Group 5: My Pham, Reshma Maliakkal, Sukruta Jadhav, William Marty, Cody Blanchard

Professor Joseph Mauriello

ACCT 6336-501

1 May, 2019

Final Project

IBM Cloud - Access Management

1. IBM - Technology Company and Access Management

The global technology company, International Business Machines Corporation (IBM), founded in Edincott, New York on June 16th, 1911, provides five segments of services: Cognitive Solutions, Global Business Services (GBS), Systems, Global Financing, and Technology Services & Cloud Platforms. Headquartered in Armonk, New York, IBM has now expanded its office locations in more than 170 countries as the Computing-Tabulating-Recording Company. Some of IBM's competitors are Alphabet Inc., Cisco Systems, Inc., Oracle Corporation, Amazon.com, Inc., SAP, Capgemini, Fujitsu, BMC, Microsoft Corporation, Salesforce.com, Accenture, Del Technologies, HP, VMWare, Hewlett-Packard, Computer Sciences Corporation, Pure Storage and General Electric Company ("International Business Machines Corp (IBM)").

The Cognitive Solutions segment provides different types of analytics (descriptive, predictive and prescriptive) and cognitive systems through cloud environments and as-a-Service models. One of them is Watson, a cognitive computing platform that is able to "interact in natural language, process big data, and learn from interactions with people and computers" ("International Business Machines Corp (IBM)"). The Global Business Services offers global process services and consulting, application management services including Watson, cloud, blockchain and Technology Services; its outsourcing service line provides finance, procurement, human resources and related business processes ("International Business Machines Corp (IBM)"). The Systems segment is comprised of operating systems software and delivers infrastructure technologies to "address computing capacity, security and performance needs of businesses,

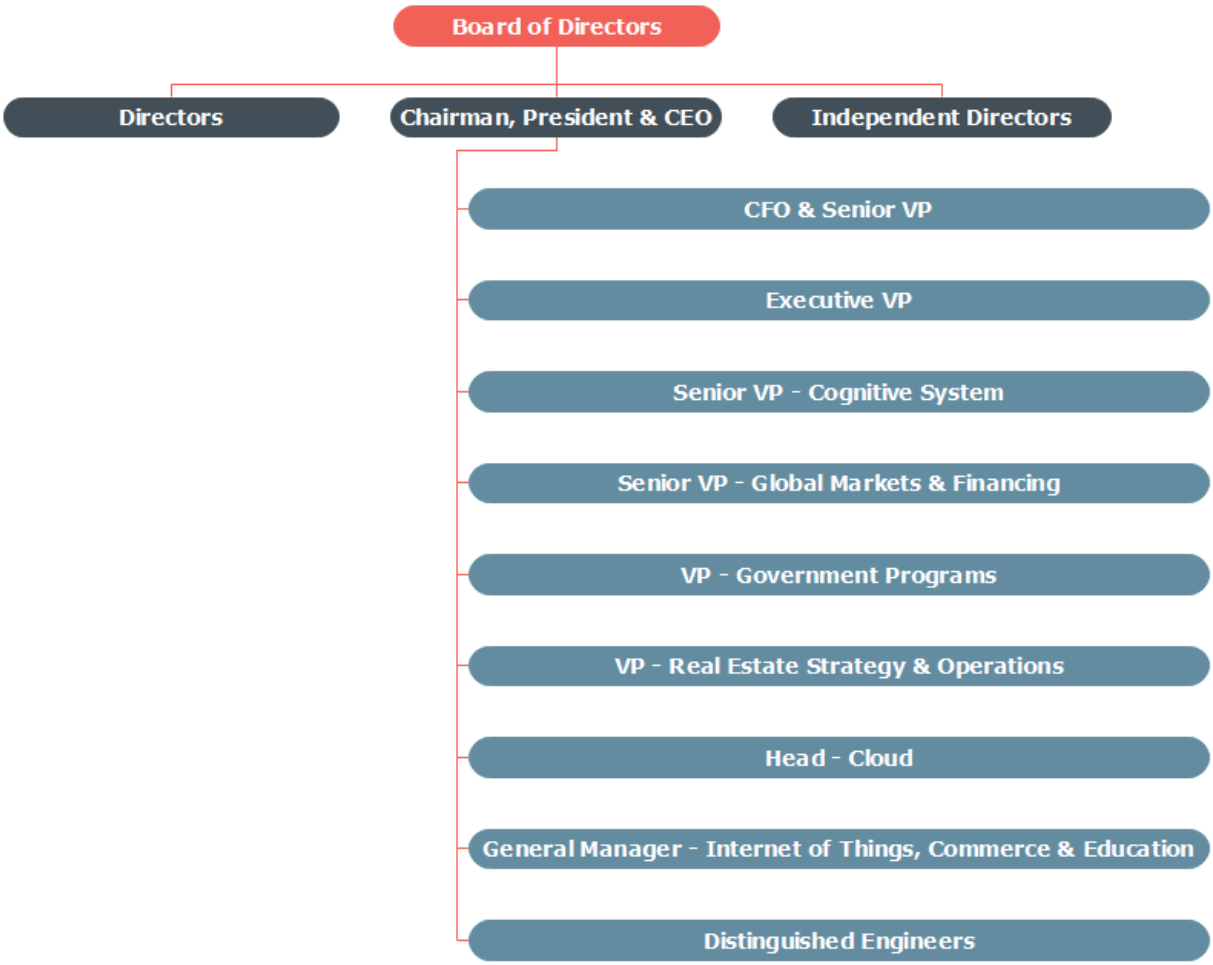
hyperscale cloud service providers and scientific computing organizations" ("International Business Machines Corp (IBM)"). The Global Financing segment consists of client financing, commercial financing, remanufacturing and remarketing and provides lease, installment payment plan and loan financing to end users and internal clients ("International Business Machines Corp (IBM)").

