CYBR 4320.20 Cyber Defensive Operations

Financial Services Team

Group Presentation, Fall 2022

Table of Contents

Team Members

Name	Career Goal
Daniel [redacted]	I ideally want to end up doing something associated with ethical hacking. What, when, and where are irrelevant as long as what I will be doing is meaningful and enjoyable
Cruz [redacted]	I want to retire.
Melissa Genovese	I want to end up as a Cybersecurity Architect.
Chris [redacted]	I would like to be a Cybersecurity Analyst.
Sheryl [redacted]	I would like to be a SOC Cybersecurity Analyst

Industry Summary

Financial Services

The financial service industry encompasses a broad range of businesses that manage financial and property assets, including credit unions, banks, payment
card issuers, insurance companies, consumer-finance companies, stock
brokerages, investment funds, individual asset managers, and some government-sponsored enterprises.

Our Industry Position

- We are 2nd in our market and when considering pandemic-induced shifts, we remained profitable. Restrictions on in-person interactions have made most of our customers more comfortable with digital banking services, making visits to bank branches, which have been long-standing relationship-building hubs, few and far in between.
- At the same time, commercial banking clients have begun to expect a level of ease, accessibility, and sophistication similar to the digital experiences they enjoy in retail banking.

Company Profile

Mid-Sized Regional Bank

- Headquarters in Texas
- Operating in Texas, Oklahoma, New Mexico and Arizona
- $750 million in Assets under management
- Two data centers (Irving, TX and Denver, CO)

Business Challenges

- Customer adoption of mobile technology for payments and transaction services
- Rising infrastructure cost of legacy systems driving cloud adoption and automation
- Growing competition with 100% online banks and alternative lending products
- Regulatory compliance a key driver in adopting CIS Controls

Cyber Risk Outlook and Trends

- Cyber attacks will grow in frequency and sophistication
  - Proliferation of attack tools and social popularization of hacking.
- Highly trained workforce will continue to be a key defense
  - Hackers continue to exploit social engineering and use fraudulent impersonation to gain access to networks and systems.
- Malicious insider activity will increase risk of cyber fraud
  - Continued compromise of trusted parties pushes demand of oversight on internal data handlers and processors.
- Third-Party assurance burdens will increase
  - Distributed computing (cloud) will expand the attack surface as third-party services replace traditional infrastructure.
- Regulatory burden will drive security and compliance challenges
  - Pace of regulatory change requires increased awareness and compliance reporting.
  - Data mobility requires improved fidelity and visibility of data location and attributes to satisfy compliance.
  - Financial and reputational risk associated with violations and breaches force responses from entities handling regulated or consumer data.

Cyber Risk MATRIX

- The following risk matrix assisted the team in determining the best controls to deploy in protecting our information assets.

Threats	Compliance Requirements	Risk
Who is attempting to attack us?	What regulations are we accountable to? What compliance frameworks are required to operate?	What is our organizational risk appetite and tolerance? What are our assets and how valuable are they to our operations?
Bad actors, black-listed countries, internal threats, and cyber criminals utilizing spoofing, malware, DDOS, CORS, SOAP, MFA, credential stuffing, cross site scripting, root traversal, privilege escalation attacks.	FINRA SEC,NIST, GDPR, UK/EU, PCI-DSS, ISO-27001, SOX, GLBA, BSA, Commodity Futures Trading Commision, PSD2, NYDFS-500, PCI, HITRUST, BYOD, MDM, FFIEC, CCPA, FRCA, Fair and Accurate Credit Transactions Act, Right to Financial Privacy Act, ITAM	Penalties and fines, Operational risks, Reputational risk, Fiduciary risk, Contractual penalties
Data	**Applications**	**Hardware/Infrastructure**
What are the data elements we store and transmit and have they been evaluated based on the threats, compliance and risk attributes?	What applications do we build, use and manage and what are their risk attributes?	What hardware and infrastructure do we use and manage and what are their risk attributes?
Mobile numbers, account numbers, routing numbers, names, social security numbers, user-name and passwords, user security question, payment history, equity, credit score, stocks and investments, Roth IRAA, saving accounts, brokerage accounts, loans, addresses, debt, consumer habits, crypto-assets, and fixed incomes.	Microsoft Edge Browser, Microsoft Office, Windows 11, MongoDB Tital, Zoom, Oracle Database, Serenity Deals CRM Software, Microsoft Windows Server, NinjaOne, Zenmap, PWNie Express, OpenNSM, GFI Languard, Goverlan, Tidal, Semantec, BeyondTrust, Faronics, Airlock, Crowdstrike	BUFFALO TeraStation 5410DN - NAS server - 32 TB, SonicWall Network Security Firewall, Cisco IP Phone 8865, Xerox VersaLink C505/X Color Duplex LED Printers, HVAC System, ServiceTitan HVAC Software, Cisco Meraki MS390-48 Switches, Cisco Catalyst 8300-1N1S-4T2X Routers, Cisco Catalyst 9100 Wireless Access Points, Dell Latitude 3520 Laptops, Dell OptiPlex 7090 Small Form Factor Desktops, BYOD Phones (Apple & Android)

Cyber Controls Review Methodology

- Questions we considered when evaluating the system:
  - What security controls are most effective to mitigate risks uncovered by risk assessment activities?
  - How mature is our current security organization and what gaps exists that require attention?
  - Which security improvements should we select based considering deployment of the new system?

