03/24/24

Laws, Regulations & Standards Proposal

PROPOSED BY
LIELA PRESSLEY

ASB

ACROSS THE STATES BANK

ITT-380 | INFORMATION ASSURANCE
PROFESSOR CHRISTOPHER MOLSTAD
GRAND CANYON UNIVERSITY | COLLEGE OF ENGINNERING AND TECHNOLOGY

ASB

ACROSS THE STATES BANK

TABLE OF CONTENTS

ORGANIZATION OVERVIEW

ACROSS THE STATES BANK

$10 BILLION BUSINESS

PERSONAL & BUSINESS/COMMERCIAL BANKING CUSTOMER NEEDS

132,00+ EMPLOYEES

17,000 BRANCH OFFICES & ATMS NATIONALLY

HOME OFFICE IS IN METROPOLIS, CA

24/ CUSTOMER SUPPORT

PHONE, EMAIL, ONLINE CHAT

CONSTUMERS CAN MANAGE FINANCES GLOBALLY

ONLINE BANKING

MOBILE BANKING

CONSTUMERS CAN COMPLETE TRANSACTIONS/ACCESS IN EU NATIONS

FOREIGN PARTNERSHIPS IN SOUTH AMERICA & ASIA

ASB STORES, PROCESSES, MOVES, & MANAGES DATA FOR A LARGE AMOUNT OF EMPLOYEES, CUSTOMERS, GLOBALLY THROUGH VARIOUS DEVICES, APPLICATIONS, STORAGE TYPES (CLOUD, SERVERS, ETC.)

ALL OF THE DATA ASB IS MANAGING NEEDS TO BE ACCESSIBLE FROM DIFFERENT AREAS OF THE USA AND GLOBE, 24/7 AND REMAIN CONFIDENTIAL.

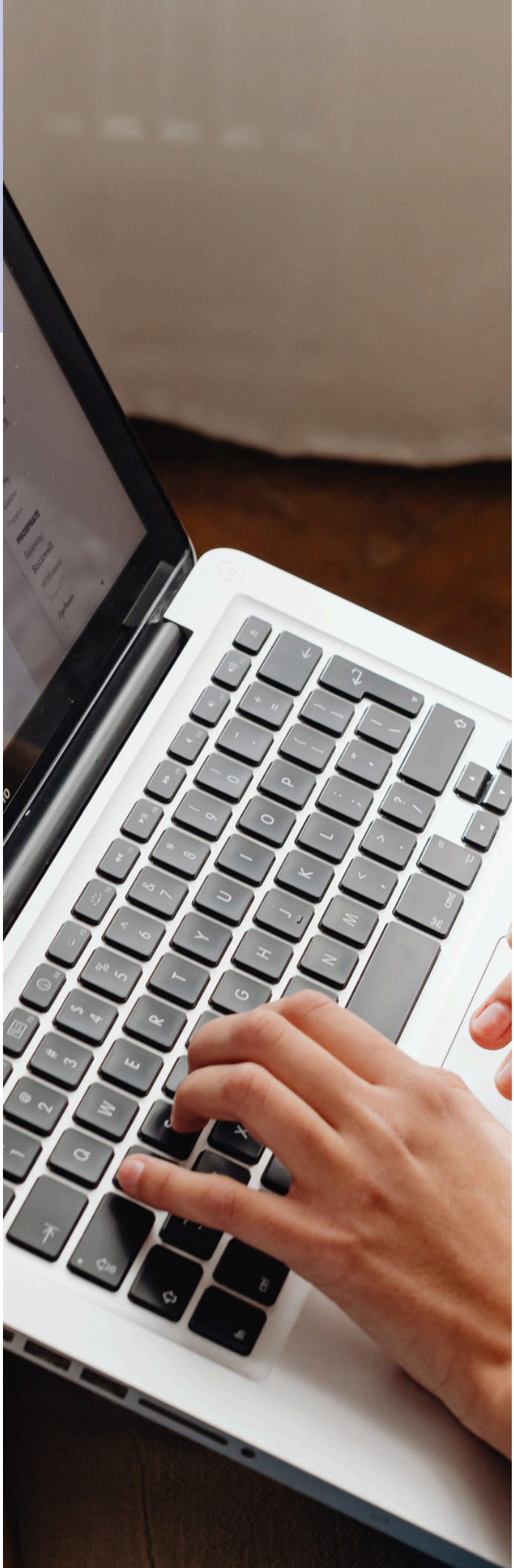
LOCAL & FEDERAL LAWS/REGULATIONS

LOCAL

ASB has over 17,000 different brick and mortar locations across the United States there for each location must adhere to the laws/regulations that are relevant to that state.
For instance, home office for ASB is located in California obligating it to adhere to the California Consumer Privacy Act (CCPA) which is established to protect the right of data subjects in CA. It refers to limiting the timeframe within legal action can be brough against a org for violating CCPA rights and duration for which the org is allowed to retain/store data of a CA consumer.