The Technology Services & Cloud Platforms segment offers IT infrastructure services by providing a portfolio of cloud, project-based, outsourcing and other managed services for enterprise IT infrastructure environments. For companies that optimize public and private clouds and traditional IT, this segment serves as a set of hybrid cloud services and solutions to help clients build and run their enterprise IT environments ("International Business Machines Corp (IBM)").

All of these above segments use IBM cloud services to host internal and external applications. Particularly, access management of IBM cloud is our focus, which covers its Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) businesses in one offering. The board of directors unanimously agreed that FedRamp High Controls should be implemented throughout environments, in efforts to gain FedRamp High Certification to show customers they are ready for higher federal needs and toughen up internal security. In order to evaluate the work they have done so far, they hired our team for auditing of findings.

Access management, also known as user access management (UAM) or identity and access management (IAM) refers to the process of "managing the roles and access privileges of individual network users and the circumstances in which users (customers or employees) are granted (or denied) those privileges" (Martin). According to Martin, the main purpose of IAM systems is that one digital identity per individual is established and must be "maintained, modified and monitored throughout each user's access lifecycle." In other words, the goal is to "grant access to the right enterprise assets to the right users in the right context, from a user's system onboarding to permission authorizations to the offboarding of that user as needed in a timely fashion" (Martin). IAM tools include API security, customer identity and access management (CIAM), identity analytics (IA), identity as a service (IDaaS), identity management and governance (IMG) and risk-based authentication (RBA) (Martin).

2. Management Overview



IBM has a board of directors and a management team that are highly qualified and specialized in their respective areas. Virginia Rometty, Chairman, President and CEO of IBM, is a member of both the board of directors and the executive team. IBM's management team consists of a significant number of executives. An example of several members serving on the board of directors and management team is presented as follows:

a. **Board of Directors:** ("IBM Board of Directors")

- ➢ Virginia M. Rometty - Chairman, President & Chief Executive Officer
- ➢ Michelle J. Howard - Director
- ➢ Martha E. Pollack - Director
- ➢ Independent Directors

b. Executives: (“Executive Bios”)

- Virginia M. Rometty - Chairman, President & Chief Executive Officer
- James J. Kavanaugh - Chief Financial Officer & Senior Vice President
- Michael Jordan - Distinguished Engineer - Systems Security
- Ed Perry - Director - Government Programs
- David A. Cass - Head - IBM Cloud
- Harriet Green - GM - Watson Internet Things, Commerce & Education
- Robert Picciano - Senior Vice President-Cognitive System
- Martin J. Schroeter - Senior Vice President-Global Markets & Financing
- Martin Jetter - Senior Vice President-Europe
- Michelle Rankin - Director - Openpower
- Randy I. Walker - Global Managing Director
- Sophie V. Vandebroek - Vice President - Emerging Technology Partnerships
- Robert W. Lord - Senior Vice President - Cognitive Applications
- John E. Kelly - Executive Vice President
- Frank L. Cuevas - Vice President - Real Estate Strategy & Operations
- Michael Elder - IBM Distinguished Engineer

3. Risk Assessment with Analysis

A risk assessment is the process of the ongoing identification of potential risks, followed by a thorough analysis that quantifies the impact and likelihood of a particular risk in order to prioritize the order and need, if any, for making improvements. A risk assessment was performed in order to assess the potential vulnerabilities that the company may encounter in regards to Identity and Access Management, and the importance and likelihood of these potential risks as depicted through the risk matrix shown below.