New Product Proposal

Business Drivers

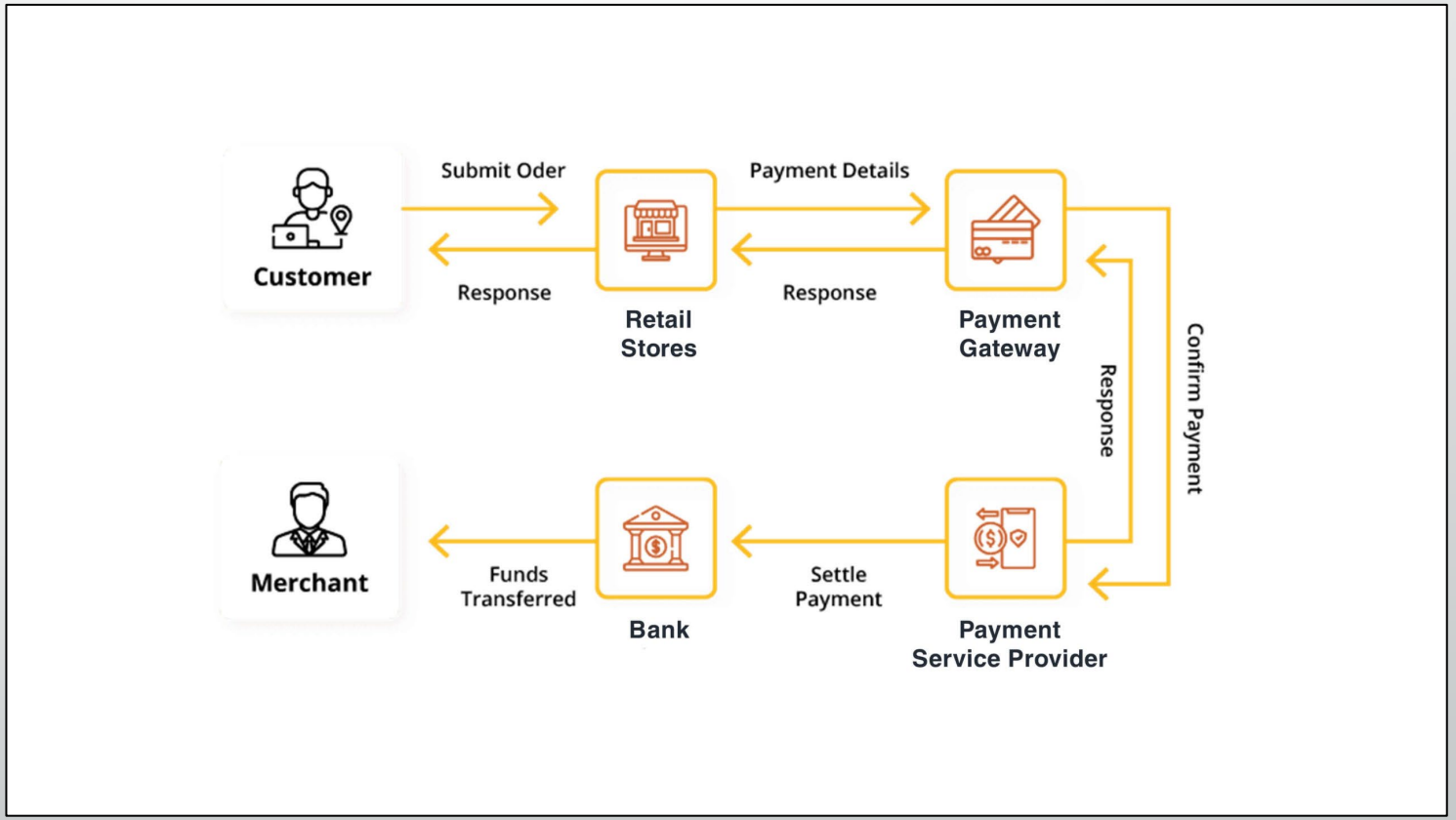
- Our peer banks rapidly embraced digitization and quickly responded to customer demand to adopt digital services for their merchant/payment products.
- Our bank has been slower to adopt and needs to shift in order to remain competitive.
- We have an engaged AWS professional services to support our investment in a cloud-based solution.

