Assessing Software as a Service Systems

Synopsis: An introduction to assessing Software and Platform as a Service (SaaS/PaaS) systems using the NIST 800-37 risk management framework.

The A&A Process Is:

Accreditation and Authorization or “A&A” is the methodology derived from the NIST standard 800-37, and is the method of applying a particular type of Risk Management Framework to IT systems. This name reflects the two major aspects of the process all IT systems should follow.
Accreditation refers to the process of defining and evaluating an IT system, which is well understood as a “SA” (Self Assessment), “SAR” (Site Audit Report), “SAS70” or that the system is being “Certified”. This lengthy process consists of understanding the scope of the system, categorizing the sensitivity of the data, describing the business functions and technical processes, evaluating the system against a standard framework via interview, analysis of documentation and configurations and vulnerability scanning. The goal is to deliver a “Plan of Action and Milestones” that seeks to mitigate risks.
Authorization refers to the process of documenting overall IT Security and Continuity Plans, and formalizing the POA&M, Categorization/Privacy, and Vulnerability results. The goal is to deliver a recommendation for the overall system, which usually boils down to:

- Authorized: the system is sufficiently secure to operate and should continue to address issues itemized in the POA&M.
- Conditional: the system has significant flaws that must be addressed within a given time period, where upon the system is re-evaluated.
- Not Authorized: the system has fatal flaws and must have all outside connectivity disconnected until the flaws are addressed.

All SaaS’s have two security “domains”, the SaaS system and the customer system. Complex SaaS systems (and PaaS) will have three, the SaaS system, the customer organization and minor applications within that customer organization.

SaaS Scope:

At the “bottom”, the Cloud SaaS Accreditation and Authorization covers security controls at the physical, operating system and application level not customizable by the organization.
An example: is there redundant power run to the servers (control PE-9(1) for 800-53, 11.1 for ISO27002)? Since this issue is covered by the data center hosting the server running the SaaS, this control would be the responsibility of the SaaS provider. Often the SaaS provider purchases or leases data center space or servers from a vendor such as Amazon Web Services, Bluelock Inc., Joyent Inc., etc. It still behooves the SaaS provider that the vendor is providing as promised. This can be done internally, but is most often satisfied by the vendor providing the results of an independent audit (usually a SAS70 or equivalent).
The Customer A&A would document any settings that are customizable, providing a determination as to whether the setting is static to the organization or is available to individual applets.

An example: how does a user access their data (control AC-2 for 800-53, 9.2 for ISO27002)? The application can use internal access controls via a database, or provide SAML v2 calls to the organization's Access Control system.
What's left is to document only security controls specific to the application.
An example: how does the business provide separation of duties (AC-5 for 800-53, 9.4 for ISO27002)? Is there data that should not be seen by the entire organization? Applications that should only be run by certain users. This is handled by putting the correct users in security groups, either on the application or (more often) within the customer's security infrastructure.

Categorization via FIPS-199:

The categorization process has a complete list of data types and recommended ratings. The customer itemizes all the data types that will be contained or processed by the system. The recommendations provided are considered in making a determination on the rating of that type. Where the recommendation is not taken, the rational is documented and the aggregate will be pretty obvious.

Many SaaS systems are designed to carry specific types of customer data, so even before customer interaction this process will provide significant insight as to the level of effort that will provide a proportional level of protection for that data. This process will also provide the rational for why certain types of data might need to be separated. For example, medical data under HIPAA is very sensitive and would produce an aggregate rating of high, requiring extra safeguards and extra effort to A&A.

Under 800-53A, systems categorized as "Low" have 127 controls, "Moderate" have 264 controls, and "High" have 384 as of Revision 3.

Privacy Impact Assessment:

The Privacy Impact Assessment documents the determination of whether the system will contain privacy data at all via two qualification questions. If the answer to both questions is "No", then the PIA can be completed on that basis. A "Yes" to either question will ensure a deeper dive into exactly what the data is, and infrastructure around the privacy data during the next phase. It is important to note that a "Yes" doesn't stop the process, it just adds to the level of effort to secure the system due to the increase ramifications of an exposure.

An effort to document how the accuracy, timeliness and completeness of this data is verified by the Data Owner.

