THE MILLENNEAL BANK

SOC 2 Type 2 Report

Service Organization Controls Assurance Report on Trust Services Principles and Criteria for Security, Availability and Confidentiality

9th December 2018

Haddox Solutions,

36 Cunard Street | 123-456-7890 | Boston, MA

Fax: +613 0078 8394, www.haddox.com

Table of Contents:

I. Scope & Responsibilities 3-4
II. Section 1(Overview of Services) 5-6
III. Section 2(System Description) 7-19
Terminology & Introduction 8
Infrastructure & Software 9
AWS Architecture 10
Network Layer 11
Data Layer 12
IT Process 14-16
Organizational Structure 17-20
IV. Section 3 20-23
Risk Assessment 21-23
Audit Approach 23-24
V. Section 4 24-27
Security Principle & Criteria 25-26
Availability Principle & Criteria 27
VI. Section 5 28-35
Audit Results 29-35
VII. Appendix 36
VIII. References 37

To,

Chief Financial Officer (The Millennial Bank)

Type 1 Independent assurance report on Security and Confidentiality Trust Services Principles for Identify

Scope:

We have taken reasonable assurance on designing and control implementation within Millennial Bank's cloud environment which is comprised of Security, Availability and Confidentiality controls as of 6th of December 2018. These controls are relevant to Security, Availability and Confidentiality control objectives which is specified by American Institute of Certified Public Accountants (AICPA). This is present within their "Section 100A – Trust service principles and criteria for security, availability, processing, integrity and confidentiality and privacy"

Millennial is responsible for

i. Services within the cloud application
ii. Identification of control objectives and related risks
iii. Designing controls to mitigate those risks and implement controls as designed

Scope and Responsibilities

Our responsibility is expressing an opinion on Millennial Statement with respect to the suitability of the design of controls to achieve the control objectives. We conducted our audit engagement to assess the suitability of controls designed to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether the controls were suitably designed and operating effectively to meet the applicable trust services criteria as of January 31, 2018.

Our Audit engagement involves reporting on control design, testing of operating effectiveness by performing testing procedures to obtain evidence related to design of controls required to achieve the control objectives, the completeness and accuracy. The procedures performed to select the evidence depends on our judgement, along with assessing of risks for those controls which are not suitably designed. We believe that the evidence obtained is sufficient and appropriate to provide a basis for audit opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Audit Opinion

In our opinion, in all material respects, based on the applicable trust services criteria the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met. However, we observed that few of the access controls designed were not operating effectively as of December 2018. Based on the risk assessment, overall risk rating for the identified control exception is “High” where control weakness was most related to information security and we found issues with controls that aim to ensure the customer data is secure. We identified 4 findings across the system with 3 identified as “High” risk and 1 identified as “Medium” risk.

Based upon our audit work, it is Haddox Solution’s opinion that the overall effectiveness of the processes and controls evaluated during the audit is rated as “Needs Improvement” (refer Appendix) . Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Issue owners have provided management action plans and have begun developing corresponding corrective measures.

Deekshitha V.

Deekshitha Venkateshaiah — **Boston, Massachusetts**

Partner — **6th December, 2017**

SECTION 1

OVERVIEW OF SERVICES

OVERVIEW OF THE MILLENNIAL BANK

Company Background

Millennial Bank was established in the late 2001 headquartered in Boston with around 1140 employees at present. Millennial Bank operates across the state of Massachusetts which enables online payments system that supports online money transfers and serves as an electronic alternative to traditional paper methods like checks and money orders. The service offered by us makes it simple to send and request money, manage credit, pool cash from peers, and create savings goals. Plus, you can easily track and monitor every transaction you make.

List of Services Provided

This description addresses Millennial's software-as-a-service public and private cloud offerings. Following services are provided by the organization all of which are not covered in the report.

Business Banking Services:

- Business Loans
- Checking Accounts
- Savings Account
- Debit & Credit Cards
- Money Deposit Services
- Credit card processing
- Online Payments

Cloud Services:

- Managed Backup
- Managed Load Balancing
- Managed Firewalling and VPN

SECTION 2

SYSTEM DESCRIPTION

MANAGEMENT DESCRIPTION OF THE SYSTEM

TERMINOLOGY

'AWS' means Amazon Web Services

'VPN' means Virtual Private Network

'Board' means Board of Directors

'Information Security Management Systems' means policies and procedures used to manage systematically Millennial confidential information

'SOC' means Service Organization Control

INTRODUCTION

The SOC 2 Type 2 Report is designed to provide reasonable assurance to Millennial clients that it maintains an adequate control environment to mitigate risks that impact services which is tagged along with handling confidential Information. This report has been prepared to provide information on the AICPA Trust Service Principles of Security and Confidentiality applicable to Millennial Bank. This section of the report (Section V) provides an overview of Millennial Bank, describing the processes and controls in place that comprise an effective control environment. Section VI provides the principles and criteria and details of the control activities supporting each criterion.