Success Measures

- Net interest margin (NIM)
- Return on assets (ROA)
- Risk-adjusted return on capital (RAROC)
- Revenue generated by APIs
- Monthly active users

Solution High Level Design

- Bank customers will leverage a new interface that we will deploy in AWS to interface with Payment Service Providers.
- The solution will need to authenticate users, transactions, payment gateways and internal staff that administer the solution.



Key Recommendation – Why CIS Controls

CIS controls are designed to assist cyber security professionals by providing guidance for implementing broad baseline technical controls that are required to ensure a robust network security posture. The CIS control framework covers key areas that address the risk posed by this technology deployment and expansion:

- ✓ Secure Configurations for Hardware and Software
- ✓ Continuous Vulnerability Assessment and Remediation
- ✓ Controlled Use of Administrative Privileges
- ✓ Maintenance, Monitoring, and Analysis of Audit Logs

Findings of the CIS Community Defense Model (CDM) 2.0, show that they're effective at mitigating approximately 86% of all MITRE ATT&CK Techniques. More importantly, the Controls are highly effective against the top five attack types found in industry threat data.

Led by the Center for Internet Security® (CIS®), the CIS Controls have matured into an international community of volunteer individuals and institutions that:

Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action

- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them
- Create benchmarks for specific technology architectures and control environments
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community

STRIDE Threat Assessment

In addition to evaluating the Business Risks, Compliance, Architecture Requirements, Control Framework and Risk Appetite, we also needed to review the proposed solution and identify the specific threats that could materialize against the application.

Our security team conducted:

1. A technical risk assessment designed to identify, evaluate and manage system or network threats, architectural design flows and recommend security mitigations.
2. The exercise included process and product owners, developers, solutions architects, control owners and security assessors.
3. It is included in the design phase of software development with a stated goal of design flaws and control gaps based on common cyber security threats: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **E**levation of Privilege

STRIDE Results

- Recommendation: Implement CIS controls within the enterprise and new application to ensure adequate defense against these threats.

Threat	Issue	Gap	Mitigation
Data Theft, Information Disclosure	Insecure handling of encryption keys in and extended session timeout	1. Keys are stored in an access control file rather than a hardware security module or key vault 2. Application allows extended session that could allow threat actor time to exploit	HSM should be used or equivalent FIPS key vault to protect encryption keys. Session time out should be no more than 15 min.
Spoofing, ID, Tampering	Insecure web traffic protocol	HTTP was used internally for data transfer via reverse proxy. Traffic should be HTTPS	HTTPS or IPSec should be used for point to point traffic.
IAM Misrepresentation	ID provider does not support biometric challenge for identification and authentication	Biometric support provides an additional factor and can be used to ensure the correct person is accessing payment services.	Select an ID provider that can utilize biometric features supported in iOS and Android.

Roadmap to Address Control Gaps

Current State

CIS Assessment Results:
129 out of 144 of CIS Controls have sufficient implementation plans
10% need implementation support or enhancement

Compliance Evaluation Results:
129 out of 144 of FFIEC-Aligned Controls are sufficient
10% need implementation support or enhancement

CIS Control Coverage Rate:
92% of IG1 Controls
91% of IG2 Controls
90% of IG3 Controls

Plan

PHASE ONE:
Identify the gaps in CIS Control Coverage

SUCCESS CRITERIA:
Successfully identified all gaps.

PHASE TWO:
Develop plan to fill in gaps in CIS Control Coverage

SUCCESS CRITERIA:
Successfully developed plan to fill in gaps.

PHASE THREE:
Implement plan to fill in gaps in CIS Control Coverage

SUCCESS CRITERIA:
Successfully implemented plan to fill in gaps.

Future State

CIS Control Coverage Target:

100% of IG1 Controls
100% of IG2 Controls
90% of IG3 Controls

Controls Effectiveness Monitoring Strategy:
Conduct quarterly control effectiveness and compliance assessments using https://csat.cisecurity.org/.
Report results to the security governance and compliance steering committee and prioritize remediation and action plans.

Priority 1 Control Implementation Items

- 1. AWS IAM Security Best Practices

Description: When users do not properly define and configure permissions attached to a service, privilege escalation could happen. This could allow a compromised low-privileged user to change the password of a high-privileged user. The same goes for improperly configured role permission policies, which could allow a malicious user to create a new policy version that could in turn allow the changing of permissions in a policy. If role permissions are not securely set, the malicious user could be granted full administrator privileges. It is important to note that although it takes time to create a comprehensive list of roles that states which users and services in the architecture are allowed to pass, such a list helps ensure a more secure, misconfiguration-free system.

