

Division of Federal Systems

Finding the Right Security Control Assessor
for Tribal Agencies

2024

First Step to Gain Access to FPLS

To gain access to the Federal Parent Locator Services (FPLS), you must submit an independent security assessment to OCSS so that we can determine whether your systems comply with our security requirements.



Purpose of the Assessment

- **Ensure Compliance:** Verify that the program adheres to regulatory and policy requirements, such as federal requirements, organizational policies, and industry standards.
- **Assess Risk:** Identify vulnerabilities in the program's systems; provide detailed findings and recommendations to improve system security plans, procedures, and practices.
- **Support Decision Making:** Provide management with the necessary information to make decisions about resource allocation, risk management, and strategic planning related to security.

Acceptable Assessments

- IRS Safeguard Review Report (SRR)
- Social Security Administration (SSA) Independent Verification and Validation (IV&V)
- 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
- Uses industry best practices and guidelines to conduct the security assessment (FISMA, NIST, OMB, IRS 1075)

What to Look for From Assessors

- DISCLAIMER:

OCSS is not responsible for providing an independent assessor to conduct security assessments on behalf of the tribes. Each tribe is responsible for finding the right assessor for their compliance needs and requirements.

- 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.

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.

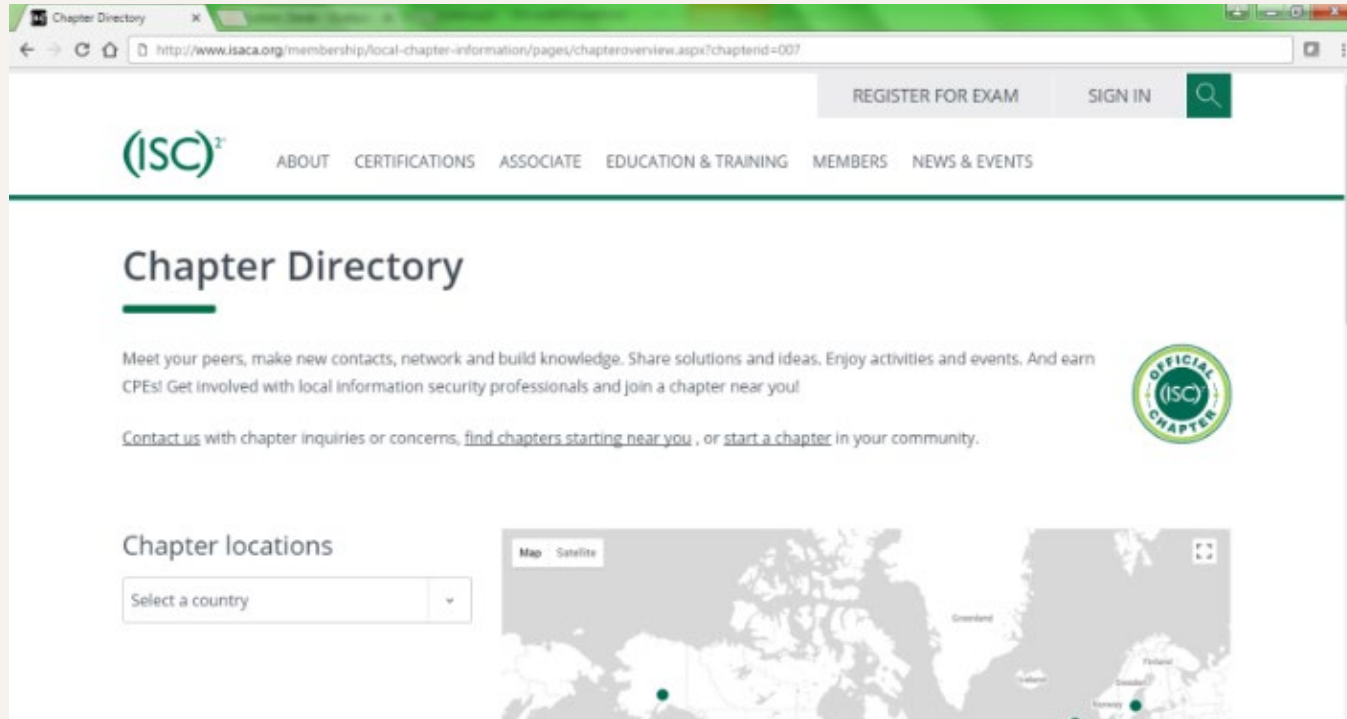
Examples of Assessor Credentials (cont'd)

- **CompTIA Security+** – This certification is trusted globally 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.
- **Certified Authorization Professional (CAP)** – CAP 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.