The system's PIA document is the aggregate of all the elements, attested to by the System Owner and Authorizing Official and provides the basis for a "Statement of Records Notice" or any other required Privacy Declaration.

Document Grinding:

Gathering the documentation as soon as possible, regardless of it's state, is important so that policies and culture can be analyzed while the technical control analysis is going on (which takes a lot longer). It will also be important to have processes and procedures handy when doing the review to understand "as stated" versus "as delivered". Examples of documents include:

- Policies: Acceptable Use, General IT, Telecommuting, etc.
- Procedures: Add/Delete User, Backup/Restore, Patch
- Checklists: System Shutdown, Evacuation
- Inventories: Lists of systems by IP or OS, Lists of Software and Licenses
- Network Topology: List of networks and how the connect
- System Architecture: Diagrams of how infrastructure is interconnected
- System Summary: Business or service functions of systems

- VISA PCI DSS Compliant or that have a McAfee Secure Seal or TrustGuard Quarterly Scanned Seal (if so, provide the results of their latest scan)
- Terms of Service
- Web Application Scans (e.g. WebInspect, Acunetix, Burp Suite Pro, etc.)
- Operating System Vulnerability Scans (e.g. Nessus, Qualys, nCircle, McAfee Foundstone).

The System Description:

Now begins the process of creating a “System Security Plan” (SSP) to chart the path between where the system is now, and where the System Owner wants it to go. The SSP’s function is to demonstrate to executive management the long term information security strategy.

We’ll start the process by using existing documentation such as the monthly inventory, previous SSPs, web sites or any other documentation the custodians can provide to create a “System Description” document stub, we’ll add to this document any gaps that will need to be addressed, and highlight areas of focus. We’ll also identify documentation that needs to be created, or existing documentation we were supplied that needs updating.

Now that the foundation of the system is well understood, it’s time to start framing. Gather the roles and who is responsible for each role.

The Authorizing Official will be an individual ultimately responsible for the entire system.

The System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. If your an ITIL person, the Service Owner is closest to that role. The System Owner works with the Custodian (if separate), who safeguards the system via patching and configuration changes).

The Security Officer is the advocate for security on the system, providing risk information along with the Custodians cost of remediation so that an informed mitigation decision can be made by the system owner. The Security Officer is also responsible for ensuring an accurate and meaningful A&A is performed periodically, or continually where possible.

The Data Owner for SaaS systems is the customer paying for the service. The Data Owner must ultimately take complete responsibility for the use, safety and accuracy of the data on the system. The Data Owner must ultimately decide on what configurable controls and access methodology is appropriate for their data and culture.

After roles and responsibilities are assigned, the business function of the overall system is documented, and then the business function of each service. Start by describing the business functions that the element delivers to it’s customers via an executive summary style description. This can be followed by a more in depth description if desired.

Similar services that use identical equipment or software should be grouped together.

With each service provided, provide a description (and picture where feasible) of the architecture used to implement the service. Include number of servers or Virtual Machines, operating systems used, software used, and any management tools used to support the system that doesn’t directly provide part of the service.

