicious outsider	Data acquisition	M	H	50
MO2	Malicious outsider	Data storage	M	H	50
MO3	Malicious outsider	Data retrieval	M	H	50
MO4	Malicious outsider	Data modification	M	H	50
MO5	Malicious outsider	Data transmission	M	H	50
MO6	Malicious outsider	System design	M	L	50
MO7	Malicious outsider	Procedure implementation	M	L	5
MO8	Malicious outsider	Internal controls	L	L	1



An annual 45 CFR 164.308 compliant risk assessment is required under several sets of regulations, including the meaningful use requirements as well as the HIPAA Security Rule. However, manual preparation of a compliant assessment is likely to be far outside the experience of most security officers. The burden these regulations place on organizations can be eased by the use of an Automated Risk Management program such as those available from ACR 2, MedComSoft, Telos or Modulo.

Appendix B – Sample ACRMS Template

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.3.9

Video Link: https://attendee.gotowebinar.com/recording/4578164540505673643

3.3.9 Limit management of audit logging functionality to a subset of privileged users.

3.3.9 Self-Assessment Workbook Questions

1. Is access to management of audit functionality authorized only to a limited subset of privileged users?
2. Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguard AU-9(4)

AU-9(4): PROTECTION OF AUDIT INFORMATION: ACCESS BY SUBSET OF PRIVILEGED USERS

Authorize access to management of audit logging functionality to only [*Assignment: organization-defined subset of privileged users or roles*] (typically "the IT Manager, the Compliance Officer, and external Auditors").

Suggested Policy Clauses:

1. The <IT Manager> sets the system to <daily> backup of encrypted audit data.

2. The Compliance Officer receives completed, signed, and dated form from the IT Manager. After review, the Compliance Officer countersigns the form and uploads the form to the DMC. Input new start dates.

3. Data access is restricted to <list authorized individuals>.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

(Editor's note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

NIST 800-171A Assessment of Policy Effectiveness

3.3.9 ASSESSMENT OBJECTIVE: Determine if, for an organizational system that processes, stores, or transmits CUI:

3.3.9[a] a subset of privileged users granted access to manage audit functionality is defined.

3.3.9[b] management of audit functionality is limited to the defined subset of privileged users.

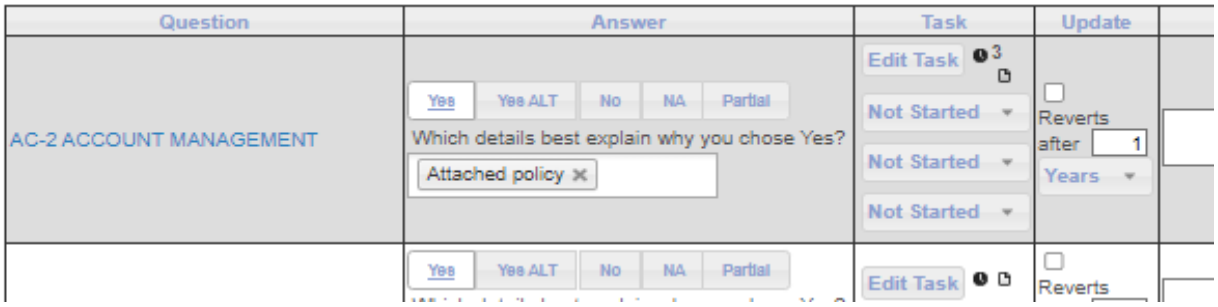
3.3.9 Potential Assessment Method and Objects SELECT FROM: Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; security plan; system design documentation; system configuration settings and associated documentation; access authorizations; system-generated list of privileged users with access to management of audit logging functionality; access control list; system audit logs and records; other relevant documents or records.

CMMC Level 3 Assessment Guide

- Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?