Impact	**Extreme**	Loss of Service due to Disaster	SOX Compliance Violation			
	High	Outdated Physical Security	HIPAA Compliance Violation	PCI Compliance Violation	Outdated Cybersecurity	
	Medium	Unreviewed Accounts	Segregation of Duties Violations	Unauthorized Changes to Accounts	Shared Accounts	
	Low			Access Outliers	Overprovisioned Access	Orphaned Accounts
	Negligible					
		Rare	**Unlikely**	**Moderate**	**Likely**	**Almost Certain**
	Likelihood					

The risk assessment can be broken down into two areas: Process Based Risks and Overarching Risks. The Process Based Risks have to do more exclusively with the company's access points into its networks and how it handles Identity and Access Management. The Overarching Based Risks have to do with physical and cybersecurity risks as well as disaster recovery plans

Process Based Risks:

- Account Management
- User Management

- ➢ Role Management
- ➢ Resource Management

Overarching Risks:

- ➢ Disaster Plan Assessment
- ➢ Legal Compliance
- ➢ Physical Security
- ➢ Cybersecurity

Process Based Risks:

Account Management	
Risk Area	**Risk**
Orphaned Accounts	Accounts that were created outside of defined process and are left enabled after termination, can create the opportunity for inappropriate access into the network.
Shared Service Accounts	Accounts not tied to a single entity, such as multiple departments within an organization sharing one account, can have an issue if one of the former account sharing entities is no longer supposed to have access to those resources or services, but still has access to the account.
Unreviewed Accounts	Accounts that were not reviewed and approved by the appropriate personnel can introduce the potential risk of inappropriate access.
Unauthorized Changes	Access that went around the usual approval process that could allow for the potential risk of inappropriate access.

User Management	
Risk Area	**Risk**
Orphaned Accounts	Accounts that were not removed when an individual left an organization, which can create the opportunity for someone to gain inappropriate access to an organization's resources (Norris 1).
Shared Service Accounts	Accounts not tied to a single entity, such as multiple individuals within an organization sharing one account, can have an issue if one of the former account sharing entities should no longer be granted access, but still has access to the account (Norris 1).
Unreviewed Accounts	Access that was not reviewed and approved by the appropriate personnel can introduce the potential risk of inappropriate access (Norris 1).
Unauthorized Changes	Access that went around the usual approval process that could allow for the potential risk of inappropriate access (Norris 1).

Role Management	
Risk Area	**Risk**
Segregation of Duties Violations	Users have inappropriate access to assets and applications that allow them to forgo a checks and balances system (Norris 1).
Overprovisioned Access	Access that was granted to an individual that is more than what is required to accomplish their job (Norris 1).
Access Outliers	Users with out of role access that may be needed in order to fulfill certain business functions; they are usually necessary in the case of crisis response or instances of necessary processes that require fast response (Norris 1).
Unauthorized Changes	Access that went around the usual approval process that could violate policy and allow for potential risk of inappropriate access (Norris 1).

Resource Management	
Risk Area	**Risk**
IT Security and System Access	Unauthorized access could be gained by an outsider or an individual within the organization that could not have access to a particular resource, which would result in inappropriate access.

Encryption of Data	An organization's data could be leaked if someone hacked into the Cloud, and that could be mitigated by the use of encryption of data such as passwords, users, accounts, and resources.
Unauthorized Changes	Access that went around the usual approval process that could violate policy and allow for potential risk of inappropriate access (Norris 1).

Overarching Cloud Risks:

Disaster Plan Assessment	
Risk Area	**Risk**
Loss of Service	During the state of disaster, there should be recovery of services in a timely manner in order to prevent the disruption of services for clients.