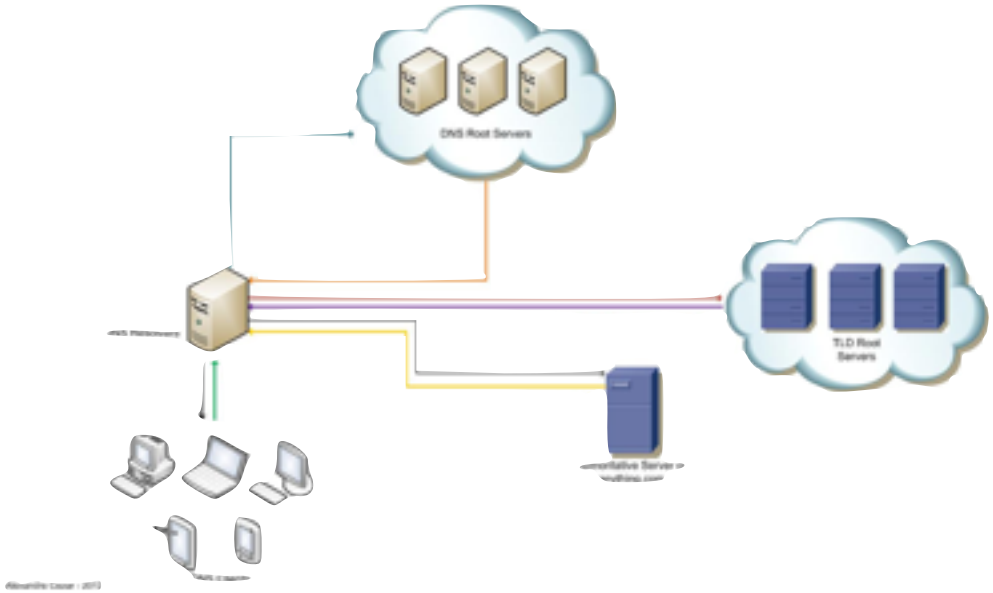
Most often missed or ignored are the interconnections. Make sure to completely document any connections outside of the defined system, such as to business partners, providers, auditors, etc. Include in the interconnection, networking information, any protocol specifications, bandwidth used, communications medium, encryption used, etc. Access to the system via these interconnections are not within the AO’s control and may not utilize the same diligence to protect the AO’s customers.

Finally, while rare, a description of services provided to the entire organization that weren’t discussed is included. This is most often functions performed in support of business continuity or incident response, but also could be “orphan” processes that are being phased out or transitioned to leverage existing infrastructure.

Creating the System Description (and descriptions of services within the system) is performed by doing an initial briefing of the stub, and repeated interviews with custodian stakeholders and support personnel with a Technical Writer who performs the document creation. A Security Specialist that ensures the content is sufficient to meet project requirements. The Security Specialist will also be gathering information on areas to highlight or that will require a "deeper dive".

Here's an example of a system description. "A picture and a paragraph" is more than sufficient. Procedures, processes and configuration documents supporting the system and services should be kept separate and only referred to by name or link.

Domain Name Service (DNS): The Domain name service is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for the purpose of locating and identifying computer services and device with the underlying network protocols.
There are 5 DNS systems deployed in OrgSaaS Corp. The DNS system currently maintains 31 domains, both forward and reverse domains, using a split-brain configuration separating OrgSaaS Corp intranet, internet domains along with capability for 250 customer named sub-domains. These systems are configured for fault-tolerant and high-availability using Cisco Content Services Switch (CSS) and Multi Node Load Balancing (MNLB).The system is managed from a central point with a master policy pushed to all systems. The master is running Solaris 11 with 2 Red Hat Fedora Linux servers, and 2 Windows 2012 servers.



800-53A Control Responses:

Now that it is well understood what the system is made up of and how it's put together, it's time to understand how its secured. In this model provide responses to "security controls". Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks relating to computer systems. My favorite example is AC-8: System Use Notification, Displays to users a system use notification message or banner before granting access to the system.

The response would be:
An Active Directory Global Policy Object is implemented to the Security Option “Interactive logon: Message text for users attempting to log on” is “This OrgSaaS system is for authorized users only. Individual use of this computer……”.

The goal is to assist in documenting SaaS strategies and methodologies to remove or reduce risk in the most useful and practicable way.

Divide and Conquer:

While every control must be accounted for, sometimes the answer is simple as the control is simply not relevant. Make sure to document why the control is not applicable. The response for SC-19: VoIP for example, would likely be “This system does not contain VoIP phones and is not applicable.” This control now need not be on the control review agenda, saving time. An important part of the process is to fully document who is responsible for which control. Some controls are applicable to the SaaS and some to the data and hence the customer/Data Owner.

Roadmap for Delivery:

Now the long road of reviewing all the applicable and relevant controls beings. A Security Officer or delegated Security Specialist will team with the System Owner and Custodians to discuss the responses.

Implemented responses will include the description of how it is implemented on every server/network/application in the system. Bonus note: Leveraging common solutions such as one Directory Service for all Authorization and Authentication saves time and money in this process as well as others.

Partially Implemented responses will include the description of how it is implemented and a brief description of how much of the system is secured in this manner (no more than a sentence).