Suggested ACRMS data inputs

Screen shot of the ACRMS data input page

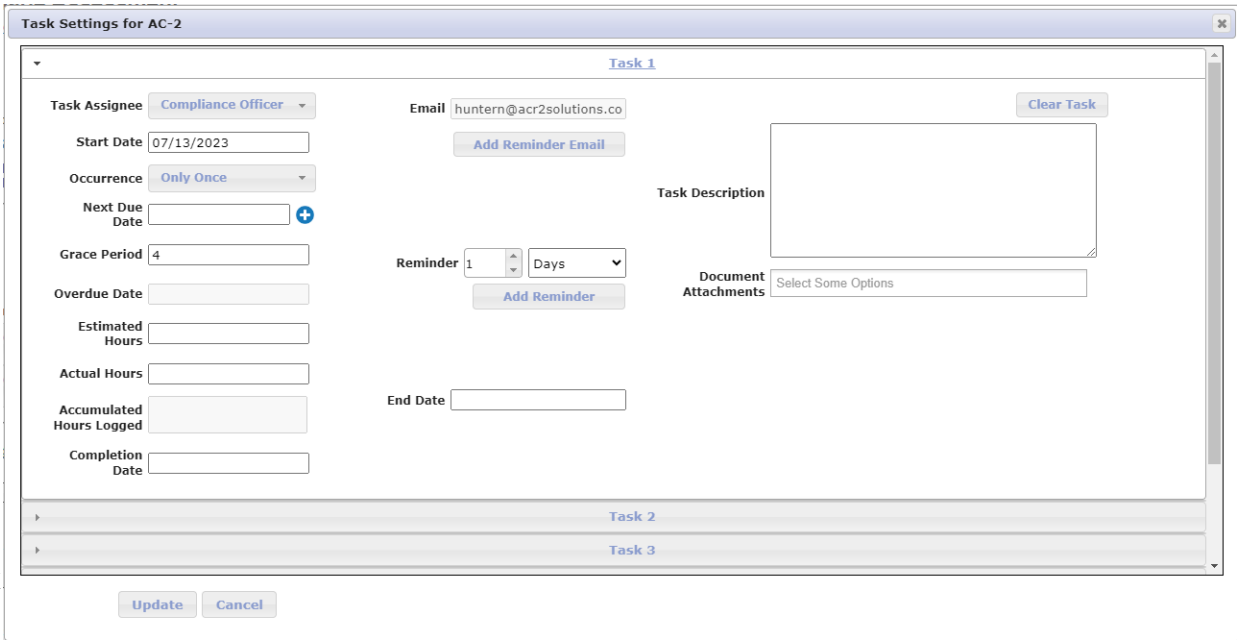


Question AU-9(4): PROTECTION OF AUDIT INFORMATION

Answer AU-9(4): ☒ Yes ☐ Yes/Alt ☐ No ☐ NA ☐ Partial

Policy File AU-9(4): CUI 3.3.9 AU9(4) MoYr

Screen shot of front of ACRMS task edit page



The <IT Manager> sets the system to <daily> backup of encrypted audit data. Note actual backups (7 days) and hours spent on weekly form. The <Compliance Officer> receives a completed signed and dated form from the <IT Manager>. After review, the <Compliance Officer> countersigns the form and uploads the form <weekly> to the DMC. Input new start dates.

Report Example: Backup of Encrypted Audit Data

Tommy Lee set the system to daily backup of encrypted audit data. Affected back-ups were done Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. It took 30 minutes.

Filename: AU-9(4) Backup of Encrypted Audit Data 09062023

Report Date: 09/06/2023_____
Report Author: Tommy Lee _____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: ____ Tommy Lee _____

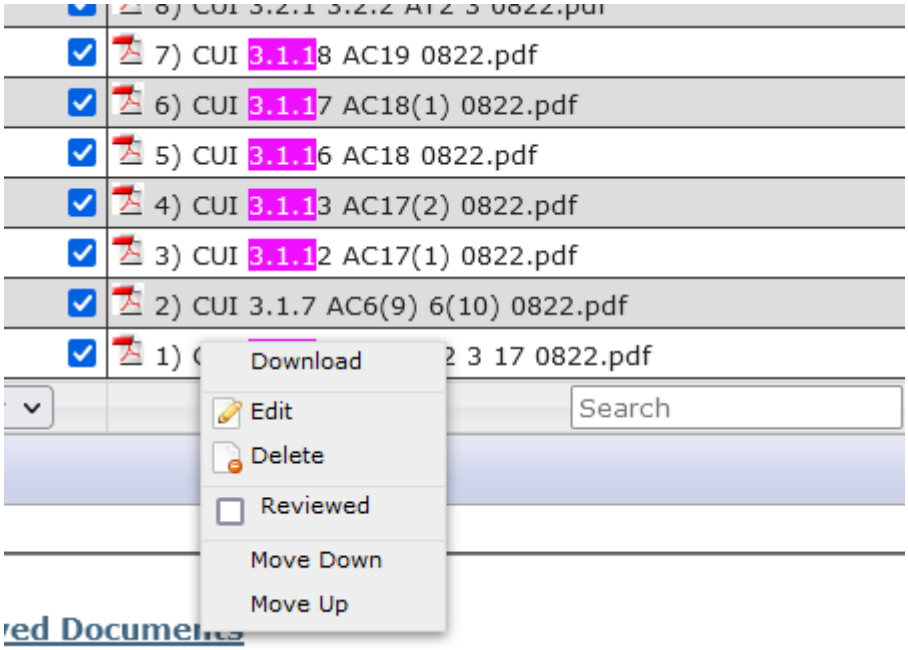
Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
1.00	--	1.00	--	2.00	--

Estimated hours: 2

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC).