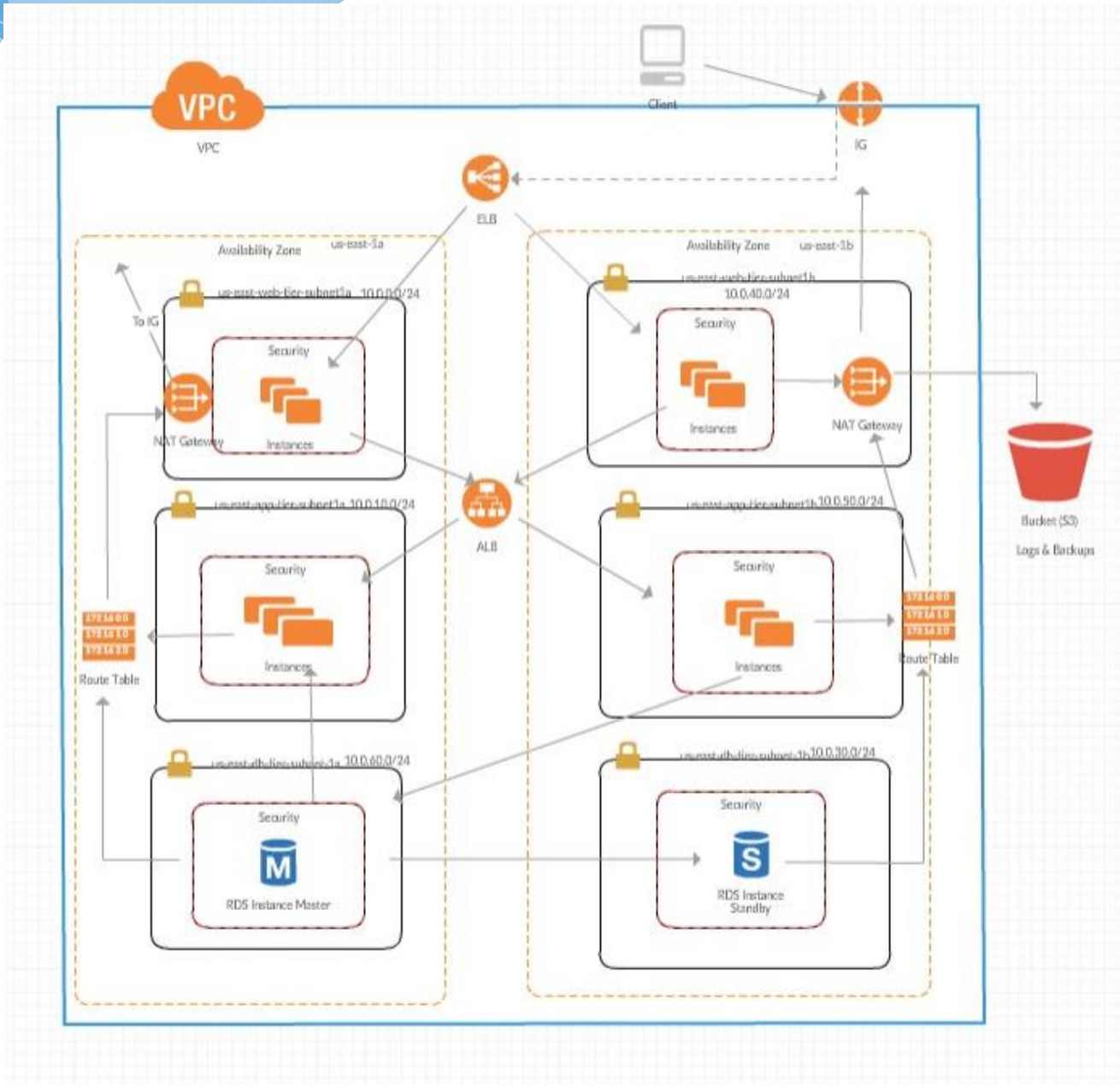
Service In-scope for Audit

One of the services offered by The Millennial Bank is **Online Payments** by facilitating electronic fund transfers through a payment gateway. These service is hosted at Massachusetts center facilities which is supported by personnel located at Boson and Maine office with one on-site staff at the MA center. The audit scope is limited to online funds transactions through cloud software/services within the period beginning 09/01/2018 and ending 20/31/2018.

