

Finding the Right Security Control Assessor for Tribal Agencies

Division of Federal Systems

August 24, 2017



ACF

OFFICE OF CHILD SUPPORT ENFORCEMENT

First Step to Gain Access to the FPLS

To gain access to the FPLS, the first requirement is to submit an independent security assessment to OCSE so that we can determine compliance with the appropriate security measures.



Purpose of the Assessment

- Validate existing security controls and make a determination of a general security posture of an IT system.
- Provide detailed findings (if any) and recommendations to improve system security plans, procedures, and practices.
- Provide a line of defense in knowing the strengths and weaknesses of an organization's information system.
- Determine whether security controls in an information system are operating in accordance with federal requirements.

Acceptable Assessments

- Internal Revenue Service (IRS) Safeguard Review Report (SRR);
- Social Security Administration (SSA) Independent Verification and Validation (IV&V);
- A review conducted by an independent tribal auditing organization; or
- A review conducted by an independent auditing firm outside the tribal organization/agency.

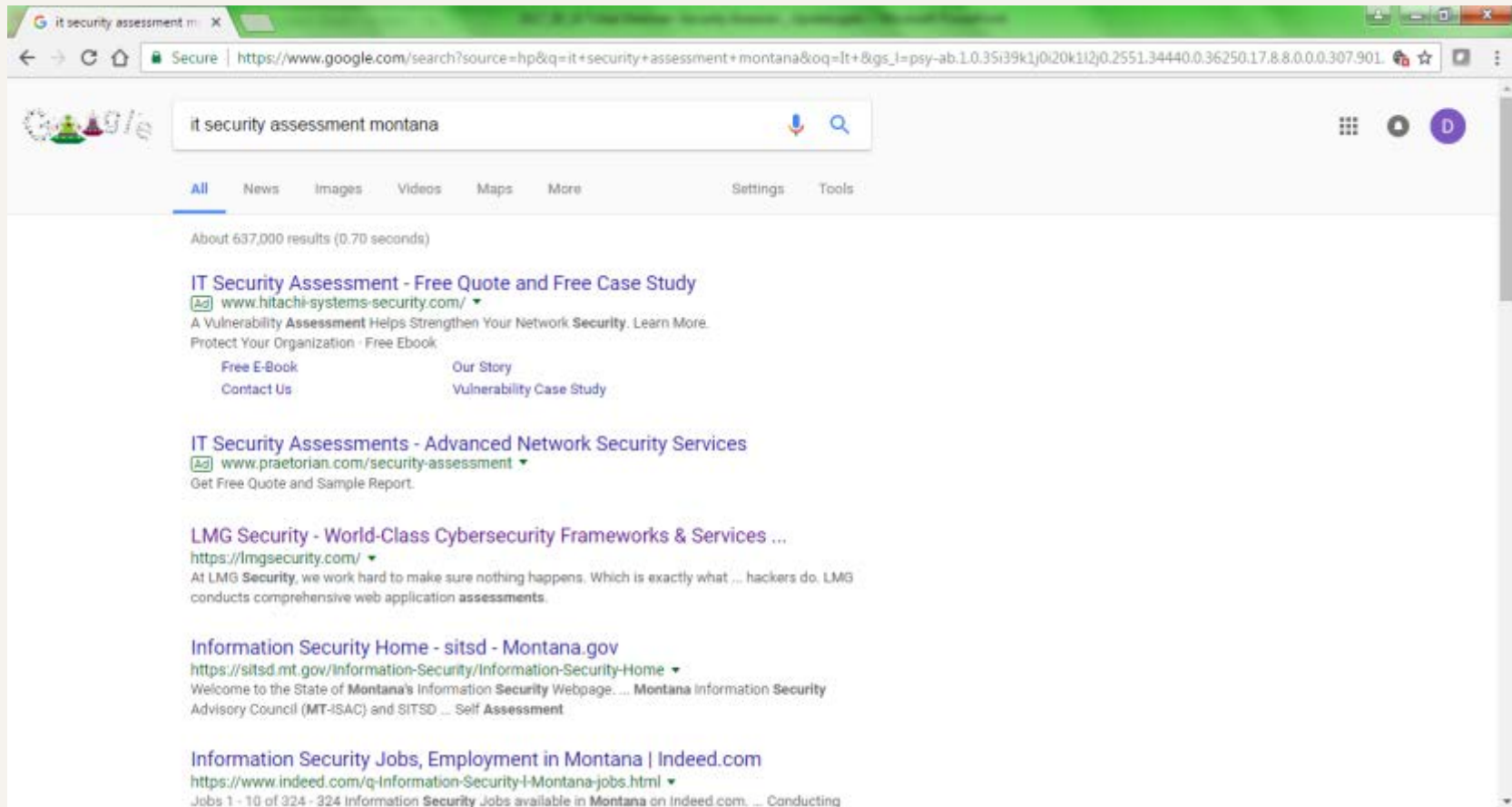
Qualifications of an Assessor

- An unbiased, outside entity.
- Competent independent evaluator, well versed in Information Assurance and IT cybersecurity technology, processes, and methodology.
- Use industry best practices and guidelines to conduct the security assessment (FISMA, NIST, OMB, IRS 1075).