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.



Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: ___09/06/2023_____(new date)_____

Authorizing Official: _Bobby Lee___(no change)_____

☒ Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.

Typed Signature: ___Bobby Lee_____(no change)__

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
0.10	typically only minor changes	0.10	typically only minor changes	0.10	typically only minor changes

Estimated hours: 0.10

Appendix C – Site Data Forms

CUI Cybersecurity Site Data Summary

General Directions: Please answer questions with whatever information is readily available. Typically, data will not be available for all questions. Do not delay the project for unavailable data but do provide as much information as can be readily obtained.

Company Name: _____Jim Bob Uniforms_____

Site Name and Address: _____255 Wolf Road, Hiram Ga_____

Point of Contact this Location: _____Jim Bob Bailey_____

Contact Phone & Email: _____

Total number of employees at this site: __5_____

Total number of employees with remote access to this site: _____0_____

Short Description of Business Activities:

Jim Bob Uniforms (JBU) started as an on-event T-shirt print shop, producing custom individualized tee shirts at high school wrestling competitions and similar events. Moving into school uniforms led to additional expansion into commercial, law enforcement and eventually military uniforms.

JBU makes contracts based on publicly available specifications and does not handle classified or controlled unclassified information. JBU does handle Federal Contract Information or FCI, including prices, quantities and delivery information, using the safeguards specified in FAR 52.204-21.

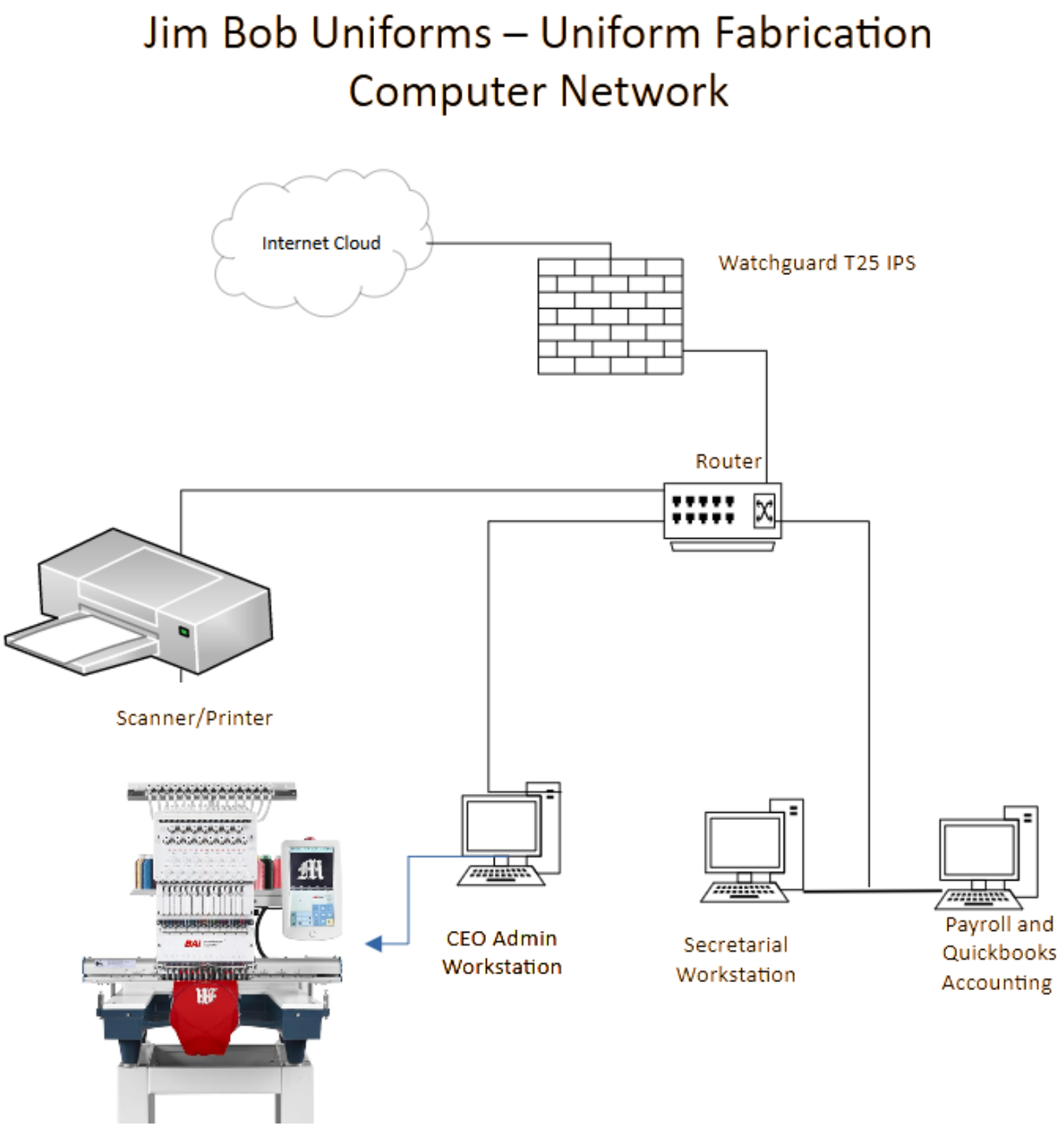
In response to the 12/26/23 draft of CMMC 2.0, JBU has upgraded its documentation and network protection. A license was obtained for the ACR 2 Solutions ACRMS-FAR-21 policy creation and task management system. The local network was upgraded with the addition of a Watchguard T25 intrusion prevention system.