Planned controls will include a recommendation on how it might be closed in the future. Inherited controls responses will include a brief description of how it is implemented, who is implementing it, and any SLA.

A list of gaps is made, and the plan to close the gap is developed during POA&M development later on.

The goal is to assist in documenting system configurations, strategies and methodologies that remove or reduce the risk presented by the control in the most useful and practicable way.

It is important to note that it is counter productive to create the fiction that all the controls will are being or will be addressed. There are always gaps, and that’s ok. What’s not ok is to not have a plan on how the custodian should look to address it (a management response). For controls that don’t have answer, work should begin determining a recommended solution and document it in the SSP as a “Planned Activity”. At the end of the project is an activity that will organize all of these activities into an overall project plan. Whitewashing gaps, or playing whack-a-mole to make the SSP sound good will make the Risk Assessment piece significantly longer and often results in a less than favorable final recommendation.

The 800-53A Control Family:

The controls are broken down into three categories: Management, Operational, and Technical and then down into “families”.

The management control family describes the measures that focus on the management of risk. The RA, PL, PM, SA and CA families are predominantly handled by policies and guidelines, support contracts, etc. Any questions in this area will usually revolve around verifying that the various policies apply, and requires only custodian and stakeholder management. This section is often completed in one short meeting depending on the level of connection to agency policies. Heavily silo’ed systems will take longer as they often employ “ad-hoc” policies that must be captured.

The operational control family describes the measures that focus on mechanisms that are primarily implemented and executed by the systems management, administration, and technical support personnel. These security controls were put in place to improve the overall security of the environment. Systems that don't leverage organizational infrastructure (such as the organizational or contracted data center, or the agency standard incident response procedures) will take a significant amount of time to capture ad-hoc processes, policies and de-facto standards.

The custodian and stakeholder management along with an operations person will be required to attend this session. Due to the length these sessions can go, it is best to limit discussions to 2 hours per day as quality suffers dramatically after that point.

The technical control family is used to minimize or prevent unauthorized users from accessing the system and to ensure integrity, confidentiality, and availability of the system. This section is the most tactical, and will take the longest. Where systems leverage existing infrastructure little time will be needed. Specific system configurations will also need to be captured, which is best done via conformance to CIS standards or documented configuration standards. Heavily silo'ed systems or where there are diverse system configurations take longer, as they often employ "ad-hoc" policies that must be captured.

The custodian and stakeholder management along with an operations person will be required to attend this session. Where signification leveraging to LDAP or other system wide AAA is utilized, a representative from that team should also be available. This section often takes the longest to complete, expect several session will be needed to complete this area.

The Control Assessment Process:

The control assessment for large systems can literally take months. The most effective means to slog through the assessment is via conference (VTC works well when screen sharing is available).
For each session the Security Specialist is responsible for providing list of controls and discussion points.
The System Owner responsible for ensuring SMEs participate.
Each assessment session is 2 hours or less. The last 30 minutes reviewing the gaps found, and discussing potential mitigation strategies.
Repeat until all applicable controls reviewed and have practicable responses.
Ensure that a collaboration file system (such as Sharepoint or Google Drive) is set up as a repository for SOP's, configurations, spreadsheets and whatever hard data the System Owner and Custodian wish to supply.
A first draft of the System Security Plan can now be sown together from the data gathered. The System Owners must proof the documentation relevant to their area and then must be willing to certify to it's accuracy. The System Security Plan will change very little after this point, as it must represents the System Owners view of how the system is secured.

Note: The level of engagement of the System Owner in this process can determines the success/failure of the approval or cause significant delay.

A start to POA&M can now be made…

The Business Continuity Plan:

The next phase is to build an Information System Continuity Plan. This plan contains the completed System Description from SSP, and documents that focuses on identifying and maintaining the constant ***availability*** of critical processes and information across the business enterprise.

The Continuity Plan provides plans and documentation for the vast breadth of the system, each service will need to have specific details on Damage Assessment, Recovery and Resumption. From this information, and up to date contact list and initial instructions form a “Jumpstart” document that the System Owner and element Custodians would use in the event of an incident activation.