FEDERAL

There are many federal laws and regulations for banks/organizations in the financial service industry to adhere to in the United States which include but are not limited to:
GLBA: which lays out the Client Data Protection for financial institutions
SOX: for Fraud Prevention
New York — NYDFS Part 500: New York Department of Financial Services Cybersecurity Bill



INTERNATIONAL LAWS/REGULATIONS

INTERNATIONAL

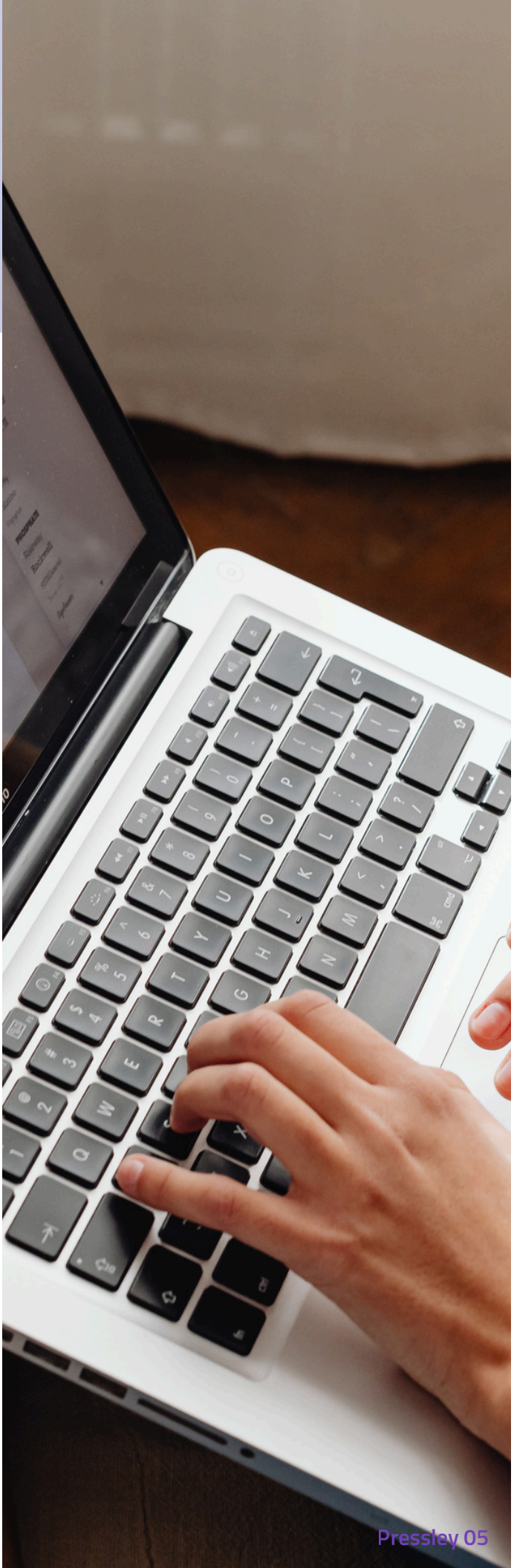
In order to maintain CIA (Confidentiality, Integrity, Accessilbility) to all ASB consumers and employees in EU and globally, it is essential that ASB abides by the global standards set in place.

Since ASB is partnered with EU organizations and allows consumers to manage and make transactions in EU, **GDPR (General Data Protection Regulation)** is a European law that applies to all companies procssing data of EU citizens. It mandates how data is used, protected and goversn how consent is used to collect it. It also requires timely reporting of breaches if it affects EU citizens.

In addition, the **UK Data Protection Act** which is similar to the GDPR but is amended for UK citizens and have fines for non-compliance.

As ASB continues to operate in EU, the **Payment Services Directive 2 (PSD2)** is a law meant to make it easier for financial services to integrate and securely share data while making those payment system safer. It also has specific technical standards for stronger customer authentication,. This is applicable to all paymetns that start, travel thorugh or end in the EU making it extremely relevent to ASB.

Basel II Banking Guidelines is a framework and security standards that aligns regulatory captial requirements to the underlying risks that exist in banks. Basel II will propel banks towards identifying risks and improve risk management.



RECOMMENDATIONS

Standards, Control, Compliance, Approach

ASB

ACROSS THE STATES BANK

Standards

There are many standards that ASB is to adhere to due to the multi-faceted nature of the business and the many different services it offers to the high volume of consumers. Some of the standards include but are not limited to: **PCI DSS** for Credit Card Transaction Security and Federal Financial Institutions Examination Council (FFIEC).

ISO/IEC 27002:2022:Best Global Standard is a great code of practice for ASB to follow and use a foundation for sets of controls in security risk management. It contains over 114 security controls, 35 control objectives in 14 different domains and is a great guide for identifying, assessing, reducing and mitgating information security risks in a information security management system.