Initial Information–Where information requested is unavailable, mark “unknown”.

1. Identify personel that will be available for onsite assistance for completing the risk management program. One person may fill multiple roles.

a. __Jim Bob Jones _Compliance Officer – able to sign and adopt policies
b. __Jim Bob Jones _Human Resources Manager – able to hire and train staff
c. __Jim Bob Jones _Operations Manager – authorized to operate physical plant
d. __Jim Bob Jones _IT Manager – able to install and manage data handling equipment
e. __GA MEP_____IT Consultant – resource for difficult technical issues

2. For this site, is a current Network Topology Diagram available, (Yes). If yes, please attach (see below).



3. Create Device Inventory of all devices connecting to the network or accessing protected information (PI) *(i.e. PCs, Smart phone, Mobile Device, etc.)* Please append Inventory to this form.

a. How many and what type of computers or servers or other devices?

i. _3___Windows 11 workstations

ii. 0 Linux,

iii. 0 Mac

iv. _3__ Android

v. __0_ iOS

vi. __0_Other

4. Software Summary – major software packages

Windows™ 11, Quickbooks, MS Office, Firefox. ACRMS FAR™-21

5. Network Details - Are computers part of an Active Directory domain? (Y / N)

7. Firewalls, including next-generations Firewalls (NGFW) and/or Intrusion detection/intrusion prevention systems (IDS, IPS)? (Yes)

a. If Yes, Manufacturer / Model: Watchguard T25

b. If Yes, Summarize Recent experience

Number of Days in Dataset __3_____

Total Number of Intrusions ___1_____

Total Number of Alerts ___8_____

Total Number of Warnings _____33_____

Total Number of Virus Detections _____1_____

8. Do you allow remote access? No If so, how? (Check all that apply)

a. ___ Virtual Private Network (VPN)
b. ___ SSH
c. ___ Terminal server
d. ___ Other

9. Cloud-based servers (Y / N) Manufacturer / Type _____

10. Cloud-based storage (Y / N) Manufacturer / Type _____

11. Cloud-based applications (Software as a Service) (Yes) Manufacturer / Type ____Quickbooks, MS Office, ACRMS FAR-21_____

12. Staff Experience

Total Number of People with Access to Protected Information ___3_____

Total Number of People with Access and < 1 year Experience ____0____

CUI Cybersecurity Site Data Summary

General Directions: Please answer questions with whatever information is readily available. Typically, data will not be available for all questions. Do not delay the project for unavailable data but do provide as much information as can be readily obtained.

Company Name: Bobby Lee Welding – Prototype Design and Fabrication

Site Name and Address: BLW Associates, 200 Wolf Road Hiram, GA

Point of Contact this Location: Bobby Lee

Contact Phone & Email: 770-381-9229, bobbylee@blw.net

Total number of employees at this site: 15

Total number of employees with remote access to this site: 2

Short Description of Business Activities:

Bobby Lee Welding (BLW) began as a simple manual welding job shop. After upgrading to computer-controlled welding units, BLW was able to enter the more lucrative business of fabricating high precision components for DOD and aerospace applications. With the purchase of ACME Design Solutions, LLC, BLW is now able to modify and produce either single examples or small lots of high precision components.

Initial Information–Where information requested is unavailable, mark "unknown".

