Black Box FISMA-based Security Control Assessment of Public Cloud Providers

Gerald Auger  
*Dakota State University, gmauger@dsu.edu*

Richard Hilgers  
*Purdue University, rhilgers@purdue.edu*

Follow this and additional works at: [https://louis.uah.edu/insure-conference](https://louis.uah.edu/insure-conference)

**Recommended Citation**  
[https://louis.uah.edu/insure-conference/INSuRECon-16/Papers/3](https://louis.uah.edu/insure-conference/INSuRECon-16/Papers/3)

This Paper is brought to you for free and open access by the Conferences and Events at LOUIS. It has been accepted for inclusion in Information Security Research and Education (INSuRE) Conference by an authorized administrator of LOUIS.
Black Box FISMA-based Security Control Assessment of Public Cloud Providers

Gerald Auger
Dakota State University
820 N Washington Ave.
Madison, SD 57042
1.888.388.9988
gmauger@dsu.edu

Richard Hilgers
Purdue University
610 Purdue Mall
West Lafayette, IN 47907
1.765.494.4600
rhilgers@purdue.edu

ABSTRACT
Public cloud computing solutions are desirable for business and government agencies to outsource infrastructure technology requirements. This decision transfers the responsibility of certain security controls to the cloud provider, and impacts the ability for system owner oversight of security. Government agencies are required by law to conform to the Federal Information Security Management Act of 2002 (FISMA) that outlines a collection of security controls that must be implemented. Cloud service providers therefore have to implement these controls, at a minimum, to be valid for government usage. Given the known library of controls that must be implemented by the Cloud service provider, this paper identifies 9% of FISMA-based NIST 800-53 security controls can be validated externally by an end-user of a cloud service provider with confidence.

CCS Concepts
• Security and Privacy→Distributed Systems Security
• Security and Privacy→Systems Security.

Keywords
FISMA; cloud-computing; FedRAMP; security assessment; black-box; NIST

1. INTRODUCTION
Federal agencies are directed to evaluate cloud-computing solutions before implementing internally managed IT infrastructure, and must still adhere to federal information security requirements [6]. Cloud providers are being assessed and authorized by objective third-party organizations through the Federal Risk and Authorization Management Program (FedRAMP), authorizing them for federal agency usage. Federal agencies can select an authorized cloud provider to host their programs IT infrastructure. A byproduct of this approach results in an inability for the agency itself to validate program security control effectiveness.

These agencies would benefit from an ability to independently validate the effectiveness of security controls that have been implemented by and are the responsibility of the cloud provider. This independent validation can only be executed from an end-user perspective, the perspective of an administrator or non-privileged user of the cloud-computing platform. Figure 1 depicts the lack of security control assurance federal agencies have with Cloud IT and how providing security control visibility (yellow arrow) provides security posture intelligence.

The security of the information hosted by the cloud systems is the responsibility of the cloud service provider. Therefore, agency decision makers must rely on third-party organization’s independent assessment of the cloud provider’s security controls.

Figure 1-Current and Future Cloud Security Visibility

This paper documents an approach to assess a subset of security controls, regardless of cloud provider. This approach increases visibility into the effectiveness of the security controls protecting their system, and identifies the limit of this visibility.

2. LITERATURE REVIEW
Cloud computing is an IT paradigm where Internet accessible shared IT resources can be leveraged by entities instead of establishing a traditional internal IT infrastructure. The shared, Internet-accessible cloud computing model allows for agile IT infrastructure scalability, redundancy and elasticity at a reduced cost enabling robustness in business IT continuity and fostering innovation. Cloud computing, offered through commercial cloud service providers (CSP), can provide organizations the opportunity to transfer the responsibility of key information technology (IT) elements. This IT paradigm is an appealing direction that allows organizations to afford reliable, scalable and on-demand technology resources in multiple service offerings.

The federal government values the flexibility and cost-saving benefits cloud computing offers. This endorsement and direction of moving federal agency programs to cloud computing platforms was strengthened and supported through the enactment of the “Cloud First” policy. The “Cloud First” policy requires federal agencies to evaluate a variety of cloud options before making any IT investments [6]. FedRAMP was established to centralize and streamline federal agencies processes of evaluating reliable cloud service providers for their needs.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and
continuous monitoring for cloud products and services [3]. FedRAMP leverages the NIST 800-53 security controls as the security requirements CSP’s have to meet. Federal agencies are required to implement NIST 800-53 security controls to be in compliance with the Federal Information Security Management Act (FISMA) of 2002 [1]. CSP’s having to implement the same security standards aligns to the agency’s FISMA requirements and makes adoption, integration and agency-awareness of control implementation more effective.