Agencies That Certify Systems Security Assessors

- **International Information Systems Security Certification Consortium, Inc. (ISC²).**
 - Link for the chapter locator for ISC²:
<https://www.isc2.org/chapters/chapter-directory>
- **Information Systems Audit and Control Association (ISACA).**
 - Link for the ISACA chapter locator:
<https://www.isaca.org/membership/local-chapters>

ISC² Website



ISACA Website

The screenshot shows the ISACA website's 'Local Chapter Information' page. The browser address bar displays 'https://www.isaca.org/Membership/Local-Chapter-Information/Pages/default.aspx'. The ISACA logo is at the top left, with the tagline 'Trust it, and value from, information systems'. Navigation tabs include ABOUT, MEMBERSHIP, CERTIFICATION, EDUCATION, COBIT, KNOWLEDGE & INSIGHTS, JOURNAL, and BOOKSTORE. The 'MEMBERSHIP' tab is active. The page title is 'Local Chapter Information'. A sidebar on the left lists various membership and chapter-related links. The main content area includes a 'Connect and Network' section, a 'Locating a Chapter' section with a map, and a 'Quick Links' sidebar on the right. The browser status bar at the bottom indicates 'Waiting for ads.isaca.org...'.

Local Chapter Information

ISACA

My ISACA

Site Content

SEARCH

Advanced Search

ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE & INSIGHTS JOURNAL BOOKSTORE

ISACA » Membership » Local Chapter Information

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

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...

The Importance of Security

- The goal of information security is to protect confidentiality, availability, and integrity.
- We have a duty to protect the information we collect to:
 - Keep their personal identifying information (PII) safe from identity theft or privacy incident (breach).
 - Use data appropriately and only for the authorized purposes.
 - Maintain data integrity and the public trust.

Tribal Security Agreement

The OCSS Tribal Security Agreement describes the minimum requirements tribes must have in place to obtain FPLS data under current laws, policies, and regulations.

- Protects PII
- Maintains the data integrity of the National Directory of New Hires and Federal Case Registry
- Covers federally mandated requirements for all OCSS data partners
- Details the type and frequency of security reviews or assessments

Tribal Security Assessment Type and Frequency

- **Annual Certification Statement:** The tribal child support program must submit a Certification Statement to OCSS each year by June 28 to affirm that it continues to comply with the security agreement. In the year in which the security agreement is signed, the agreement itself serves as the annual certification.
- **Independent Security Assessment:** Every three years, the tribal agency must arrange for an independent security assessment of the business processes involving FPLS information, child support program information, and the computer systems storing and processing this information.

The Changing Landscape

- OCSS must comply with all laws, rules, and regulations affecting data security regardless of when they become effective. Therefore, we may need to update the security agreement to address changes in processes or technologies as well as new or revised federal security requirements and guidelines.
- OCSS 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 will comply with the new or revised security requirements.

Security Controls

- Understand your organization's security posture.
- Maintain security controls, procedures, and artifacts commensurate with the level of complexity of your IT system, including (but not limited to):

System Security Plan (SSP), system boundary, network segmentation, user authentication/access controls, vulnerability management, secure configurations, admin privileges, application whitelisting, patch management, and physical controls

- Coordinate use of multiple security countermeasures.

Security Controls (cont'd)

- Security controls fall under three categories:
 - **M**anagement
 - **O**perational
 - **T**echnical
- Referred to as the **MOT** security controls

Security Controls (cont'd)

- 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 hardware and software to reduce vulnerabilities and protect systems against cyberattacks.
 - Ex: Firewall, Antivirus, etc.

OCSS Is Here to Help!

Contact your OCSS tribal coordinators and OCSS Security team if you need any help during this process.

Email OCSS Security at OCSSsecurity@acf.hhs.gov