6. Identify personel that will be available for onsite assistance for completing the risk management program. One person may fill multiple roles.

a. Bobby Lee Compliance Officer – able to sign and adopt policies
b. Bobby Lee Human Resources Manager – able to hire and train staff
c. Bobby Lee Operations Manager – authorized to operate physical plant
d. Tommy Lee IT Manager – able to install and manage data handling equipment
e. N/A IT Consultant – resource for difficult technical issues

7. For this site, is a current Network Topology Diagram available, (Y). If yes, please attach. (Note: the free software program LibreOffice has a Visio clone drafting program that makes it simple to turn a pencil drawing into a useful diagram. A YouTube video detailing the process is at https://www.youtube.com/watch?v=4laWj95PimI)

8. List of employees:

Owner: Bobby Lee

IT Manager: Tommy Lee

Administrator: Sarah Lee

Remote workers: Brandon Lee (accountant) and Jimmie Lee (Tech Crew)

Production: Mike Evans, Matthew Evans, Luke Hunter, Chris Smith, Billy Morrison, James Tyler

Design: Cindy Wells, Johnny Hughes, Lucas Granger, George Shaw, Will George, Riley Mortar

9. Create Device Inventory of all devices connecting to the network or accessing protected information (PI) *(i.e., PCs, Smart phone, Mobile Device, etc.)* Please append Inventory to this form.

a. How many and what type of computers or servers or other devices?

i. _9_____Windows, Win 10 workstations with Office 365

ii. _6_____Linux, welding machine controllers

iii. _0__Mac

iv. _17__ Android phones with full device encryption and Office 365

v. _0__ iOS

10. Software Summary – major software packages

MS Office

Quickbooks

AutoCad

WeldPro

11. Network Details - Are computers part of an Active Directory domain? (Y **/ N**)

7. Firewalls, including next-generations Firewalls (NGFW) and/or Intrusion detection/intrusion prevention systems (IDS, IPS)? (**Y** / N)

a. If Yes, Manufacturer / Model _____Fortinet WiFi 50_____

b. If Yes, Summarize Recent experience

Number of Days in Dataset _____30_____

Total Number of Intrusions _____4_____

Total Number of Alerts _____17_____

Total Number of Warnings _____120_____

Total Number of Virus Detections _____3_____

8. Do you allow remote access? If so, how? (Mark all that apply)

e. _X__ Virtual Private Network (VPN)
f. ___ SSH
g. ___ Terminal server
h. ___ HTTPS
i. ___ Other

