Cybersecurity Analyst

Omar Elliottgreen

2021-08-02

# Three Steps to Achieving an Enterprise Certification

Certification/Authorization is one of the primary ways that an entity can demonstrate mastery of a subject. It allows two parties to objectively ensure that an agreed upon minimum standard has been met. Certification also allows a standardized method for testing of said mastery. A certification can also foster a continued relationship between entities. Given that most certifications are an inherently public endeavour, the success of the relationship can raise the perceived value of both parties.

## Step Outline

**The three steps to ensure that an entity is ready to attempt a certification:**

1. Identify and Understand the Objective
2. Inventory and Map
3. Document and Verify

# Understand the Objective

The first step in an effort to achieve any certification is to identify and understand the standards set forth by the certifying body. That is to say, the certification itself is a result of achieving the standards. That achievement is verified by a neutral third party with testing and review. Thus, in order to be successful, it is paramount to understand what is required and how it will be verified.

To illustrate the implementation of this approach, we can look at the Federal Risk and Authorization Management Program (FedRAMP).

[FedRAMP](https://www.fedramp.gov/) is the Federal approach to SaaS evaluation and authorization. In this case, identifying and understanding the standards is easily achieved by examination of the document used for final evaluation. There is little room for interpretation or deviation, thus providing a clear standard which must be reached, attested to, and evaluated in order to achieve certification.

The standards that are attested to, then evaluated for FedRAMP certification, are those set forth by the National Institute of Standards and Technology [NIST](https://www.nist.gov/). By using the publicly available and clearly defined standards of NIST, the path to achieving FedRAMP is clear.

While there are myriad NIST standards that must be adhered to and evaluated, the central defining standard for a SaaS IS is the Special Publication [800-53](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) Working from that definitive document, anyone attempting to achieve FedRAMP certification can identify exactly what is required regarding their IS.

# Atomic Mapping

Once the requisite standards set by the certifying body are understood, the next step is to ensure maximum situational awareness of the entity seeking certification.

In the case of FedRAMP, the provider of a SaaS Information System (IS) must be fully aware and able to describe **every** attribute of that IS. Some such attributes which must be attested to in documentation are:

* Security Technologies in use
  + Transport Layer Security
  + Secure Sockets Layer
* Encryption Methods
  + Full Disk Encryption
  + Tunneling Protocols
  + Virtual Private Networks
* System Interconnections
  + Platform as a Service (PaaS)
  + Security information and event management (SIEM)

While this is not an exhaustive list, the depth and breadth of the knowledge required to attest to those few lines is extensive.

# Document and Verify

Once the requirements of the certification are identified, and the IS is mapped, then, the next and most important step is to document the status of the IS.

## Documentation

The most prominant form of attestation regarding the technologies used and their implementation is a definitive document. Typically called the System Security Play (SSP), the documentation of an IS must detail every aspect within the scope of the certification. One concept used to limit the scope of documentation when attempting the FedRAMP certification is the Authorization Boundary.

By articulating an Authorization Boundary, the scope of the required documentation becomes finite and specific. This is particularly important when documenting a SaaS that utilizes either an enterprise or commercial Platform as a Service (PaaS). PaaS providers such as Amazon Web Services (AWS) or Microsoft Azure are common but by no means make up the entire field of PaaS offerings. However, they offer tremendously helpful, readily available documentation regarding what NIST 800-53 based security products, policies, and procedures they provide for their customers.

Once the boundary is identified, all IS attributes that exist inside that boundary must be documented. For example, the FedRAMP SSP is broken down into 13 documents that cover the majority of system attributes within a boundary.

1. System Security Plan (SSP)
2. SSP ATTACHMENT 2 - User Guide
3. SSP ATTACHMENT 3 - Digital Identity Worksheet
4. SSP ATTACHMENT 4 - Privacy Threshold Analysis (PTA)
5. SSP ATTACHMENT 4 - Privacy Impact Assessment (PIA)
6. SSP ATTACHMENT 5 - Rules of Behavior (RoB)
7. SSP ATTACHMENT 6 - Information System Contingency Plan (ISCP)
8. SSP ATTACHMENT 7 - Configuration Management Plan (CMP)
9. SSP ATTACHMENT 8 - Incident Response Plan (IRP)
10. SSP ATTACHMENT 9 - Control Implementation Summary (CIS) Workbook
11. SSP ATTACHMENT 10 - Federal Information Processing Standard (FIPS) 199
12. SSP ATTACHMENT 11 - Separation of Duties Matrix
13. SSP ATTACHMENT 12 - Laws and Regulations
14. SSP ATTACHMENT 13 - Integrated Inventory Workbook

By using this model of separate specific documents that pertain to an area of the IS, FedRAMP has provided a manageable framework. Specifically each area of the IS and the pertinent documentation can be updated and revised commensurate with the need of the component itself. Thus, when the company reorganizes, the IRP can be updated without changing the Rules of Behavior. Thusly, when new legislation is introduced requiring adherence, the Laws and Regulations document can guide the requisite changes in the SSP.

## Verify

By endeavouring to document an IS with %100 coverage, it becomes pivotal that the documentation be reviewed and verified by more than one party. Thus, one method utilized by successful entities is to create and maintain an internal team who’s mandate is to verify the veracity of any documentation used as part of the SSP.