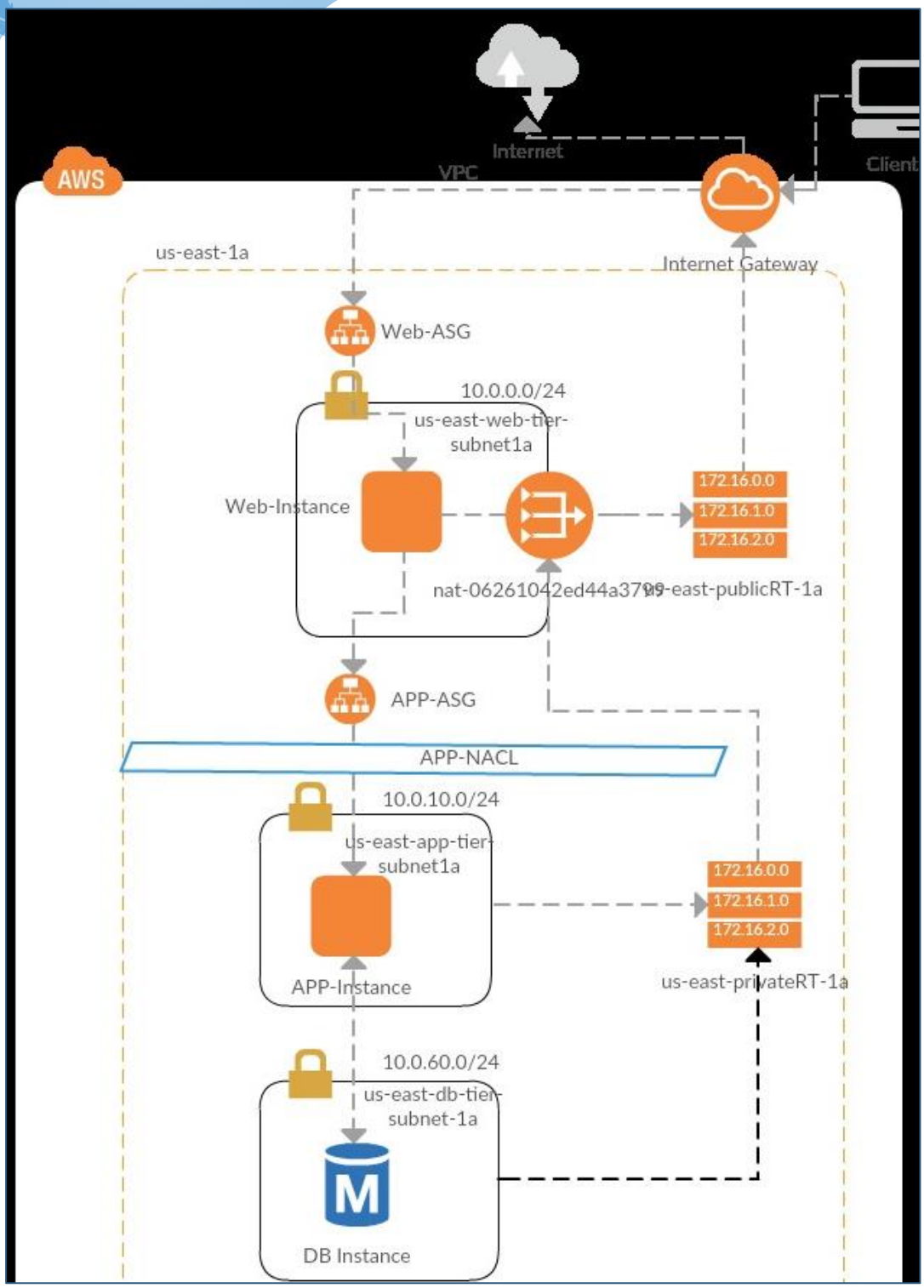
INFRASTRUCTURE & SOFTWARE

Resource Type	Resource ID/Name	AZ	Functions
EC2 Instance	i-03aa8d764d2bfe29c	us-east-1b	web application hosted User login user sign up UI for create account UI for deposit/withdraw money
EC2 Instance	i-0ab298d286a43ee24	us-east-1a	web application hosted User login user sign up UI for create account UI for deposit/withdraw money
EC2 Instance	i-05f79e5862735f863	us-east-1b	Backend java application hosted validation of users validations for account info Actual business logic for withdraw/deposit
EC2 Instance	i-0291fcf6fd76425dc	us-east-1a	Backend java application hosted validation of users validations for account info Actual business logic for withdraw/deposit
Internet gateway	igw-0dbea9c21bf87fa91		Connects to the outside internet
NAT Gateway	nat-06261042ed44a3799	us-east-1a	Connects the private subnet resources to outside internet
NAT Gateway	nat-09a403d49e1a64144	us-east-1b	Connects the private subnet resources to outside internet
Private Route table	rtb-0386eb18be5717fb9	us-east-1a	directs traffic flow from private subnets
Private Route table	rtb-0107a39f86d6d1f0b	us-east-1b	directs traffic flow from private subnets
Public Route table	rtb-06a1bf8dfb72381fd	us-east-1a	directs traffic flow from public subnets
Public Route table	rtb-06d959dc86ccf3474	us-east-1b	directs traffic flow from public subnets
web load balancer	web-app-lb	us-east-1b, us-east-1a	Distributes web traffic between web instances
app load balancer	app-lb	us-east-1b, us-east-1a	Distributes app traffic between app instances

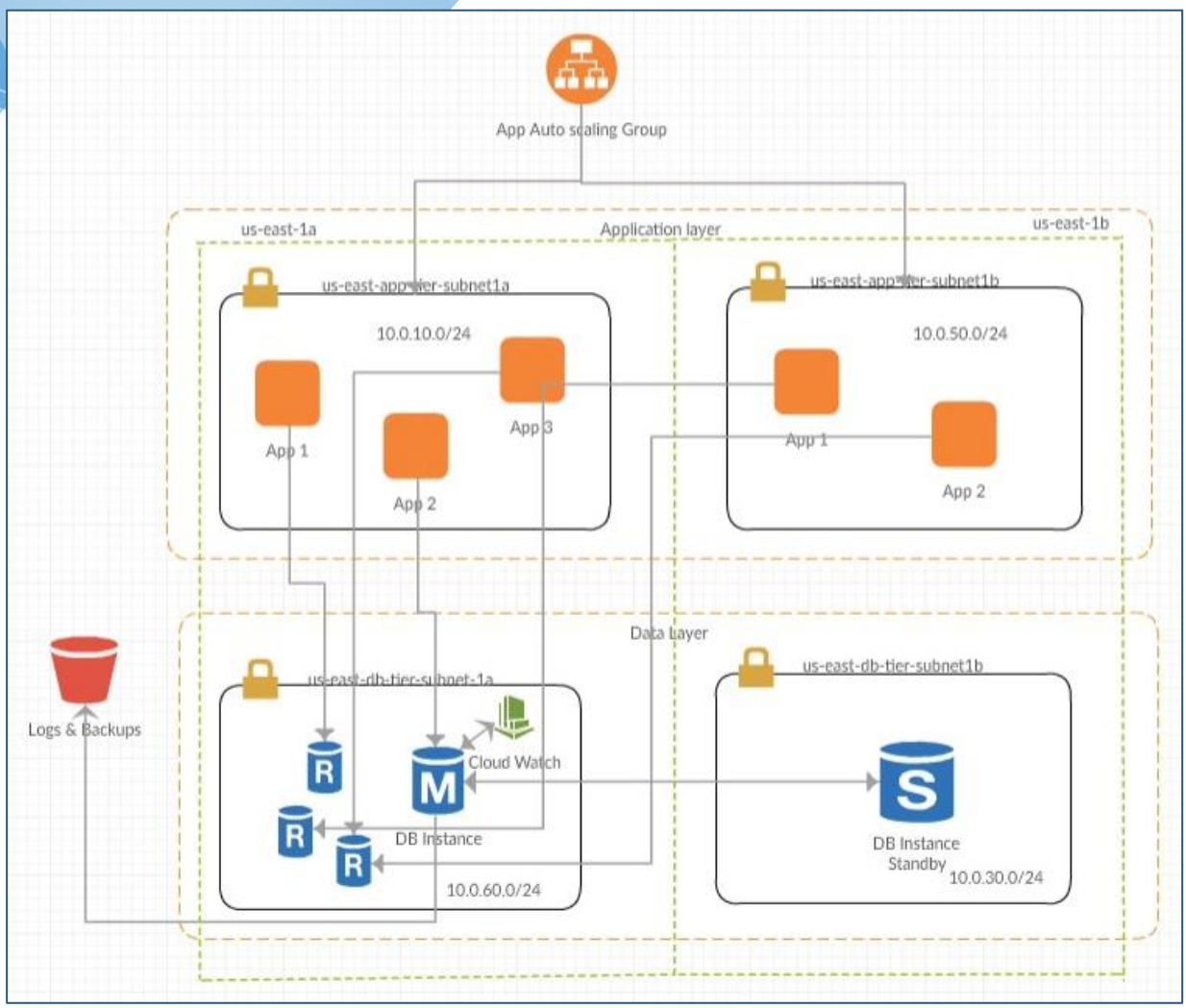
AWS Architecture



Network Layer



Data Layer


App Auto scaling Group
us-east-1a
Application layer
us-east-1b
us-east-app-tier-subnet1a
10.0.10.0/24
App 1
App 2
App 3
us-east-app-tier-subnet1b
10.0.50.0/24
App 1
App 2
Data Layer
Logs & Backups
us-east-db-tier-subnet-1a
Cloud Watch
DB Instance
10.0.60.0/24
us-east-db-tier-subnet1b
DB Instance
Standby
10.0.30.0/24

IT PROCESS

When the user launches the website, the elastic load balancer will direct the request to the available web layer's EC2 instance and then data is transferred onto the client side, clients can log in to their accounts or can create their new account online (Client Environment)

The log in data which client input is then sent through the application load balancer to the available application layer's EC2 instance, there the java application, will make a rest/get call to the relational database and check whether the data is a match in the repository or not, if it's a match then the account information of the client will be pulled and displayed on the client end and if it's not a match error will be displayed and the user will be asked to check credentials and reenter credentials. Now the client can see the account information and can make a bill payment or transfer of money.