Legal Compliance	
Risk Area	**Risk**
SOX Compliance	The company must meet federal requirements.
HIPAA Compliance	If the company is providing service to healthcare companies that store Protected Health Information, the company must meet HIPAA compliance standards when storing data and granting access to data.

PCI Compliance	If the company is providing service to a company that handles branded credit cards,the company must meet PCI compliance standards when storing data and granting access to data.

Cybersecurity Assessment	
Risk Area	**Risk**
Inadequate Cybersecurity	The company should make steps to protecting their resources and network access in the case of hacking. Some measures that should be checked are the current state of firewalls and currently placed protections.
Outdated Cybersecurity	The company has to be aware of the limitations of their cybersecurity measures, make time sensitive patches, and work towards combating them so hackers do not exploit those weakness.

Physical Security Assessment	
Risk Area	**Risk**
Inadequate Physical Security	The company should ensure that the server buildings are safe, secure and only are accessible through proper identification in order to avoid instances of inappropriate access to servers.

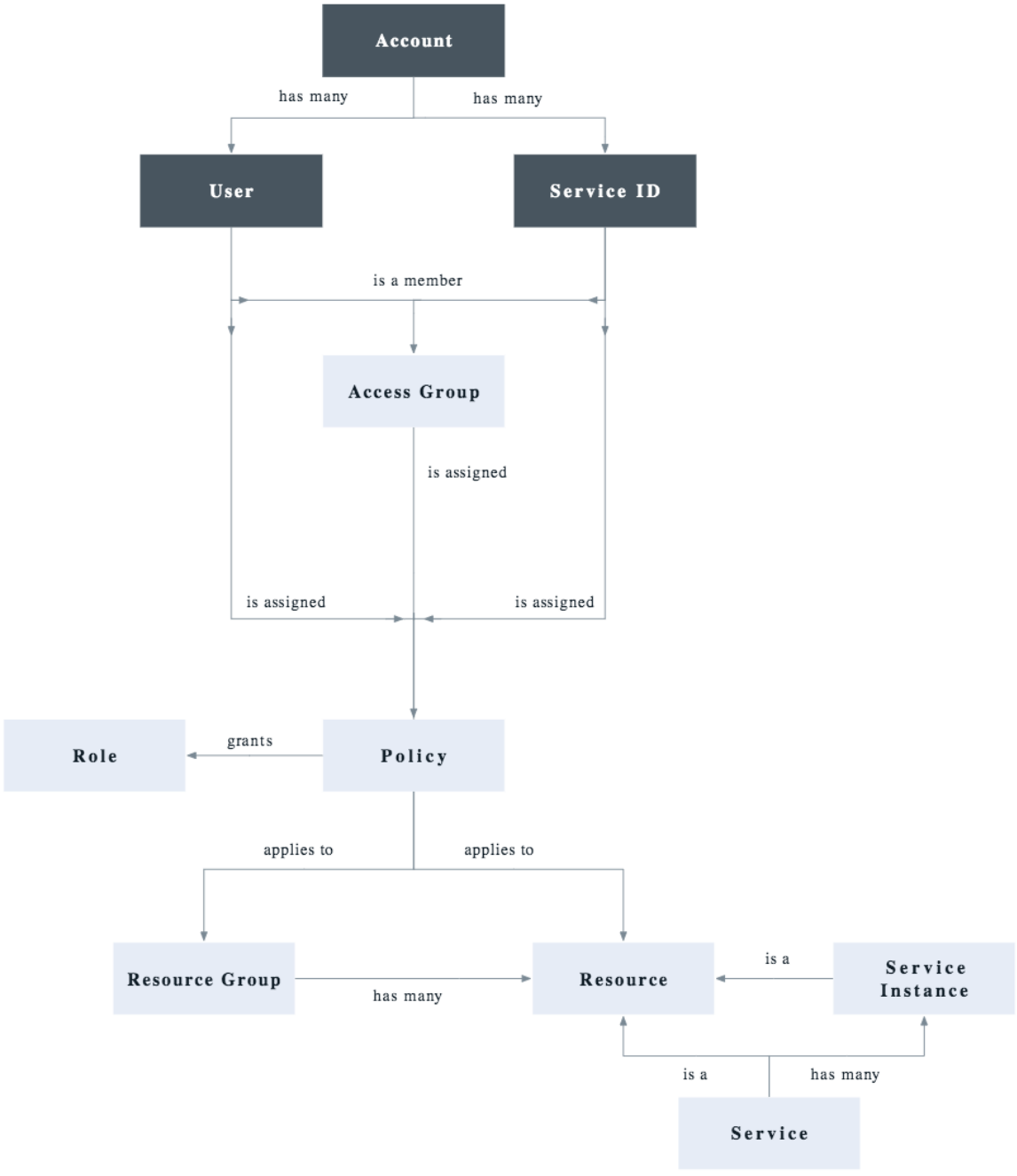
Outdated Physical Security	The company has to be aware of the limitations of their physical measures and work towards combating them so buildings and servers are protected.