What to Look for from Assessors

- Research various IT security companies in your area to determine if they are in the business of doing security control assessments.
 - Hint: Google searches are very effective in finding appropriate companies.
- Verify that the assessors have proper certifications/credentials.


Example: Google Search for Assessors





The screenshot shows a Google search results page for the query "it security assessment montana". The search bar at the top contains the text "it security assessment montana". Below the search bar, the "All" tab is selected, and the search results are displayed. The results include several advertisements and organic search results. The first advertisement is for "IT Security Assessment - Free Quote and Free Case Study" from www.hitachi-systems-security.com/. The second advertisement is for "IT Security Assessments - Advanced Network Security Services" from www.praetorian.com/security-assessment. The third result is for "LMG Security - World-Class Cybersecurity Frameworks & Services ..." from https://lmgsecurity.com/. The fourth result is for "Information Security Home - sitsd - Montana.gov" from https://sitsd.mt.gov/Information-Security/Information-Security-Home. The fifth result is for "Information Security Jobs, Employment in Montana | Indeed.com" from https://www.indeed.com/q-Information-Security-I-Montana-jobs.html.


it security assessment montana


About 637,000 results (0.70 seconds)

IT Security Assessment - Free Quote and Free Case Study
www.hitachi-systems-security.com/ 
A Vulnerability Assessment Helps Strengthen Your Network Security. Learn More.
Protect Your Organization - Free Ebook
Free E-Book Our Story
Contact Us Vulnerability Case Study

IT Security Assessments - Advanced Network Security Services
www.praetorian.com/security-assessment 
Get Free Quote and Sample Report.

LMG Security - World-Class Cybersecurity Frameworks & Services ...
https://lmgsecurity.com/ 
At LMG Security, we work hard to make sure nothing happens. Which is exactly what ... hackers do. LMG conducts comprehensive web application assessments.

Information Security Home - sitsd - Montana.gov
https://sitsd.mt.gov/Information-Security/Information-Security-Home 
Welcome to the State of Montana's Information Security Webpage. ... Montana Information Security Advisory Council (MT-ISAC) and SITSD ... Self Assessment

Information Security Jobs, Employment in Montana | Indeed.com
https://www.indeed.com/q-Information-Security-I-Montana-jobs.html 
Jobs 1 - 10 of 324 - 324 Information Security Jobs available in Montana on Indeed.com. ... Conducting

Examples of Assessor Credentials

- **Certified Information Systems Security Professional (CISSP)** – CISSP recognizes information security leaders with the knowledge and experience to design, develop, and manage the overall security posture of an organization. CISSP Concentrations recognize CISSPs who expand their knowledge into specific subject matter areas such as architecture, engineering, and management.
- **Certified Information Security Manager (CISM)** – The management-focused CISM is the globally accepted standard for individuals who design, build, and manage enterprise information security programs. CISM is the leading credential for information security managers.
- **CompTIA Security+** – This certification is globally trusted to validate foundational, vendor-neutral IT security knowledge, and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career.
- **Certified Authorization Professional (CAP)** – This credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

Examples of Agencies that Certify Systems Security Assessors

- **International Information Systems Security Certification Consortium, Inc. (ISC²).**
 - ISC² chapter locator:
<https://www.isc2.org/chapters/chapter-directory>
- **Information Systems Audit and Control Association (ISACA).**
 - ISACA chapter locator:
<https://www.isaca.org/Membership/Local-Chapter-Information/Pages/default.aspx>

ISC² Website

Chapter Directory

Meet your peers, make new contacts, network and build knowledge. Share solutions and ideas. Enjoy activities and events. And earn CPEs! Get involved with local information security professionals and join a chapter near you!

[Contact us](#) with chapter inquiries or concerns, [find chapters starting near you](#), or [start a chapter](#) in your community.

Chapter locations

Select a country

Map Satellite

Greenland

Iceland

Finland

Denmark

Norway

ISACA Website

The screenshot shows a web browser window displaying the ISACA website. The address bar shows the URL: <https://www.isaca.org/Membership/Local-Chapter-Information/Pages/default.aspx>. The page features the ISACA logo with the tagline "Trust in, and value from, information systems". Navigation tabs include ABOUT, MEMBERSHIP, CERTIFICATION, EDUCATION, COBIT, KNOWLEDGE & INSIGHTS, JOURNAL, and BOOKSTORE. The main content area is titled "Local Chapter Information" and includes a sub-header "ISACA > Membership > Local Chapter Information". A sidebar on the left lists various membership options, with "Local Chapter Information" selected. The main text describes the benefits of joining a chapter and provides sections for "Connect and Network" and "Locating a Chapter". A "Quick Links" widget is visible on the right side of the page.