First, he decides to make a bill payment (refer diagram 1: User Payment), everything till now is on client side, once client presses payment option, he'll be asked whether he wants to make payment of the whole amount or their custom amount. Once client enters the information, the data will be sent to the application layer and the java application will make a rest/check balance call to the relational database and make sure that the entered amount is less or more than the balance, if it's more than clients balance error will be displayed to client saying "Insufficient Balance", if it less than the client will receive message saying bill amount will be posted in 2 business days and the updated client information will be displayed. After that client can logout or continue other activity.

Secondly, if client decides that they want to make a transfer to another person, (refer diagram 2: Money Transfer)they'll find two options one for transferring money to same bank and the other would be transferring money to different bank, if the client decides that they want to send money in the same bank they'll be asked receivers account number and if the bank is different they'll be asked about the routing number and the account number of the receiver. All of this takes place on client side. Once client enters the information, the data will be sent to the application layer and the java application will make a rest/check balance call to the relational database and make sure that the entered amount is less or more than the balance, if it's more than clients balance error will be displayed to client saying "Insufficient Balance", if it less than the client will receive message

according to the type of transfer and the update client information will be displayed. After that client can logout or continue other activity.

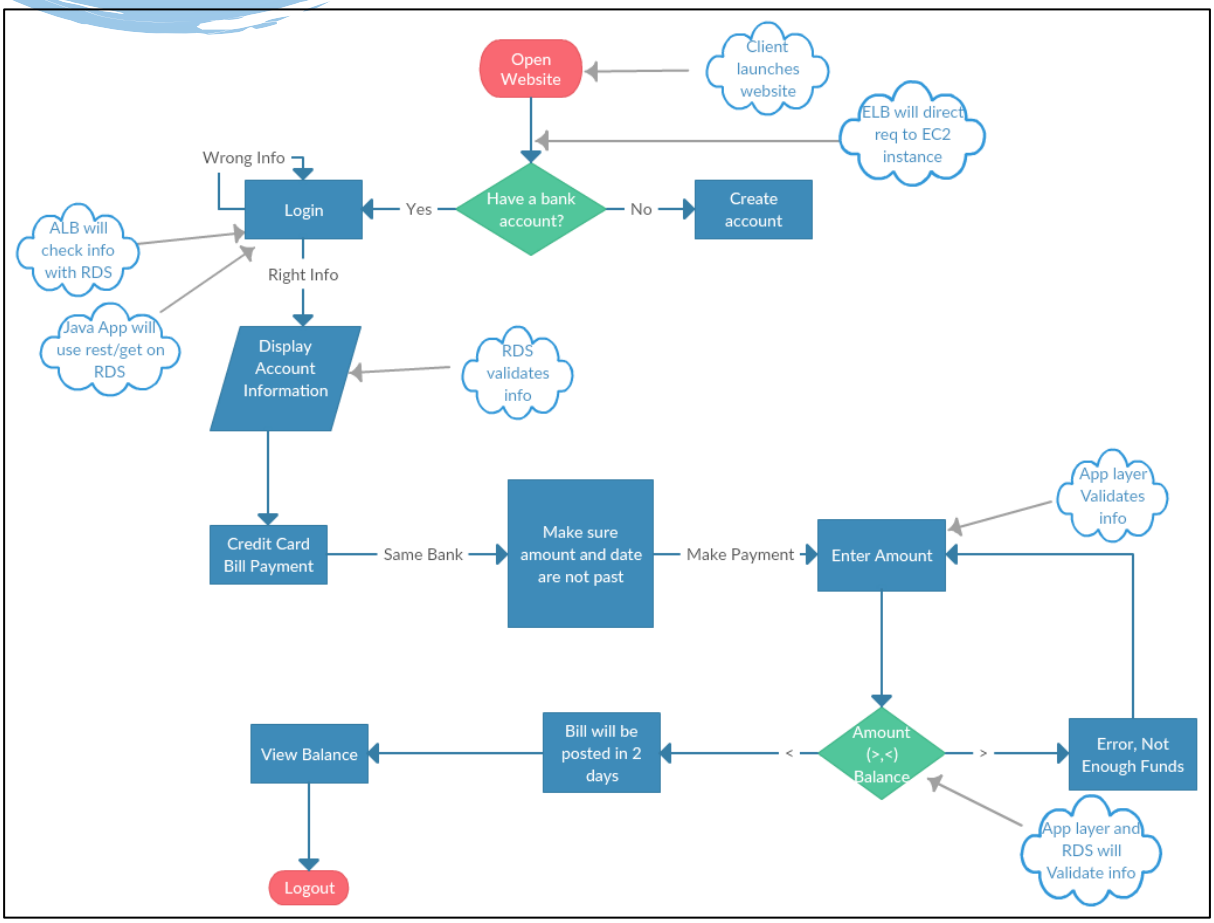


Diagram 1: Bill Payment

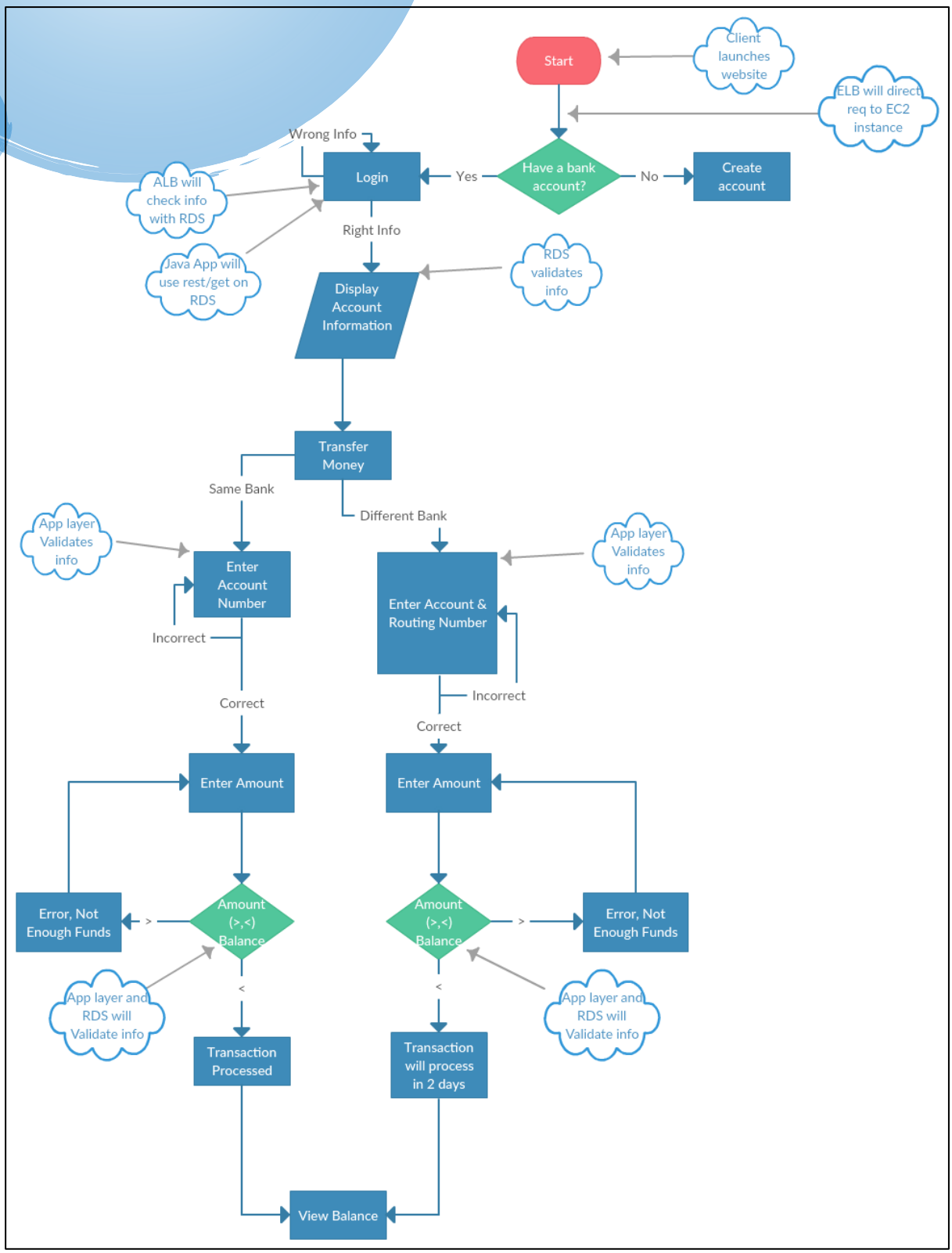
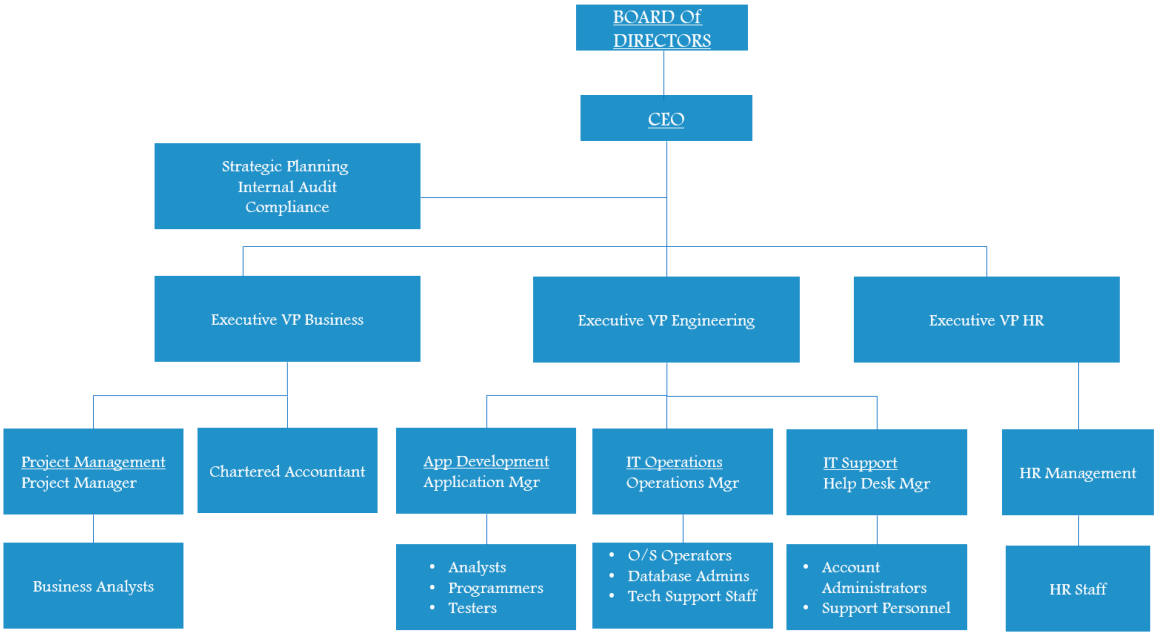


Diagram 2: Money Transfer

ORGANIZATIONAL STRUCTURE - ROLES AND RESPONSIBILITIES



Responsibilities of the Board of Directors[i] **-** The responsibility of the Board of Directors with respect to implementing a modern, scientific and acceptable Internal Control and Compliance Process in a Bank. The board shall be observant on the internal control system of the bank to accomplish a satisfactory standard of its portfolio. The board will form an Audit Committee with such directors who are not the members of Executive Committee of BOD and a Risk Management Committee from its members. Ensuring that internal audit reports are provided to the board (if asked for) without management filtering and that the internal auditors have direct access to the board's audit committee as and when required.