4. Management Controls Assessment

- ➢ The leadership team in the organization provided their IT Security Standards document in which they share throughout the organization with managers and employees to describe processes and expectations. Document seems to be up to date as of April 2019.
- ➢ Applicable to this audit, IT Security Standard document has a section for access control that includes policy, user access management, user identities, application or system identities, access provisioning, managing privileged access rights, review of access rights, revocation of access rights, supplier support access, secure logon procedures, password management, and certificate authentication.
- ➢ The Chief Information Security Officer office announced recently that it is requiring internal and external customers' accounts to have 15-character passwords as minimum. Passwords should also contain at least two-character types, including uppercase, lowercase, numbers, special characters, and spaces will be allowed. They have updated their IT security standards to reflect this change.
- ➢ Access controls seems to be well defined by leadership team, policies address and identify organization's objectives and strategy, governing bodies, separation of duties, safeguarding of assets, and adherence to industry standards.
- ➢ The board of directors unanimously agreed that FedRamp High Controls should be implemented throughout environments, in efforts to gain FedRamp High Certification to show customers they are ready for higher federal needs and toughen up internal security.

5. Flow Diagram for Cloud Identity and Access Management

The company uses the following process for their Cloud Identity and Access Management in order to authenticate the user's identity before accessing their Cloud stored materials as seen below:



("IBM Cloud Identity and Access Management")

Each account has many users, people using the services available within the account, and service IDs, which identify which potential services could be accessed by the users within the account ("IBM Cloud Identity and Access Management" 1). Account owners can be individuals, departments of companies, or collective companies. Users and service IDs are grouped into access groups that are assigned certain access roles based off of a policy ("IBM Cloud Identity and Access Management" 1). The policy is what defines the scope of access to a target and this can be during a singular service instance or for the user's general access to complete tasks defined by the account owner and granted within their role through the policy ("IBM Cloud Identity And Access Management" 1). The policy allow applies to the resources available to the account users, and define resource groups that are comprised of many resources ("IBM Cloud Identity and Access Management" 1). Each time an account requests a service instance, as long as the preassigned role granted by the policy allows it, a user is granted access to the requested service through the cloud ("IBM Cloud Identity and Access Management" 1).

6. Audit Program with Audit Steps

Objective: To plan the audit and obtain sufficient background information for the area to be audited which includes going through past reports, applicable laws and regulations, policies and standards and benchmark against best practices; determine organization's strategies and objectives by going through mission, vision, strategic plans, annual business plans and goals.

Determine Audit Subject: Perform an audit of Identity and Access Management area of IBM Cloud Services which involves processes and supporting infrastructure to create, maintain and use of digital identities.

Define Audit Objective:

1. Assure the policies and procedures are directed and approved by management, when using cloud services to remediate risks and comply with laws and regulations.
2. Evaluate the current state of IAM processes, controls and supporting technologies. (Cook, Bryan)
3. Identify if there is streamlined management of user identities and access rights.
4. Identify the user identities, identity life cycle components and identity repositories, and evaluate the controls used to protect this data. (Bresz, Frank, et al)
5. Assure that the controls in place to prevent people from bypassing authentication or authorization controls is string and benchmarked against best practices.
6. Identify controls to deactivate and delete user access permissions, controls to check access to privileged accounts
7. Identify security controls and assessment procedures for Federal Information Systems and Organizations

(Cook, Bryan)

Audit Scope: With the preliminary survey and risk assessment, the audit period covered the identity and access management operation of IBM from February 18, 2019 to May 1, 2019. Audit procedures included:

- ➢ Interview of key personnel
- ➢ Review applicable laws, regulations, policies and procedures
- ➢ Verify the existence of policies and procedures
- ➢ Gather information from key personnel
- ➢ Analyze access rights and account management
- ➢ Test of IAM controls in place