Compliance

ASB has goals of expanding to having annual sales be $12 billion in the next 3 years, improve their customer relations, increase services in commercial sector by 15% and acheive high customer service satisification. In order to reach these goals while maintaining and improving security there needs to be regular audits and compliance checks. The Dams Sector Cybersecurity Capability Maturity Model (C2M2) allows organizations to conduct self-evaluations to improve cybersecurity programs no matter the size/type allowing for flexibility for growth/expansion/departments.

Approach

Due to ASB being such a large business; being one of the biggest banks in the world with various devices and data that needs to be storage, transferred, processed and collected , it will be using cloud services to outsource some of the storage and diversify its location. Because of the signficant importance of information security being infilitrated into every crevice of ASB's operations it needs to be the #1 priority of senior leadership. I highly suggest that a Top-Down Approach in information assurance operations is the only approach appropriate for ASB to succesfully build a reliable ISA and maintain it.

THREATS, RISK, VULNERABILITIES

ASB

ACROSS THE STATES BANK

Biggest Threats in Finance Services/Banking

In order for ASB to provide CIA for its consumers and employees, senior leadership must work closely with security professionals to ensure that the company makes security threat, risk, and vulnerabiltity awareness a top priority. The more aware ASB is aware the more the organization can determine its attack surface, where to prioritize risk assesments and more.
The Biggest Threats to look out for in a organization like ASB includes but is not limited to the following:

- **Phishing Attacks (Convo Thread Hijacking, Links, etc.)**- over 90% are successful, increased by 22% in the first months of 2021, most targeted industry
- **Ransomware-** Publishing greater portions of seized sensitive data until ransom is paid, very effective against financial, attacks increased by 151% in first months of 2021
- **SQL Injections, Cross-Site Scripting, Local File Inclusion, OGNL Java Injection-**94% of cyber attacks in financial industry are by one of these four methods
- **DDoS Attacks-** 2020, financial services had the highest number of DDoS attacks, due to diverse attack surface: banking IT infrastructure, customer accounts, payment portals, etc.
- **Supply Chain Attacks**- vendors don't take cybersecurity risks as seriously as clients,
- **Bank Drops-** cybercriminals store stolen funds in fake bank accounts (bank drops) opened with stolen customer creds

SECURE & MANAGE RISK

ACROSS THE STATES BANK

After reviewing the standards, regulations, and legislation as a foundation for your ISA and looking at the biggest threats and attack vectors there are some methods I suggest reviewing first.

To combat the likelihood fo cybercriminals committing identity theft, stealing credentials, and reduce credential stuffing ensure that **Zero Trust Architecture and Privileged Access Management Policies** are created and implemented by leadership and within your information security operations. Ensure that **Third Party Risk Management** which holds 3rd parties accountable for security vulnerabilities but making it the responsibility of ASB security operations to ensure they are being followed. And to have **Multi-Factor Authentication** implemented on every endpoint throughout the company from consumer user to every employee regardless of their position or location. Having this policy in place will reduce the ease for threat actors to take advantage of credentials.

Firewalls that are regularly maintenced and updated are essential to detecting and blocking malware injection attempts but can not be the only line of defense. Security teams need to be ready to defend but also prepare for when a data breach will occur. Ensuring that ASB has a reliable and **regular data back-ups** on hand to restore business continuity and acccessibility for consumers and employees alike during ransomware attacks or natural disasters. In addition, ensure that **Attack Surface Mangement i**s being implementd which allows for professionals to detect data leaks which will reduce the likelihood of successfull data breaches internally and through a third-party/vendor network.

REFERENCES

CIS controls. (n.d.). CIS. https://www.cisecurity.org/controls

Cloud banking: More than just a CIO conversation. (2023, March 27). Deloitte. https://www.deloitte.com/za/en/Industries/financial-services/perspectives/bank-2030-financial-services-cloud.html

DAMS Sector Cybersecurity Capability Maturity Model (C2M2) 2022 | CISA. (2022, October 26). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/dams-sector-cybersecurity-capability-maturity-model-c2m2-2022#:~:text=The%20Dams%20Sector%20Cybersecurity%20Capability,or%20size%20of%20the%20organization.

Department of Homeland Security. (2013). INFORMATION ASSURANCE AND CYBER SECURITY STRATEGIC PLAN. In INFORMATION ASSURANCE AND CYBER SECURITY STRATEGIC PLAN. https://ets.hawaii.gov/wp-content/uploads/2012/09/Governance_Info-Assurance_Cyber-Security.pdf

Iannarelli, J. (2023, November 8). The 9 Best Cybersecurity Frameworks for Financial Institutions | FBI John. FBI John. https://fbijohn.com/best-cybersecurity-frameworks-financial-institutions/

Pecb. (n.d.). ISO/IEC 27002:2022 — Information security, cybersecurity, and privacy protection. https://pecb.com/whitepaper/isoiec-270022022--information-security-cybersecurity-and-privacy-protection

Team, H. (2023, December 5). Financial Services Cybersecurity: Top 2023 Regulations to Know. Hypr Blog. https://blog.hypr.com/top-financial-services-cybersecurity-regulations

The 6 biggest cyber threats for financial services in 2024 | UpGuard. (n.d.). https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services