Structure and Responsibilities of the Audit Committee of the Board - The board will approve the objectives, strategies and overall business plans of the bank and the audit committee will assist the board in fulfilling its oversight responsibilities. The committee will review the financial reporting process, the system of internal control and management of financial risks, the audit process, and the bank's

process for monitoring compliance with laws and regulations and its own code of business conduct.

Responsibilities of the Management - In setting out a strong control framework within the organization the role of Managing CEO is very important. The board of directors of the bank will form Senior Management Team that should include the CEO and the Executive Vice Presidents. Any officer that perform a policy making function or is in charge of a principal business unit may be member of senior management system. However, any executive of Internal Control and Compliance audit should not be member of senior management system.

Responsibilities of the Board of Directors for compliance - The Bank's Board of Directors are responsible for supervising the total process of the bank's compliance work. The bank has a compliance policy of their own approved by the Board of Directors, which will be a formal document, for establishing a permanent and effective compliance function. At least once a year, the Board or audit committee of the Board reviews the scope of compliance policy whether it is working effectively or not. The board may delegate these tasks to the audit committee, if necessary.

Responsibilities of senior management for compliance - The bank's senior management is responsible for establishing a compliance policy to be approved by the BOD, which contains the basic principles to be followed and explains the main processes through which compliance risks are to be identified and managed through all levels of the institution. The duty of senior management is to ensure that the compliance policy is observed for ensuring appropriate, corrective and disciplinary action has taken in the event that breaches are identified.

Responsibilities of an Executive VP - Creating, communicating, and implementing the organization's vision, mission, and overall direction within his or her areas of responsibility such as the finance or HR department. Leading, guiding, directing, and evaluating the work of other executive leaders including assistant vice presidents, senior directors, and managers. Formulating and implementing the strategic plan that guides the direction of the Bank's business, such as developing the strategic marketing plan, in addition to implementing the overall strategic direction.

EVP HR - The Executive VP of HR is essential to the successful administration of Millennial's human resource function. The HR experts are skilled at determining and directing the company's staffing goals and strategies to support

productive and profitable business operations. In addition, they provide leadership and focus to advance the company's vision. Senior VPs of HR develop and drive organizational effectiveness and CEO on all major initiatives.

EVP Engineering - The EVP Engineering is the direct supervisor of the technical staff and also manages contributing engineering managers, who serve as the direct supervisor of the technical staff. The VP Engineering is responsible for ensuring that the bank's vision is realized through excellence in execution. The EVP Engineering is responsible for developing and maintaining a technical roadmap that will continue to innovate from a technical standpoint. The EVP Engineering may personally serve as a systems architect or may assign another engineer to assume that role.

EVP Business - The Executive Vice President, Business Management at Millennial bank is responsible for the strategic positioning of the Company and overseeing enterprise-wide marketing, digital and social media, customer research, chartered accountants, business analytics and corporate communications. Also responsible for sales and service processes, marketing analytics and project management.

Chartered Accountant – The work done under the supervision of the CA includes Statutory Audit in Millennial because none other than CA can signed the final audited balance sheet. Many people know about Internal audit, but few are known to the process settings involved. CAs also play a decisive role during formulating, defining and implementation of Standard Operation Procedure (SOP) for Millennials.

Business Analysts – Millennial's business analyst our adept at analyzing the banking business across the state. Their responsibilities are not merely restricted to. The process of analyzing the financial data, but they also provide the appropriate software solution necessary to enhance the overall productivity, profitability and the market value of the bank to help us in staying far ahead in this competitive arena.

Application Developer - The function of the application manager at Millenials is to make sure that website successfully performs specific tasks, based on the client's specifications. The developer will establish a detailed program specification through discussion with clients. clarifying what action the program is intended to perform, and keep on checking it periodically to affirm that there is no bug running inside the website and the application.

Testers – The testers are responsible for doing automated web and application testing periodically to make sure that the functionality hasn't been faltered at any point of time.

SECTION 3

RISK ASSESSMENT and AUDIT APPROACH

RISK ASSESSMENT

Risk Identification

Haddox Solutions performs risk assessment for identifying, assessing and managing of risks of Cloud Services provided by The Millennials. This is done to achieve the objectives and management also performs monitoring of controls to verify whether the controls are operating as intended. The process involves management staff, team leaders to identify significant risks related to areas of services offered to the customers.

i. Risks include misconfiguration or incorrect code fed into system which might be running on the firewalls or traffic.
ii. Risks pertaining to traffic overflow and backup of customer data which might be misconfigured or failure of the component.

We focus on responding to threats by identifying and assessing risks along with assisting management in important decision factors.

Risk Factors

Both internal and external risks need to be identified to determine the probability and impact of its occurrence.

i. Internal Factors
   a. Complexity of organizational structure.
   b. Untracked changes in the policies and procedures.
   c. Fraud opportunities and incentives.
   d. The quality and attitude of personnel hired
   e. Method of training used
   f. Unclear or changed management responsibilities.

ii. External Factors
   a. Fluctuating government and economic conditions
   b. Change in customer expectation
   c. Variation in rules and regulations
   d. Technology developments in the digital world
   e. Competitions in the market/service

Risk Analysis

Haddox Solution performs analysis which is important for company's/service success. We assess the impact of various risks to the in-scope services that needs to be assessed.

Based on the risk rating, The Millennials perform either risk review either quarterly/half yearly or yearly. To assess the impact and probability of risk, we followed the matrix below by differentiating different levels of risks for own area of activity with respect to services offered to the customers. Scores are plotted in the following table to determine if the risk falls under category of high, medium and low.