Pre-Audit Planning: Determine risks from business strategies and activities, risk mitigation activities to see if they have to be developed to manage risks; understand the risk appetite of the organization; in order to re-assess risks, maintain ongoing monitoring activities and check the controls managing risk. ("Audit Plan Activities: Step-by-Step")

In pre-audit planning, a risk assessment was conducted to further refine the scope and audit procedures. Interviews were conducted to inquire about the activities or areas of concern that needed to be included in the scope. ("Audit Plan Activities: Step-by-Step")

Data Gathering: Based on the previous steps, we identified and obtained policies, standards and guidelines to review. Determine methods to perform evaluation, develop tools and methodologies to test and verify controls. Few individuals were identified for interview:

- ➢ Access administrator
- ➢ Cloud architect
- ➢ Security operator
- ➢ Cloud administrator
- ➢ Network administrator
- ➢ Database administrator

("Cloud Operating Model Transformation")

The audit of IAM reviewed and checked the following areas:

- ➢ Access control policy and procedures
- ➢ Account management
- ➢ Information flow
- ➢ Least privileges
- ➢ Session lock
- ➢ Remote access
- ➢ Use of External Information Systems

Defined methods, inquiry, observation, inspection, reperformance and computer assisted tools to test and verify the results to be accurate

("Audit Plan Activities: Step-by-Step")

7. Audit Fieldwork

This section presents:

- The control objectives as specified by the management
- Controls established to achieve the specified control objectives
- Description of the testing performed to determine if the controls were performing with effectiveness to achieve the control objectives
- Results of tests performed to determine the effectiveness of controls

Control Area: Access Control Policy and Procedures

Control Objective: To address the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements.

ID	**Test of Operations**	**Results**
AC-1	1. Reviewed access control policy that addresses scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance 2. Reviewed the procedures for facilitating the implementation of policy and access controls 3. Reviewed the documentation update log and check out log to see if only the authorised users have access to the documentation	No exceptions found

Control Area: Account Management

Control Objective: User with organization specified roles and group membership are allowed access to the information system accounts

ID	Test of Operations	Results
AC-2(1)	1. Reviewed and tested the automated system account management using few samples: ● Sample emails and text were sent to notify account managers when users are terminated or transferred ● Used the accounts to increase the usability and did not have any usability to test the monitoring usage of accounts ● Tested the telephonic notification mechanism to trap any atypical usage	No exceptions found
AC-2(2)	Selected a sample of accounts to test the removal of temporary/emergency accounts. Set the time period for one day for a few accounts and one hour for emergency accounts. Tested for the timely removal of these accounts after the time period expired	Removal of temporary/emergency accounts were handled by system administrator and not automated to remove timely removal. The accounts that were to be removed from the system in a day was not removed for a period of two days.
AC-2(3)	With the above sample, disabling of inactive accounts was tested to verify the working of automated mechanism. Set the time period for an hour a day and a week. Observed the automated disabling of the test samples.	No exceptions found
AC-2(4)	Reviewed and tested a sample account creation, modification, enabling, disabling, and removal of actions by authorized personnel	No exceptions found
AC-2(5)	Reviewed the organization defined logout period and tested a few samples to verify the description of when to log out. With test samples, prompt was checked for timely logging out after inactivity was discovered	No exceptions found
AC-2(7)	Reviewed role based schemes to: ● Establish and administer privileged user accounts ● Monitor privileged role assignments ● Take defined actions when the privileged accounts	No exceptions found

	are no longer appropriate	
AC-2(9)	Reviewed restrictions on use of shared accounts/groups. Tested a few samples to comply with the organization defined conditions for establishing shared/group accounts. ● Created a shared group and allowed access for certain accounts and restricted access for test samples ● Restricted test samples were tested to access the shared group and join	No exceptions found
AC-2(10)	Reviewed the conditions for shared/group account credential termination. Tested a few samples to check the automated termination of credentials once users leave the group. With the above test sample: ● Members were removed one by one to check the activity ● Once all the members left the group, the test samples were used to access the same group with same credentials	No exceptions found
AC-2(11)	Reviewed the conditions defined by the organization for accounts usage under certain circumstances. Tested a few samples to ● Check if the accounts are permitted usage on certain weeks, days and time of the day. ● Restricted some sample accounts to verify the usage	No exceptions found
AC-2(12)	Tested the account monitoring/atypical usage process with few samples: ● Used the accounts on a day and time that was not consistent with normal usage patterns ● Checked for any notifications that was sent to authorised personnel	No exceptions found
AC-2(13)	Reviewed the process used for disabling accounts for high risk individuals. Ensured there is coordination between authorized officials, system administrator and human resources for timely execution of this control	No exceptions found

Control Area: Least Privilege

Control Objective: Users should only have authorized access to complete tasks that are assigned to them, and further access is only considered as necessary by the organization.