The benefits of agility, efficiency and innovation come with additional risks. Some responsibilities for the organization’s information security controls are transferred to the CSP. The cloud consumer now has to weigh the trust and reliability of the CSP when managing the risk to the program. This trade-off is a significant concern as noted in the cloud security alliance 2015 survey of 212 IT and security professionals that showed 73% of respondents described the top challenge holding back cloud projects was concern about the security of data [2]. These benefits are important to the federal government from a cost savings and efficiency perspective. FedRAMP is in place to assist in mitigating that risk and make pursuing migration to a cloud-computing platform a safer, more secure option.

From 2009 to 2011 the Office of Management and Budget worked with an alliance of public and private sector organizations to develop a program, in concert with the Obama Administration International Strategy for Cyberspace and Cloud First policy that supports federal government adoption of cloud computing solutions in a responsible manner. The program, called FedRAMP, establishes policy, guidance and tools to define security requirements, provide objective security assessment cases and standardize contract language. Additionally, a reduction in cost can be realized by agencies by leveraging an existing CSP’s Authority to Operate (ATO), instead of the classic approach of each program having to seek their own ATO [3].

FedRAMP relies on the security controls defined in NIST 800-53 for a low or moderate baseline with additional controls required specific to cloud computing security risk [4]. Prior to a public CSP being authorized to host federal agency clients, they must document how security controls are implemented, have those security controls assessed and receive an ATO. It is the cloud providers’ responsibility to implement these required controls and have a certified independent third party organization assess the controls for validation. This guarantees minimum-security compliance with the 800-53 standard.

Information technology is a fast changing environment and minimum compliance does not equate to maximum security. CSPs are independently assessed by certified organizations for the entire in-scope security control set, put forth by FedRAMP. Additionally, CSPs are legally required to receive annual reassessments to maintain an ATO [5].

Step six of the federally required NIST 800-37 risk management framework is to monitor and accept the ongoing level of risk [7]. The transfer of ownership of some security controls introduces a challenge for an agency to perform this step. Annually, a third party assessor reassesses the security controls for the cloud provider. This provides some assurance to the status of the security controls. Ultimately it is the responsibility of the authorizing official over a program to authorize a program’s security controls, both cloud controlled and organizationally controlled [7]. This decision has to be made based on the efforts of parties not affiliated with the agency.

FedRAMP requires 325 security controls for a moderate security baseline [8]. These controls provide compliance with the minimum-security requirements, but do not address all threats and associated risks. For example, an availability risk not addressed relates to the confiscation of physical hardware that is directly hosting an agency’s data at a CSP, in support of a law enforcement investigation. Identifying these risks allows an organization to determine what controls would be appropriate. Furthermore, an agency can develop additional security control test cases and incorporate into a FedRAMP aligned self-assessing methodology. This would provide an agency more accuracy in calculating risk and ensuring risk aligns with the agency’s risk appetite.

3. METHODS AND PROCEDURES
An exploratory research method was used to develop an approach for understanding what FedRAMP security controls for a moderate security baseline can be assessed from an end-user perspective for a cloud computing platform.

Each security control is composed of one or more control objectives. For example, having a contingency plan (CP) is a control. Three control objectives for this control include the CP has recovery metrics, addresses contingency roles, and addresses assigned individuals with contact information.

There are 164 unique controls within the FedRAMP moderate baseline, and there are 161 control enhancements. A control enhancement is an additional risk mitigation aligned to a security control. For example, AC-17 is a security control focused on remote access risk. The control requires documented usage restrictions, configuration/connection requirements, implementation guidance for each type of remote access allowed, and that remote access is authorized prior to allowing such connections. AC-17 control enhancement 1 requires remote access be monitored and controlled. Both of these items are required in a moderate baseline. For this research, each control enhancement is identified as a unique control that is aligned to a similar risk area as the control it enhances, as noted in this example. This supports the value of 325 (e.g. 164+161) controls in-scope of the research.