		Assessed Risk Level		
Probability	3	High	High	High
	2	Medium	Medium	High
	1	Low	Medium	High
		1	2	3
		Impact		

Few considerations taken to arrive at the assessment of what constitutes a high, medium or low

Risk Score	Probability	Impact
3	• Certainty is high • High chance of reoccurring • Area without policy or procedure in place • Specialized skills required to mitigate the risk	• Major impact on the bank • Potential loss > half million • Reputational damage
2	• Policies exist but fail to comply • Requires reviews to higher extent to manage exception	• Potential loss upto half a million • Fines from regulators • Less potential for recovery • Exposure due to weakness in control
1	• Unlikely to reoccur • Isolated incident • Policy exists and complies	• Low impact on business • Customer service are within expected level

Frequency of Testing based on Risk Rating: This is determined by the business which also includes business control testing

Risk Rating	Frequency
High	Quarterly
Medium	Half Yearly
Low	Yearly

Audit Approach

Our Audit Approach follows the below Audit procedures to focus on the impact of the environment in which client operates, client's business or financial information, financial results and its internal controls. To maintain confidentiality, integrity and availability of data, we performed proper risk assessment to increase data protection measures like data encryption, multi-factor authentication etc.,

1. Setting up audit meetings for initial audit planning
2. Understand the entity and its environment to identify risk and internal control.
3. Review the applicable and relevant laws, regulations, policies and procedures
4. Verify the existence of The Millennial's policies and procedures
5. Request information from key personnel
6. Obtain relevant evidence through enquiry /observation / inspection
7. Understand internal controls to test for existence and operating effectiveness
8. Perform risk-reassessment post testing
9. Respond to identified risk (interim/year-end testing, sampling/substantive testing)

Audit Criteria

We have identified high risk areas during our audit and have considered the below audit criteria:

i. ISO 9001:2008
ii. ITIL
iii. Market Risk
iv. PCI DSS Standards
v. IT Risk Management

SECTION 4

APPLICABLE TRUST SERVICES

CRITERIA AND RELATED CONTROL ACTIVITIES

SECURITY PRINCIPLE AND CRITERIA

Criteria	Control Activities Specified by Organization	Testing Results
CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	Policies and procedures require that employees sign an acknowledgment form upon hire, indicating that they have been given access to the employee manual	Exceptions noted
	Employee code of conduct policy is in place outlining the expectations regarding employees behaviour towards their colleagues, supervisors and overall organization	
	Background checks are performed for employees as a component of the hiring process.	
CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	A role- based security process has been defined with an access control system that is required to use roles when possible.	Exceptions noted
	The network domain is configured to authenticate users with a user account and password. The network domain is configured to enforce predefined user account and password requirements.	
	Administrative users authenticate to the access system via a user account and password.	
	Encrypted VPNs are required for remote access to production and authenticate users with a user account and password.	

CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	On a weekly basis, the human resources system sends to the security group a list of terminated employees for whose access is to be removed. The list is used by security personnel to remove access.	Exceptions noted
	The removal of the access is verified by an appropriate individual (usually a security manager).	
	System owners disable user accounts assigned to terminated employees.	
	Entity policies prohibit the reactivation or use of a terminated employee's ID without written approval of the chief information security officer. Requests for reactivation are made using the change management record system and must include the purpose and justification of the access (for business need)	
CC5.3: Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Two-factor authentication and use of encrypted VPN channels help to ensure that only valid external users gain remote and local access to IT system components.	Exceptions noted
	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	
	Password complexity standards are established to enforce control over access control passwords.	
	Privileged user access reviews are performed on an annual basis to help ensure that access to data is restricted and authorized.	

AVAILIBILITY PRINCIPLE AND CRITERIA

Criteria	Control Activities Specified by Organizaiton	Testing Results
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Business continuity and disaster recovery policy are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Exception Noted
	Weekly full-system and daily incremental backups are performed using an automated system.	
	The automated backup systems are configured to log the status of backup jobs and notify operations personnel via e-mail regarding the success or failure of backup jobs.	

SECTION 5

AUDIT FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPPONSE

AUDIT RESULTS

Finding #1: Identity and Access Management

Identity and Access Management Identity is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. According identity and access management policy and password policy, Millennial bank should enforce complex, strong passwords and password lifetime restrictions and prohibit password reuse.

CC5.4 Password complexity standards are established to enforce control over access control passwords.

Finding: We observed that password complexity requirement is not in line with Password Policy.

Analysis: As per the Password Policy, below are the requirements:

1. Password is required to have a minimum length of at least 7 characters
2. Contain both numeric and alphabetic characters.
3. Users to change passwords at least every 90 days.
4. Password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
5. User accounts are temporarily locked-out after not more than six invalid access attempts.

However, we observed that minimum password length is set to 6 which is not as per the password policy i.e., 7, and password is changed every 180 days instead of 90 days which is recommended.

The risk for this finding is considered "**Medium**" even though the password complexity standards are compromised, multi factor authenticating system is in place which might reduce the likelihood of an attacker guessing credentials and obtaining access to network resources which might lead to unauthorized access resulting in data loss or data modification.

Recommendations:

To strengthen the identity and access management, we recommended that Millennial Bank:

1. Require password complexity to be set in line with the Password Policy.
2. Require that whenever a new password is created, whether for a new user or password change request, it should follow the same password parameters.

Management Response:

Management will develop and implement procedures to ensure that password controls for servers, databases comply with the policies. Areas these processes will address include, but are not limited to, strong, complex passwords and password frequency. These processes will eliminate the need for information security control exceptions.

Responsible Party:

Scott Jr Finch, Chief Information Security Officer

Proposed Implementation Date:

March 31st, 2019

Finding #2: IT Access Control Management

Access to information and information systems will be controlled on the basis of business and security requirements. An access management process for every system would created, documented, approved, enforced and communicated to all relevant employees and partner organizations. System administrator is responsible for managing and controlling access to the application and associated information

CC5.1: A role- based access has been defined to restrict authorized internal and external user access to system components. Access should be limited to individuals with a valid business purpose

Findings: Per enquiry and inspection of user roles and privileges, we noted that 2 out of 7 users who did not have administrative level access had access to the system.

Analysis: As per the Access Control Policy, access rights are defined on need to know criteria and level of privileges are defined for each role. The ability to create and modify access records is limited to designated system administrators. We noted that 2 out of 7 active users had admin privileges to modify, delete, or update. Bill and John who had Developer role had update access that was not

required for their duties or allowed them to perform incompatible duties which was inappropriate.

The risk of this is considered "**High**" since the developers might gain unauthorized access to sensitive data, that could result in undesirable financial, reputational or operational risks. The confidentiality of data is also at risk.