Local Chapter Information

Learn about the benefits of joining a chapter, and how to locate a chapter in your area. With 200 chapters worldwide, there may be one close to your location.

Professional Membership

Recent Graduate Membership

Student Membership

Local Chapter Information

Browse by Map

Browse by List

Join ISACA

Membership FAQs

Code of Professional Ethics

Member Loyalty Levels

Member Get a Member

Member Tutorials

Connect and Network

As an ISACA member, you belong to a community of professionals that share mutual goals, interests and commitments. Becoming involved with your local chapter will allow you to make valuable connections with peers, share knowledge and discover new opportunities in your profession.

Locating a Chapter

ISACA has more than 200 chapters worldwide, all of which offer an opportunity to share a broad range of professional expertise from diverse business communities. Chapters sponsor local educational seminars and workshops, engage in IT research projects, conduct regular chapter meetings, and help to further promote and elevate the visibility of the IS audit, control and security professional.

To locate a chapter:

Browse by List

Browse by Map

Africa

Quick Links

I want to...	My Bookmarks	Saved Searches
• Explore certification opportunities		
• Find a local chapter exam review course		
• Join ISACA		
• Understand the value of membership		
• View member benefits		
• View member dues		

Please Login to View Your Quick Links
Please Login to View Your Quick Links.

Waiting for ads.isaca.org...

Why Security is So Important

- The goal of information security is to protect confidentiality, availability, and integrity.
- We have a duty to protect individuals' personal information that we collect—
 - To keep their personal identifying information (PII) safe from identity theft or privacy incident (breach);
 - To use data appropriately and only for the authorized purposes; and
 - To maintain data integrity and the public trust.

The Tribal Security Agreement

- The Blanket Security Agreement developed by OCSE sets the minimum requirements that tribes must have in place to obtain FPLS data under the current laws, policies, and regulations.
 - It is meant to protect individuals' PII and maintain the data integrity of the NDNH and FCR.
 - It is a compilation of federally mandated protections that all partners that obtain data with OCSE must follow.
- It was drafted based on access approved for tribes and set forth statutorily.
- This security agreement is designed as a form that can be quickly modified as security and statutory requirements change. However, it may not be modified except through established OCSE processes.

The Changing Landscape

- The federal government has rules for data maintenance, security, and use that all agencies are required to follow.
- Partners who are authorized to obtain data must also comply with these federal requirements for security and privacy.
- Because security issues change as technology develops, the laws, rules, and policies may change as well.
- OCSE is required to comply with any laws, rules, and regulations affecting data security regardless of when they become effective. Therefore, this security agreement may be updated to address changes in processes or technologies, as well as new or revised federal security requirements and guidelines.
- OCSE will provide the tribal child support agency with written notification of any changes and require written assurance from the tribal child support agency that it shall comply with the new or revised security requirements.

Security Controls

- Understanding your organization's security posture is extremely important in safeguarding data.
- Maintain security controls that are commensurate with the level of complexity of your IT system.
- System Security Plan (SSP), System Boundary, Network Segmentation, User Authentication/Access Controls, Vulnerability Management, Secure Configurations, Restrict Admin Privileges, Application Whitelisting, Patch Management, and Physical controls
- Defense in Depth - coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise.
- Note: This is not an exhaustive list. When it comes to security MORE is BETTER.

Security Controls

Security controls fall under 3 categories:

- Management
- Operational
- Technical

Referred to as the MOT security controls.

Security Controls

- Management controls – use planning and assessment methods to reduce and manage risk. Ex: Risk assessment, vulnerability assessment, etc.
- Operational controls – help ensure that day-to-day operations of an organization comply with their overall security plan. People (not technology) implement these controls. Ex: Security Awareness training, Contingency Plan, etc.
- Technical controls – use technology to reduce vulnerabilities. Ex: Firewall, Antivirus, etc.

OCSE is Here to Help

Contact your OCSE Tribal Coordinators and OCSE Security Team if you need any assistance during this process.



Contact Information

Paige Hausburg – Tribal Coordinator

Paige.Hausburg@acf.hhs.gov

202-401-5635

LaShawn Scroggins – FPLS Access Coordinator

LaShawn.Scroggins@acf.hhs.gov

202-260-4524

Karol Nangosia – Security Team Lead

Karol.Nangosia@acf.hhs.gov

202-401-5456

Derek Cullum – Security Engineer

Derek.Cullum@acf.hhs.gov

202-690-0029

Questions???