The methodology to determine the feasibility of a security control being end-user assessable was based upon NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. The NIST SP 800-53A is developed to apply to the controls in NIST SP 800-53, the same controls FedRAMP requires cloud service providers to implement, to become available to host federal programs. The 800-53A outlines testing procedures for assessors to execute to test a controls validity by defining testing procedures for each control’s objectives. For each control objective, the procedure was evaluated to determine if it was possible to execute from the end-user perspective. If all control objectives aligned to a control were assessable from the end-user perspective, then that control was included in the set of CSP implemented controls that could be effectively tested by the end-user organization.

Each control was initially reviewed to determine if it was a managerial, operational or technical control. Managerial refers to a control that comes from individuals being put into a place of

1 The term control and control enhancement should be used interchangeably for this research.
authority to accept the risk and accountability of the system. Operational means controls associated with processes such as audit log reviews and incident response testing. Technical means controls that are implemented through a configuration of a system such as password complexity enforcement or audit log generation.

An additional category, physical, was identified that can cross-cut operational or technical. Physical indicated controls that are physical in nature outside of the information system such as the presence of fire extinguishers or water shutoff valves. These could be assessed via a physical walkthrough, and therefore received a special designation. An assumption was made that a CSP would allow a physical walkthrough from a client by request.

Managerial and operational control are not accessible from the end-user perspective. For example, it is not possible from an end-user perspective to determine if management has been put in place over information security, if budget has been allocated for information security or if operations staff is performing audit log reviews.

Each technical control was then reviewed individually to determine which could be assessed from the end-user perspective. If it was possible, the control was marked in-scope. If it was not possible, an explanation was documented. Questions asked to determine applicability included:

- Is this control involved exclusively with back-end CSP processes or technology? If so, it is likely not assessable from the end-user perspective. (e.g. auditing configuration on cloud service systems).
- Does this control relate to user accounts? If so, it is likely assessable from the end-user perspective as the federal program stakeholders will have user accounts to the underlying cloud provider system, such as the virtual machine management interface or overall account management interface. (e.g. password complexity requirements for user accounts)
- Can this control be validated with a basic physical tour of the cloud service provider? If so, then it’s assumed a basic facility tour can be scheduled, and the control is assessable. (e.g. fire extinguishers are present)

There are controls identified as end-user assessable, and received an additional designation of red team or black team. This designation indicates an invasive approach to testing that can disrupt the cloud provider operations and potentially violate a service level agreement. Red team indicates the use of hacking tools, social engineering and deployment of malware to the cloud service provider to determine the status of a control. Black team indicates bringing a cloud service provider production facility down for an extended period of time, forcing an enactment (and validation) of the cloud service provider’s business continuity controls. Caution should be taken before proceeding with assessing security controls through red team or black team assessment methods, but they are assessable from the end-user perspective, so were identified accordingly.

For example, monitoring physical intrusion alarms and responding to them is a required control. This can only be effectively assessed through intentional unauthorized physical access. Additionally, ensuring audit files are not modified or deleted is a required control. This can be assessed by gaining unauthorized access to CSP systems (e.g. backend systems or elevated privileges on the Hypervisor) and attempting to delete system audit files. These techniques will inform the controls effectiveness, but can result in adverse impact to the CSP.

4. FINDINGS

The primary objective of this paper is to determine what security controls are assessable from the end-user perspective for a program hosted on a FedRAMP-accredited cloud service platform. It was determined thirty controls were completely assessable and eighty-nine controls were partially assessable. The count for partially assessable controls are inclusive of completely assessable. Table 1 shows the controls counts by NIST 800-53 control family that are assessable, completely (CA) and partially (PA).

The research revealed 9% of security controls the CSPs are required to implement can be assessed from the end-user perspective and 27% can be partially assessed. Partially assessed implies at least one objective of the control can be assessed, but all objectives of the control, per NIST definition, cannot be assessed.