Recommendation:

1. To prevent unauthorized access to sensitive data, that could result in undesirable financial, reputational or operational risks, Millennial bank should consider performing quarterly reviews of all users across application, network and database.
2. Any exception should be noted and remediated immediately.
3. Any user account role and/or permission modifications are noted
4. Periodically review user access to data and other information resources to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

Management Response:

Management has confirmed that the 2 users where given admin access during staff role changes. While informal security audits were performed when staffing role changes occurred, access reviews were not performed regularly. Millennial concurs the findings and will complete a second formal review of user account access reviews as per policy guidelines. Also, quarterly reviews will be scheduled

Responsible Party:

Scott Jr Finch, Chief Information Security Officer

Proposed Implementation Date:

March 31st, 2019.

Finding #3: IT Access Control Management – User Termination Access Review

Access to information and information systems will be controlled on the basis of business and security requirements. All the access is revoked once the user is terminated or transferred. HR personnel communicates with the system

administrator to identify the employee's final day of employment and to inform the employee of his or her rights and responsibilities. The final day is entered into the HR management system and automated email is sent to the admin to revoke all the user rights.

CC5.2: On a weekly basis, the human resources system sends to the admin a list of terminated employees for whose access is to be removed. The list is used by security personnel to remove access.

Findings: Per enquiry and inspection of user access list, we noted that 1 terminated user was active in the system.

Analysis: As per the Access Control Policy, access rights are defined on need to know criteria and level of privileges are defined for each role. The access needs to be revoked once the user is terminated or transferred. We noted that 1 terminated user – Deekshitha out of 7 users was found active. The user had access to the production group even after termination which was inappropriate.

There was no formal or timely process for notifying security administrators of employees leaving employment or changing positions.

The risk of this is considered "**High**" since the user having access to the production environment might gain unauthorized access to sensitive data, that could result in undesirable financial, reputational or operational loss. The confidentiality of customer data might get compromised.

Recommendations:

To prevent unauthorized access to sensitive data, that could result in undesirable financial, reputational or operational risks, Millennial bank should

1. Disable employees access upon termination of employment
2. Ensure that user access privileges align with job duties and modify user access privileges when job duties changes
3. Disable unused system accounts in timely manner including accounts affected by termination or change of employment
4. Ensure appropriate procedures are in place and train the appropriate person to perform the process
5. Periodically review user access to data and other information resources to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

Management Response:
Management indicated that human error was the reason for the failure to remove access of the terminated employees who was under contract. Management acknowledges the audit findings to develop and implementation procedures to disable employees' and contractors access upon termination to ensure user access privileges align with job duties and modify job duties. Upon an employee's termination of employment, they proposed to develop system that automatically generates an access deletion record in the event management system on the last day of employment and alerts to the access administration for deletion to remove human errors. Procedures will be developed no later than March 31st, 2019

Responsible Party:

Scott Jr Finch, Chief Information Security Officer

Proposed Implementation Date:

September 31st, 2019.

Finding #4: Employee Background Check Review

Human Resource Department are required to implement effective procedures that provide reasonable assurance to comply and maintain effective human resource practices. Employee fingerprints need to be submitted and/or cleared for criminal background investigations for all new and re-hire employees prior to the employees beginning any work.

CC1.4: Background checks are performed for employees as a component of the hiring process.

Findings: Per enquiry, we determined that, the auditee did not perform background screenings with fingerprints for all employees or contractors.

Analysis: During our audit, we noted that required pre-employment background and security screenings were not consistently conducted and verified for several of the hired employees examined as per background verification policy. The auditee's contract for application services did not require that appropriate background screenings be conducted of contractor staff and adequate background checks were not performed for all contracted staff.

The risk of this is considered "**High**" since failing to properly screen employees not only puts management at risk for being a victim of a crime, but it also puts business at risk as well. If someone with a history of violent crime is hired and they hurt someone while on the job, management is responsible which will lead to reputational and financial loss.

Recommendations:

We recommend that Millennial strengthen its internal controls over employee background check process to ensure that

1. All new employees submit finger print for background check before they begin employment

2. All the employees do not start employment until they receive clearance to work after investigation results

3. All employee personnel records are updated with current finger print information.

4. In addition, Human Resources should ensure information ascertained during background check phase is well documented and uniformly applied during every phase of the selection process.

5. A background check matrix should be developed to thoroughly document the process.

Management Response:

Management has reviewed the audit related to Employee Background Policy and concurs with the finding. New hires and promotions between 2015 and 2017 were performed but not tracked in as much detail as from 2017 to present. HR will begin on corrective action plan to address the findings and submit it in the next 30 days. Management proposes to include background verification and hiring process trainings to HR Department personnel and obtain a consent from the HR Manager once completing the background checks.

Responsible Party:

Emma Fischer, HR Lead

Proposed Implementation Date:

March 31st, 2019.

APPENDIX

Satisfactory:

Indicates that the control environment is strong and indicates that Management effectively identifies and controls all major types of risks posed by the area / function under their responsibility.

Generally Satisfactory:

Indicates that the control environment is sufficient to mitigate all high-risks related to the area / functions are being reviewed. While minor weaknesses exist, those have been recognized and are being addressed by Management.

Needs Improvement:

This indicates that the internal control may be lacking in some important respects, particularly as indicated by control exceptions or by the failure to adhere to written policies and procedures. The risks associated with the internal control system could have adverse effects on the efficiency and effectiveness of operations if corrective actions are not taken by Management.

Unsatisfactory:

This rating indicates a critical absence of effective internal controls to identify, monitor, or control significant risk exposures together with the existence of severe weaknesses or deficiencies in internal controls that can constitute an unsafe and unsound practice and possibly lead to significant losses or otherwise irregularities and misconduct. When audit reviews present this grading; it requires Management's and the Audit Committee's immediate attention and action.

REFERENCES

1. https://www.citizensfla.com/documents/20702/2847745/20160927+02H+OIA+2016-AUD-IT01+Network+Design+and+Architecture+Report+Executive+Summary+.pdf/e89c9822-434e-4e52-88f1-170a7aa9a332
2. https://comptroller.nyc.gov/wp-content/uploads/documents/7A03_133.pdf
3. http://www.maxi-pedia.com/top+10+risk+security+audit+findings
4. https://www.si.edu/Content/OIG/Audits/2016/OIG_A_16_05.pdf
5. PCI SSC Quick Reference Guide
6. Your Council-Policy-Access Control Policy_v4.0
7. SOC2_CSA_CCM_Report
8. LightEdge-2015-Type-1-SOC-2-Report
9. https://app.auditor.mo.gov/Repository/Press/2016112401006.pdf