Cybersecurity Plan

**Cybersecurity Plan**

**Purpose**

The Taxare Application Cybersecurity Plan serves as the bedrock of our commitment to fortifying the security infrastructure of our organization. It underscores our unwavering dedication to protecting both our clients' data and our operational integrity. In a world increasingly defined by digitalization, the significance of data security cannot be overstated. As such, this cybersecurity plan is pivotal, serving a dual purpose:

**1. *Protecting Our Organization***: At its core, this plan is our organization's primary defense against the diverse and ever-evolving landscape of cyber threats. It stands as a comprehensive shield that safeguards not only our sensitive data but also our day-to-day operations and the invaluable reputation we have built over the years.

**2. *Instilling Confidence***: Equally crucial, this plan is designed to instill unwavering confidence in our clients, partners, and stakeholders. It is a testament to our commitment to handling their data with the utmost care and security, forging a deep and lasting trust in the services we provide.

**Scope**

***Principle***: Define how the policy applies to the organization. This includes:

The scope of our Taxare Application Cybersecurity Plan is far-reaching, encompassing every facet of our organization to ensure a comprehensive and unrelenting commitment to cybersecurity. This includes:

***Personnel***: The policies and measures outlined in this plan apply to every member of the Taxare Application team, including employees, contractors, and associates. If they access any of our systems, networks, or data, they fall under the protective umbrella of this cybersecurity initiative.

***Equipment, Networks, and Processes***: No stone is left unturned as this plan covers all computing equipment, networks, and processes used within our organization. This includes both company-provided infrastructure and personal devices used by our staff to access our systems and data.

***Timing***: The policies laid out in this plan are always in effect, without exception. Cybersecurity is not bound by time, and our commitment to it remains unwavering regardless of the hour.

***Locations***: Whether within the confines of our physical premises or during remote work scenarios, the policies articulated within this plan apply uniformly to all locations where Taxare Application conducts its operations.

***Exceptions***: In the interest of upholding the integrity and consistency of our security standards, this cybersecurity plan allows for no exceptions. Any deviations from these policies must receive explicit approval from Taxare Application's Chief Information Security Officer (CISO), ensuring that our security remains steadfast.

**Plan Framework**

A robust cybersecurity plan is built upon a well-established framework that draws from expert guidance and industry best practices. For the Taxare Application Cybersecurity Plan, we have chosen to anchor our strategy in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework is widely recognized as an international standard, providing organizations of all sizes with the tools to apply risk management principles effectively and enhance security and resilience. (Reference: [NIST Cybersecurity Framework] (https://www.nist.gov/cyberframework))

**Categories and Subcategories*:***

**1.Identify (NIST CSF):**

***Inventory Physical Devices and Systems (ID.AM-1):*** This subcategory plays a pivotal role in maintaining visibility into our physical devices and systems. By doing so, we address the cybersecurity challenge of ensuring that our inventory remains accurate and up to date. This reduces the risks associated with unauthorized or undocumented assets, bolstering our overall security posture.

***Legal and Regulatory Requirements (ID.AM-6***): Ensuring compliance with legal and regulatory requirements is paramount in the ever-evolving landscape of cybersecurity. This subcategory addresses this challenge, ensuring that our organization remains in full compliance with relevant laws and regulations. By doing so, we reduce the risks of non-compliance, which can have legal and reputational consequences.

***Roles and Responsibilities (ID. GV-3):*** To manage cybersecurity effectively, it's crucial to have well-defined roles and responsibilities within our organization. This subcategory ensures that everyone knows their role in protecting our data and systems. By reducing ambiguity and miscommunication, we mitigate risks associated with a lack of clarity in responsibilities.

**2.Protect (NIST CSF):**

***Account Management (PR.AC-4):*** Effective account management is essential for maintaining the security of our systems. This subcategory addresses the cybersecurity challenge of managing user accounts properly. By doing so, we reduce the risks associated with unauthorized access and misuse of accounts, protecting our sensitive information.

***Account Authentication and Password Management (PR.AC-7):*** Passwords are often the first line of defense against cyber threats. This subcategory focuses on enhancing authentication and password management practices. By reducing the risks associated with weak or compromised credentials, we bolster our overall security posture.

***User Training (PR.AT-1)***: Human error is a significant cybersecurity challenge. This subcategory addresses the need for user training and awareness programs. By doing so, we reduce the risks associated with employees falling victim to social engineering attacks and other cyber threats.

***Data Backups (PR. IP-4):*** Data is an asset that requires protection. This subcategory emphasizes the importance of regular data backups. By reducing the risks of data loss or corruption, we ensure business continuity and data integrity.