Table 1 – Security Control Assessable Details

<table>
<thead>
<tr>
<th>Control Family</th>
<th>CT</th>
<th>CA</th>
<th>PA*</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS CONTROL</td>
<td>43</td>
<td>5</td>
<td>18</td>
</tr>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>19</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>AWARENESS AND TRAINING</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CONFIGURATION MANAGEMENT</td>
<td>26</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>CONTINGENCY PLANNING</td>
<td>24</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>IDENTIFICATION AND AUTHENTICATION</td>
<td>27</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>INCIDENT RESPONSE</td>
<td>18</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>MAINTENANCE</td>
<td>11</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>MEDIA PROTECTION</td>
<td>10</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>PERSONNEL SECURITY</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PHYSICAL AND ENVIRONMENTAL PROTECTION</td>
<td>20</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>PLANNING</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RISK ASSESSMENT</td>
<td>10</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SECURITY ASSESSMENT AND AUTHORIZATION</td>
<td>15</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>SYSTEM AND COMMUNICATIONS PROTECTION</td>
<td>32</td>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td>SYSTEM AND INFORMATION INTEGRITY</td>
<td>28</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>SYSTEM AND SERVICES ACQUISITION</td>
<td>22</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>325</strong></td>
<td><strong>30</strong></td>
<td><strong>89</strong></td>
</tr>
</tbody>
</table>

* - inclusive of completely assessable count
CT= Control Total
CA = Completely Assessable
PA = Partially Assessable

The results from the third-party organization audit of the CSP implemented security controls can be requested by any federal
agency from a FedRAMP participating CSP. These results can provide greater visibility into the security control implementation, but caution for the effectiveness of the third-party assessment organization must be considered. This extends the research for the interested federal program from just the cloud service provider to include the reliability, reputation and quality of the third-party organization in its ability to effectively execute a security control assessment and report the findings accurately.

5. ISSUES
These security controls are aligned to federal requirements for federal agencies. These results can be leveraged for testing non-FedRAMP accredited CSP, but there is no understood agreement that the controls being tested have been attested as in place by the CSP. Therefore, this methodology and its results are useful, but intended for entities assessing a FedRAMP approved CSP.

This research considered NIST and FedRAMP guidance. Security controls required by FedRAMP are included in the NIST SP 800-53. The NIST SP 800-53A recommends specific approaches to assessing NIST 800-53 security control objectives. This document was intentionally written to complement the 800-53A, but is only a recommendation. A unique perspective on assessing the controls that make up each control could have been taken. For the sake of time, repeatability and consistency across research, the NIST 800-53A was used.

Black team assessed controls must be exercised with extreme caution or not at all. Assessing these controls external to the cloud service provider requires tactics that can have significant adverse impacts on the CSP. Black team assessed controls are concerned with validating a CSP’s business continuity and disaster recovery. If these controls are determined to be ineffective or not in-place the CSP could experience downtime and loss of consumer confidence. This could result in invalidation of SLA’s with the CSP or legal action. For example, disabling total power to a production facility would test their backup power controls. If these controls are not effective, the entire production site would be unavailable.

The final determination of whether a security control was end-user assessable was left to the professional judgement of the researchers. Each decision was not further supported by attempting to assess the security control to prove it was not possible or was possible.

6. FUTURE WORK
Unique validation procedures for each security control can be developed to determine if additional controls can be included in the in-scope collection of controls that can be validated from the end-user perspective. As noted in the research, the NIST 800-53A revision 4 was used to provide an accepted and unbiased validation technique, but could possibly be restricting a control from end-user validation.

The determination of whether a control is end-user accessible was a professional judgement by the researchers. Additional research repeating the processes should be performed to determine if findings are consistent.

Detailed security control and corresponding objectives identified as in-scope are available to researchers by request to either author, being too voluminous to be appropriate for this paper as an inclusion.

7. CONCLUSION
The primary objective of this paper is to determine what security controls are assessable from the end-user perspective for a program hosted on a FedRAMP-accredited cloud service platform. Knowing these controls provides the ability for an organization to retain awareness of security control implementation while gaining the benefits of utilizing a cloud platform.

This work determined utilizing a CSP to host and complement an organization’s IT infrastructure comes with the cost of losing visibility into security control implementation assurance. The research indicated 9% of FISMA required security controls for the CSP can be independently validated from the consumer perspective.

The research was intentionally limited to the security controls documented within the NIST SP 800-53 revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. These are the known controls CSP’s are required to implement to receive FedRAMP accreditation.

A third-party organization is responsible for fully assessing a CSP security control implementation. An organization can increase its confidence in security control implementation by focusing on assessing the quality and professionalism of the third-party organization providing the independent verification and validation of the CSP for FedRAMP accreditation, in addition to assessing the controls identified in this paper as end-user assessable.

8. ACKNOWLEDGMENTS
Our thanks to the federal government for directing this research problem, the InSure program for facilitating this research and Dr. Wayne Pauli for his guidance during research and development.

9. REFERENCES