Justification: Security Requirement

- 2. AWS WAF

Description: A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others

Justification: Security Requirement

- 3. Amazon EC2 API Gateway

Description: Don't expose EC2 to the wider Internet unless strictly needed. If they are exposed, do not expose them for direct invocation, but put them behind an API Gateway. API Gateways provide DDOS protection, rate limiting and simple integration with "Authentication as a Service" providers like Cognito or Okta.

Justification: Security Requirement

- 4. AWS VPC Network Access Control Lists (ACLs)

Description: In case of AWS VPC misconfiguration, a Threat Agent may easily connect to any internal AWS component or service

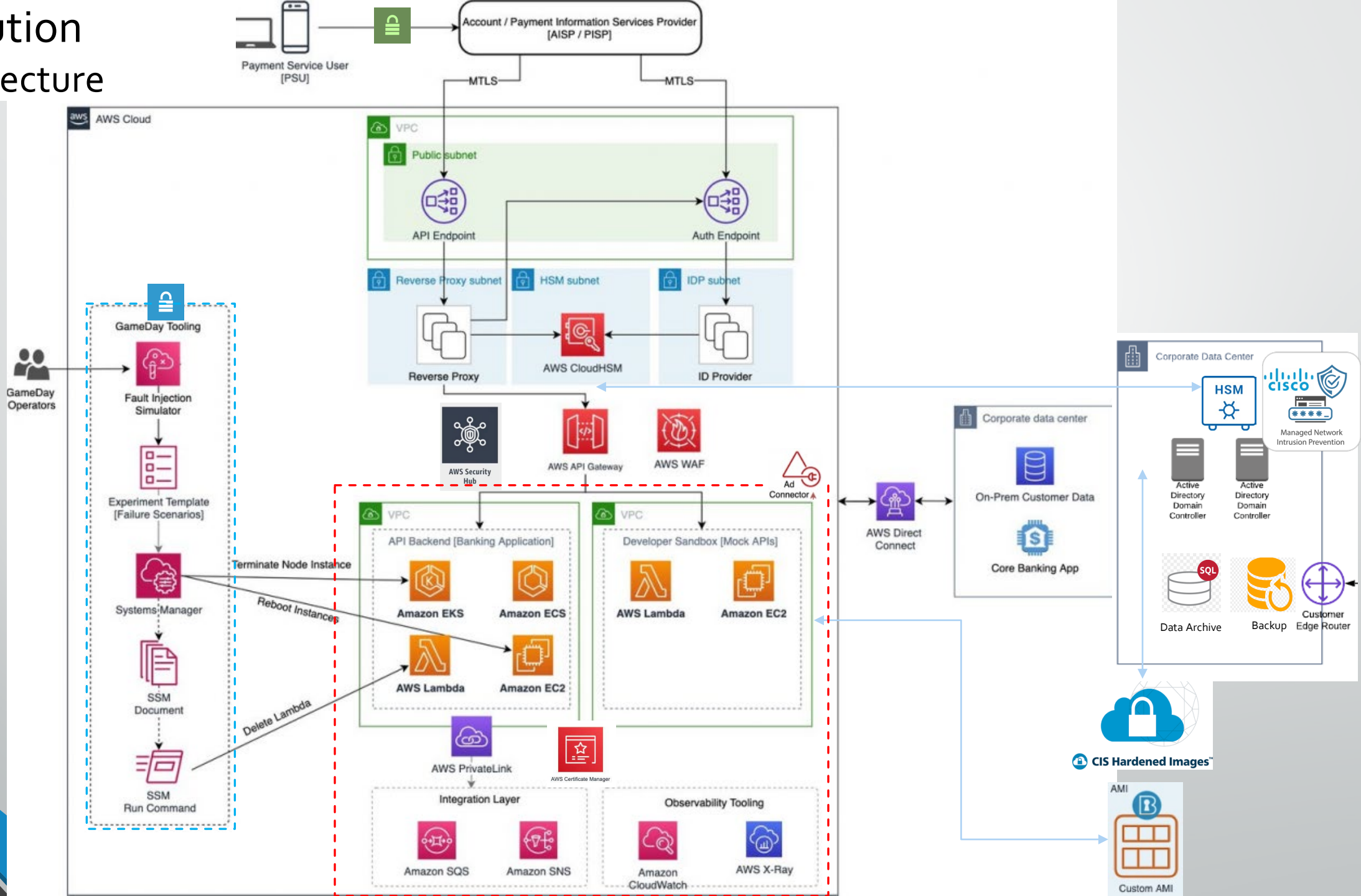
Justification: Security Requirement

- 5. AWS Storage Encryption

Description: Ensure AWS Storage sensitive information encrypted at Rest to prevent data leakage, unauthorized access or compromise

Justification: Security Requirement

Solution Architecture



CIS Controls