***Incident Response Plan (PR.IP-9):*** Cyber incidents are a matter of "when" rather than "if." This subcategory establishes a robust incident response plan, ensuring swift and effective responses to security incidents. By doing so, we reduce the potential impact of incidents on our organization.

***Incident Recovery Plan (PR.IP-9):*** In addition to incident response, incident recovery is critical. This subcategory addresses the cybersecurity challenge of incident recovery, minimizing downtime and data loss during the recovery process.

***Vulnerability Management Plan (PR.IP-12):*** Proactive vulnerability management is essential for staying ahead of threats. This subcategory focuses on identifying and addressing vulnerabilities promptly, reducing the risks associated with unpatched vulnerabilities and potential exploits.

**3.Detect (NIST CSF):**

***Execution of the Vulnerability Management Plan (DE.CM-4 and DE.CM-8):*** Efficient execution of our vulnerability management plan is crucial for detecting vulnerabilities and addressing them promptly. By reducing the risks associated with unpatched vulnerabilities, we enhance our overall security posture.

**4.Respond (NIST CSF):**

***Execution of the Incident Response Plan (RS.RP-1):*** Timely and effective incident response is vital. This subcategory ensures that our incident response plan is well-executed, reducing the potential impact of incidents and minimizing risks.

**5.Recover (NIST CSF):**

***Execution of the Incident Recovery Plan (RC.RP-1)***: Incident recovery is a critical phase. This subcategory focuses on the execution of our incident recovery plan, reducing the risks associated with downtime and data loss during recovery efforts.

These categories and subcategories were carefully selected to align with our organization's specific cybersecurity objectives and address the cybersecurity challenges we face. Drawing from reputable sources like NIST and industry best practices, our cybersecurity plan is poised to strengthen our security posture effectively.

**References:**

National Institute of Standards and Technology (NIST) Cybersecurity Framework. NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. NIST Framework for Improving Critical Infrastructure Cybersecurity

Center for Internet Security (CIS) Controls. CIS Controls

ISO/IEC 27001. International Organization for Standardization (ISO). ISO/IEC 27001 Information Security

**Identify**

1. ***Asset Inventory:***
   1. We are planning to Identify and maintain an inventory of all data assets within Taxare, including user tax data and Chartered Accountants' details. Planning to use AWS Config to maintain an inventory of AWS resources and configuration changes, which can help identify and track assets.

This involves tracking data types, locations, and access points.

1. ***Data Classification:***
   1. Classifying the user tax data and Chartered Accountants' details based on sensitivity and confidentiality. Planning to achieve this by Leveraging Amazon S3 bucket policies and IAM policies to classify data stored in Amazon S3 based on its sensitivity and apply appropriate permissions.

For instance, user tax data should be categorized as highly sensitive, and Chartered Accountants' details as confidential.

1. ***Risk Assessment:***
   1. Conducting a risk assessment specifically for these critical assets to identify potential threats and vulnerabilities that could compromise user tax data and Chartered Accountants information. Utilize AWS Trusted Advisor to assess AWS environment's security and identify risks and vulnerabilities.

By Considering risks like unauthorized access or data breaches.

1. ***Threat Modeling:***
   1. Developing threat models that focus on threats and attack vectors that could target user tax data and Chartered Accountants' details. Implement AWS Identity and Access Management (IAM) for fine-grained control over user and application access to AWS resources, helping to mitigate threats.

Considering factors like data exfiltration, insider threats, and external attacks.

1. ***Business Impact Analysis:***
   1. Performing a business impact analysis to determine the criticality of user tax data and Chartered Accountants' details. By Assessing the potential impact of a breach on users' privacy and the reputation of Chartered Accountants. Also, try to assess how the availability of the application is going to impact. Using AWS CloudFormation to manage and provision AWS resources and analyze the impact of changes on the application.
2. ***Compliance Requirements:***
   1. Identifying and adhering to compliance requirements specific to the handling of tax data. By ensuring compliance with tax-related regulations and data protection laws to protect user data and Chartered Accountants' information. AWS provides compliance documentation and offers services like AWS Artifact for access to AWS compliance reports to align with regulatory requirements.
3. ***Stakeholder Analysis:***
   1. This is done by analyzing the stakeholders involved with user tax data and Chartered Accountants' details, including users, Chartered Accountants, administrators, and regulatory authorities. Determine their roles and responsibilities in protecting this data. Implement AWS Organizations to manage and govern AWS accounts and define IAM roles and policies for different stakeholders.
4. ***Security Policies and Procedures:***
   1. By Developing and enforcing security policies and procedures tailored to the protection of user tax data and Chartered Accountants' information. Implement AWS Identity and Access Management (IAM) policies and Service Control Policies (SCPs) to enforce security policies and procedures.