9. Cloud-based servers (Y / **N**) Manufacturer / Type _____

10. Cloud-based storage (**Y** / N) Manufacturer / Type _____AWS___Gov Cloud__

11. Cloud-based applications (Software as a Service) (Y / **N**) Manufacturer / Type

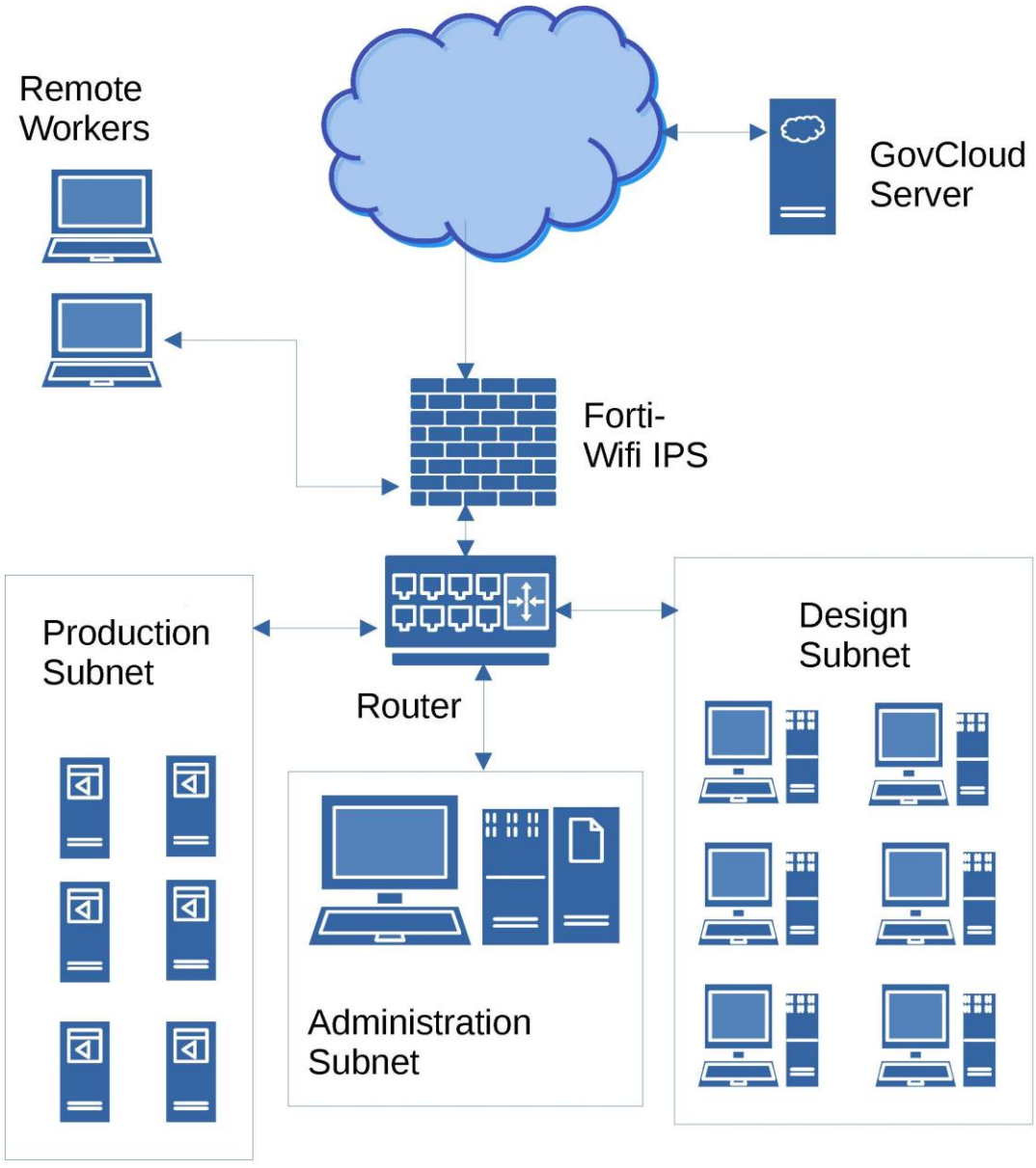
_____

12. Staff Experience

Total Number of People with Access to Protected Information ____17____

Total Number of People with Access and < 1 year Experience _____1___

Bobby Lee Welding Network Diagram

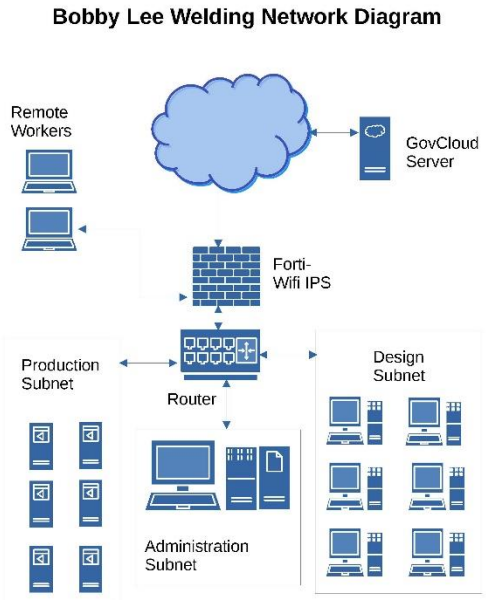


Network Security Auditing at Bobby Lee Welding

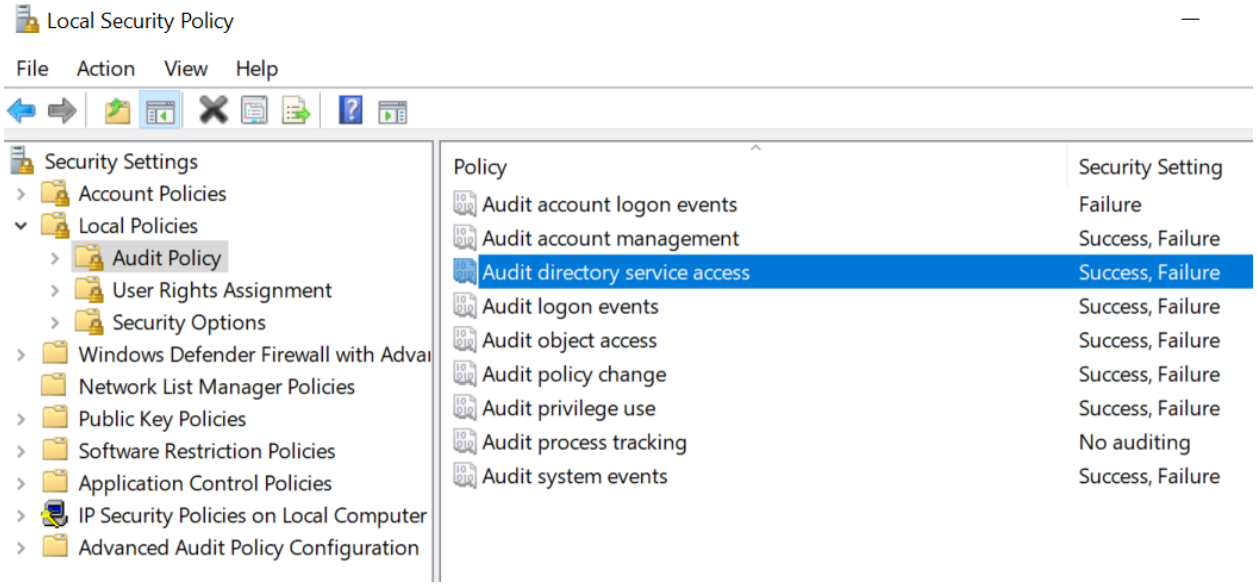
Auditing of network and computer functions is a major part of the DFARS cybersecurity program. Security auditing for the Bobby Lee Welding computer network shown at right involves two basic tasks;

1. Perimeter monitoring using a Fortinet Unified Threat Management (UTM) device.
2. Windows™ 10 monitoring using the built in Windows™ security policy (secpol.msc) and event viewer functions (eventvwr.msc).