ID	Test of Operations	Results
AC-6(1)	1. Selected a sample of accounts with access to organization-defined security functions, and reviewed for the following: ● Account, along with its privileges, is listed in the company's security policy ● Reviewed the audit log to ensure those accounts did not access systems outside their purview	No exceptions noted.
AC-6(2)	2. Reviewed the audit logs for access to nonsecurity functions, and ensured that: ● Users of information system accounts with access to security functions did not use these accounts to access the nonsecurity functions	No exceptions noted.
AC-6(3)	3. For the sample selected: ● Reviewed that these user accounts were restricted to organizationally defined personnel or roles ● Reviewed the audit logs, including time/date and location of access, to ensure access to these accounts was restricted to the privileged users	No exceptions noted.
AC-6(7)	4. Ensured that management reviews and discusses the need for the organizationally-defined roles/accounts at least once annually.	No exceptions noted.
AC-6(7)	5. For account classes that had their privileges removed, selected a sample and reviewed the audit logs to determine if the access was actually removed	No exceptions noted.

Control Area: Remote Access

Control Objective: Access to the organization's information systems via remote locations is restricted unless authorized by the organization.

ID	Test of Operations	Results
AC-17(4)	1. Reviewed management documentation showing that: ● Remote access to privileged data is allowable only for certain organizationally-defined needs ● The organization documented the rationale for such needs	No exceptions noted.
AC-17(3)	2. Selected a sample of users with remote access and reviewed for the following in the audit logs and other relevant documentation: ● All traffic is routed through management-controlled access points ● Communication is encrypted using end-to-end encryption ● The organization has the capability of speedily disabling remote access to the information system using the controlled access points	No exceptions noted.

Control Area: Information Flow

Control Objective: The organization effectively controls the flow of information within and between the different information systems.

ID	Test of Operations	Results
AC-4(1)	Tested the information flow by attempting to send an information object with one label to a destination object that should not accept said label.	No exceptions noted.
AC-4(3)	Tested sending an information object before and after changing the risk tolerance, noting the difference in behavior	No exceptions noted.

Control Name: Concurrent Session

Control Objective: The information system limits the number of concurrent sessions for each privileged and non-privileged account to 3 and 2 respectively. (“FedRAMP Security Assessment Framework”)

ID	Test of Operations	Results
AC-10	1. Tested privileged account session from 4 different machines (2 Windows and 2 Linux systems) and was not able to login from fourth machine after 3 sessions were active. 2. Tested non-privileged account session from 3 different machines (all Windows systems) and was not able to login from third machine after 3 sessions were active.	No exceptions noted.

Control Name: Session Lock

Control Objective: The information system locks out after 15 minutes of inactivity or after the user locks out and retains session till the user re-establishes access. (“FedRAMP Security Assessment Framework”)

ID	Test of Operations	Results
AC-11	1. Left an active session idle for 15 minutes and 25 seconds, when returned I was prompted to enter password and two-factor authorization code after password.	No exceptions noted.

Control Name: Session Lock | Pattern-Hiding Displays

Control Objective: The system conceals information previously visible on the display with a publicly viewable image. (“FedRAMP Security Assessment Framework”)

ID	Test of Operations	Results
AC-11(1)	1. Upon session lock in previous test, noticed blue background on Windows system 2. For Linux testing, previously visible screen was concealed with blue background.	No exceptions noted.

Control Name: Session Termination

Control Objective: The system terminates session after user initiates disconnect or shut down "The information system automatically terminates a user session after user initiates system disconnect or system shut down."("FedRAMP Security Assessment Framework")

ID	Test of Operations	Results
AC-12	1. Left a number of applications open with saved and unsaved work 2. Clicked on the disconnect button in the start menu. 3. Was prompted to save unsaved work, declined. 4. Session appeared to be over, reinitiated session and previously left open work was not open.	No exceptions noted.