For personnel new to their role or that desire a refresher, a briefing can be provided so that a consistent set of plans across all elements is produced.
Start the process by using existing documentation such as the monthly inventory, previous ICSPs, web sites or any other documentation the custodians can provide, then add to this document any gaps that will need to be addressed, and highlight areas of focus. Also identify documentation that needs to be created, or existing documentation that was supplied that needs updating.

As in the SSP phase, an initial briefing of the stub, and repeated interviews with custodian stakeholders and support personnel should occur. A Business Continuity Specialist will also be gathering information on areas to highlight or that will require a “deeper dive”, and recommend strategies for areas identified as gaps. Elements with mature continuity plans or that contain redundancies that can span an incident will take very little time to complete, and can usually be covered in one session.

Plans will be turned over to the System Owner for review. A session with the element custodian will cover areas that were flagged but can be easily completed, areas of concern that an independent audit might question, and open questions that the custodian has.

The ISCP will then be assembled, and finalized. Unless the system is mature and has few vulnerabilities, it would be unwise to schedule a test of the ISCP while the A&A process is still going on.

The Risk Assessment:

As the Control Assessment wraps up, risk assessment can begin. This is a three step process with the goal of producing a System Security Plan, POA&M, and Risk Assessment that accurately reflects the cultural, strategic, and tactical gaps between “as documented” and “as delivered” along with solutions that don’t meet industry best practices.
The Risk Assessment process happens in three phases:
Document grinding starts at the beginning of the process, but while it continues in parallel during the control assessment; it must be frozen once Risk Assessment starts lest scope creep occurs. This “freeze date” will feature prominently on the Risk Assessment as the results are 100% valid only for that specific point in time.
Additional interviews may be needed to dive down into issues raised or where inconsistencies are found.
Configuration Capture, Vulnerability Scanning and Code Scanning should be scheduled as late as possible so that the results arrive as close to the “freeze” date as possible.
Results are in the form of “findings” or “vulnerabilities” are denoted on the Risk Assessment. Change only the status of the control on the System Security Plan as appropriate (from Implemented to Partially Implemented for example). Examples would include but are not limited to: Insufficient response to the control, the control not fully implemented system wide, the control not implemented as stated by the response, the configuration is vulnerable to attack, the response does not meet industry best practices, etc.
When the RA is complete, provide a complete review to the System Owner, who should be assisted in providing a mitigation strategy for every finding. Each one is a risk management decision which should be fully explored in the RA document.

The Plan Of Action and Milestones:

The Plan of Action and Milestones is a project list containing the vulnerability, target dates, strategies, and resources needed to remediate:

Gaps identified by the Control Assessment, Outside Audits (such as penetrations tests) and vulnerabilities known not to be mitigated (from sources such as CERT, and vendor updates), and accepted findings in the Risk Assessment.

Final Assembly:

With the completion of the ISCP, the final assembly of the A&A/Continuous Monitoring documentation package can be completed. The package includes the SSP, ISCP, Risk Assessment Report or independent Site Audit Report, Vulnerability/Web/Database Scans the POA&M and any Penetration Test results.
From these documents, the “Accreditation Letter”, a recommendation is made whether to Authorize, Conditionally Authorize or Not Authorize the operation of the system is created and attested to by the Security Officer.
The “Authorization Letter” attests that the “Accreditation Letter” and all the other documents were considered by the Authorizing Official and they Authorize, Conditionally Authorize or Not Authorize the operation of the system for a given period of time (usually 3 years).
Depending on the maturity of the system, an optional “Continuous Monitoring Plan” is created to describe how the system is maintaining an ongoing awareness of information security, vulnerabilities, and threats that support organizational risk management decisions. It documents how the system maintaining situational awareness of all systems across the organization; maintains an understanding of threats and threat activities; constantly assesses all security controls; collects, correlates, and analyzing security-related information (usually via a SIEM); provides actionable communication of security status across all tiers of the organization; and show how active management of risk by organizational officials is accomplished.

Review:

Phase 1, Qualification: Scope, Categorization, Document Grinding
Phase 2, Build the SSP: System Description, Architecture, Control Review, ISCP
Phase 3, Final Assembly: Risk Assessment, POA&M, Accreditation Letter, Authorization Letter