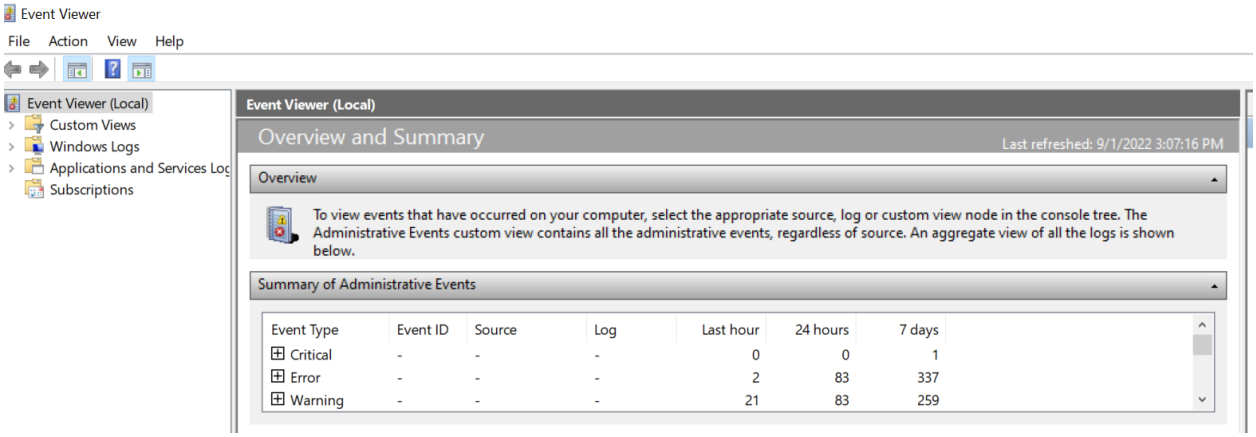
Perimeter monitoring is straightforward using the Fortinet reporting tools. The UTM logs attempted viruses, intrusions, warnings and alerts. This data is used as part of the ACRMS™ auto calculated NIST 800-30 risk assessment required as part of the DFARS 252.204-7012 System Security Plan (SSP).



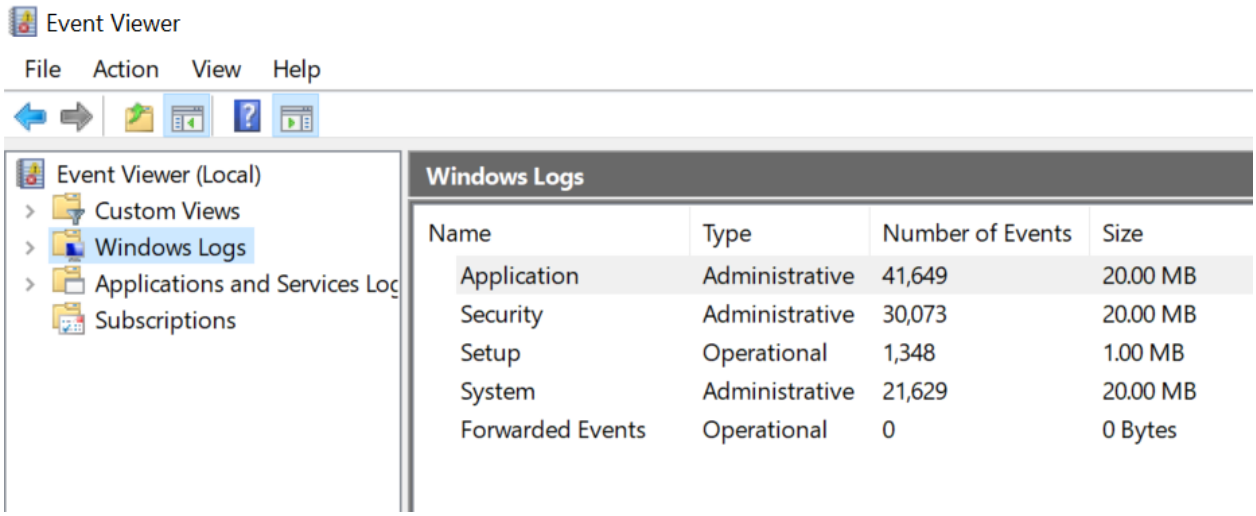
To set a security policy on a windows 10 machine click Windows™ key + R and enter secpol.msc. Clicking on "Local Policies" brings up a large number of options, as shown below. Audit Policy gives useful information about various events and functions.