Control Name: Session Termination Display

Control Objective:

a. Provides a logout capability for user who have initiated authentication through trusted mechanism, and

b. Displays logout message to users indicating the trusted termination of authenticated sessions.

("FedRAMP Security Assessment Framework")

ID	Test of Operations	Results
AC-12(1)	1. Connected to business-critical database 2. Attempted to log out and disconnect from session and was presented a confirmation screen that my session was terminated along with a time stamp.	No exceptions noted.

Control Name: Use of External Information Systems

Control Objective: Established terms and conditions, that are normally required with any trust relationships established with external organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

a. Access the internal system from external systems; and

b. Process, store, or transmit organization-controlled information using external systems. ("FedRAMP Security Assessment Framework")

ID	Test of Operations	Results
AC-20	1. Attempted to initiate external remote session from external workstation to organization bastion server, was prompted with terms and conditions for use of system.	No exceptions noted.

Control Name: Use of External Information Systems | Limits on Authorized Use

Control Objective: The organization allows authorized individuals to use an external systems to access information system or to process, store, or transmit internal information only when:

a. External system's security controls are verified to comply with organization's policies

b. Use of approved establish connections or agreement with organization hosting external systems. ("FedRAMP Security Assessment Framework")

ID	Test of Operations	Results
AC-20(1)	1. Manager expressed confidence on security control for external information systems and generated artefact demonstrating limitations set on external authorize use.	No exceptions noted.

Control Name: Use of External Information Systems | Portable Storage Device

Control Objective: Restrict or prohibit use of controlled portable device by authorized personnel or external systems. ("FedRAMP Security Assessment Framework")

ID	Test of Operations	Results
AC-20(2)	1. The organization demonstrated terms of use policy limiting use to certain conditions for portable storage devices.	No terms of use could be provided

8. Recommendations

Throughout our audit, we noticed a couple of areas where the organization's controls were lacking in effectiveness. The most primary area of concern was in their account management. The company had an internal policy of removing temporary/emergency accounts within one day for temp accounts and one hour for emergency accounts. However, this control was not consistently implemented and the process took longer than a day for some temporary accounts. We recommend the company implement an automated, rather than manual, process for these accounts to more effectively control this area in the future.

The other significant error was the lack of a formal company policy for the use of a portable storage device. While the company had restrictions on when such devices could be used, the lack of a formal policy distributed to all systems users could lead to the misuse of such devices in the future, making this a high priority item to fix in the future. We suggest the company implement a clearly communicated policy for the usage of these devices.

In spite of these issues, IBM provided reasonable assurance that their controls were operating effectively throughout the period under audit. In our professional judgement, sufficient and appropriate audit procedures have been performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report.

Works Cited

"Audit Plan Activities: Step-by-Step." *ISACA*, m.isaca.org/COBIT/Documents/Audit-Plan-Activities_res_eng_0316.pdf.

Bresz, Frank, et al. "Identity and Access Management." *THE IIA*, chapters.theiia.org/montreal/ChapterDocuments/GTAG 9 - Identity and Access Management.pdf.

"Cloud Operating Model Transformation |EMC." InFocus Blog | Dell EMC Services, 22 June 2018, infocus.dellemc.com/choong_kengleong/cloud-operating-model-transformation/.

Cook, Bryan. "Top Reasons to Audit an IAM Program." *ISACANTX*, www.isacantx.org/Presentations/April 040317 Top Reasons to Audit an IAM Program.pdf.

"Executive Bios." *IBM*, newsroom.ibm.com/executive-bios.

"FedRAMP Security Assessment Framework". *FedRAMP*, 15 Nov. 2017, *www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf*.

"IBM Board of Directors." *IBM*, www.ibm.com/investor/governance/board-of-directors.html.

"IBM Cloud Identity and Access Management". IBM Cloud, 2018, https://console.bluemix.net/docs/iam/index.html#iamoverview. Accessed 1 May 2019.

"International Business Machines Corp (IBM)." *Reuters*, www.reuters.com/finance/stocks/company-profile/IBM.

Martin, James, and John Waters. "What Is IAM? Identity and Access Management Explained." *CSO*, 9 Oct. 2018, www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.

Norris, Tim. "8 Critical Identity Risk Factors – And How to Manage Them". CSO Online, https://www.csoonline.com/article/3216064/article.html.