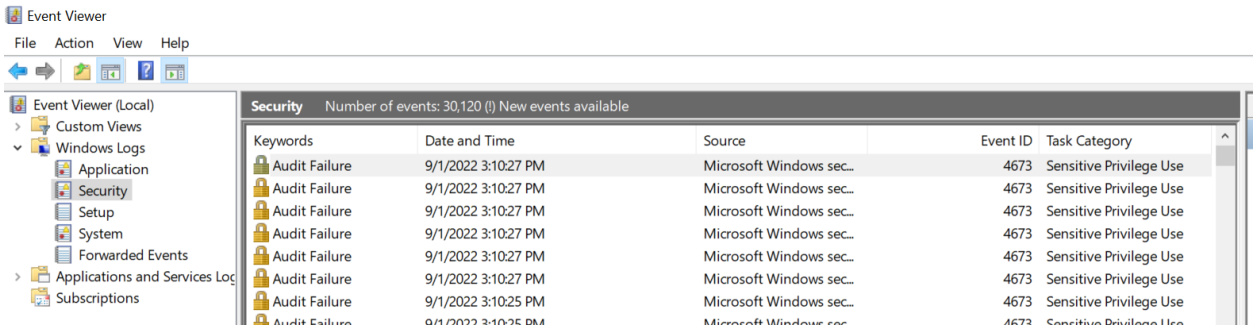
Periodic review of the audited policies is best done using the built-in Windows 10 Event Viewer. Click on Windows™ + R and enter eventvwr.msc.



Open the “Windows Logs” tab as shown below.



Typically the security logs and application logs will be of most interest.



Appendix D – Excerpt of Typical DFARS -7012 Tasks

The following pages show a partial listing of the tasks for a DFARS -7012 cybersecurity program. A full listing of tasks for meeting all 110 requirements of NIST 800-171 rev. 2 is more than 20 pages long.

NIST Safeguard	Freq.	Assignee	Task Description
AC-02 ACCOUNT MANAGEMENT	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.
AC-02 ACCOUNT MANAGEMENT	Annually	Compliance Officer	The <IT Manager> creates access control lists with specific access designated for each list member, including remote and local access. The initial list will be created within 90 days.
AC-02 ACCOUNT MANAGEMENT	Annually	IT Manager	The <IT Manager> reviews accounts for compliance with account management requirements <annually>.
AC-03 ACCESS ENFORCEMENT	Annually	IT Manager	The IT Manager will define how often the access rules review takes place, at least annually.
AC-04 INFORMATION FLOW ENFORCEMENT	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.
AC-04 INFORMATION FLOW ENFORCEMENT	Annually	IT Manager	Securing the direction of information streams between systems is the responsibility of the IT Manager. They decide which systems are sources of information and which systems may receive that information. Information flow within systems is also controlled.
AC-05 SEPARATION OF DUTIES	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.
AC-05 SEPARATION OF DUTIES	Annually	IT Manager	The security software on the computer system(s), managed by the <IT Manager>, prevents users from having all of the authority or all of the information required for access in order to prevent fraud.
AC-05 SEPARATION OF DUTIES	Annually	Compliance Officer	The Compliance Officer decides the proper divisions of responsibility.
AC-06 LEAST PRIVILEGE	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.
AC-06 LEAST PRIVILEGE	Annually	Compliance Officer	<Compliance Officer> shall designate a job description for each employee.

NIST Safeguard	Freq.	Assignee	Task Description
AC-06(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	Annually	IT Manager	Security level access shall be enforced by the <IT Manager>.
AC-06(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.
AC-06(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Annually	Compliance Officer	The Compliance Officer shall direct all staff to use non-privileged accounts or roles, when accessing non-security functions.
AC-06(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS	Annually	IT Manager	Procedures describing the configuration of system settings to capture the execution of all privileged functions in audit logs shall be written by the IT Manager.
AC-06(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS	Monthly	IT Manager	Privileged functions shall be logged and audited on a monthly basis by the IT Manager.
AC-06(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	Annually	Compliance Officer	Procedures describing the configuration of system settings to capture the execution of all privileged functions in audit logs shall be written by the <IT Manager>.
AC-06(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	Annually	IT Manager	Procedures describing the configuration of system settings to capture the execution of all privileged functions in audit logs shall be written by the <IT Manager>.
AC-06(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	Monthly	IT Manager	Privileged functions shall be logged and audited on a monthly basis by the <IT Manager>.
AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	Annually	Compliance Officer	The <Compliance Officer> reviews the policy and updates as needed.