Implement encryption, access controls, and data protection measures specific to these assets.

1. ***Security Awareness:***
   1. Promote security awareness among Chartered Accountants and users regarding the sensitivity and importance of this data. Educate them about best practices for data protection. AWS offers security training and certification programs, such as AWS Certified Security - Specialty, to raise security awareness among the team.

Mandatory training to be completed as part of the application access. All the stakeholders including the people who maintain the application must make sure they take the mandatory training.

1. ***Vulnerability Scanning and Assessment:***
   1. Regularly scan and assess the security of systems and applications handling user tax data and Chartered Accountants' information to identify vulnerabilities that could compromise these assets. Using AWS Inspector to perform vulnerability assessments on EC2 instances and applications running on AWS.
2. ***Security Controls:***
   1. Implement stringent security controls for the protection of user tax data and Chartered Accountants' details. This includes strong authentication, encryption of data in transit and at rest, and access restrictions. Implement AWS Security Hub to centralize security findings and automate continuous security monitoring and compliance checks.
3. ***Incident Response Plan:***
   1. Develop a specific incident response plan for user tax data and Chartered Accountants' information. Define roles and responsibilities for handling security incidents involving these assets. Utilizing AWS services like AWS CloudFormation, AWS Lambda, and Amazon CloudWatch for automating incident response actions and executing the incident response plan.
4. ***Security Governance:***
   1. Establish a governance framework specifically addressing the security of user tax data and Chartered Accountants' details. Ensure there is a clear chain of command and decision-making related to the protection of these assets. AWS provides best practices for governance and offers AWS Control Tower to set up and govern a secure, multi-account AWS environment.
5. ***Documentation and Record Keeping:***
   1. Maintain detailed records of activities related to user tax data and Chartered Accountants' information, including access logs, audit trails, and incident response reports. Using Amazon S3 to store and secure documentation related to security policies, risk assessments, and compliance efforts.
6. ***Security Education and Training:***
   1. Provide specialized security education and training programs for individuals who access or handle user tax data and Chartered Accountants' information. Ensure they are well-informed about data security and privacy best practices. AWS provides training resources and certification programs to educate your team on AWS security best practices.

***Legal and Regulatory Requirements (ID.AM-6)***

Taxare will identify and comply with applicable legal and regulatory requirements.

***Explanation:*** This control ensures that Taxare acknowledges and adheres to the legal and regulatory obligations relevant to its operations. In the context of Taxare, these may include:

***Data Privacy Laws:*** Taxare must comply with data privacy laws that protect the personal and financial information of users. This includes understanding and following the requirements of laws such as the General Data Protection Regulation (GDPR) in Europe, or specific state-level data privacy laws in the U.S.

***Tax Regulations:*** Given that Taxare is involved in tax-related services, there may be specific tax regulations and laws that it must adhere to. For example, it might need to ensure compliance with tax filing deadlines and specific tax laws that vary by jurisdiction.

***Industry-Specific Regulations:*** Depending on the nature of its services, Taxare might need to adhere to industry-specific regulations, such as those governing financial services or online marketplaces.

References:

- To identify and understand the legal and regulatory requirements, Taxare should consult legal experts specializing in tax, data privacy, and online services.

- Taxare can seek assistance and guidance from local resources, such as Small Business Development Centers, to start the process of understanding and complying with legal requirements.

- Taxare should stay informed about relevant legislation through resources like The National Conference of State Legislatures (NCSL) for comprehensive overviews of laws and regulations that affect online businesses.

***Roles and Responsibilities (ID.GV-3)***

***Action/Control:*** Assign specific roles and responsibilities for cybersecurity within Taxare.

***Explanation:*** This control ensures that responsibilities are clearly defined and assigned for effective cybersecurity management. In the context of Taxare:

***Business Owner/CEO:*** The CEO takes on the responsibility of providing the vision for cybersecurity efforts and is accountable for the organization's response to security incidents.

***Chief Information Security Officer (CISO) or Head of IT:*** The CISO is responsible for defining cybersecurity policies, directing preventive and response activities, user training, and regular exercises of the cybersecurity posture.

***Employee:*** Employees play a crucial role in maintaining cybersecurity. They are responsible for completing user training as defined by the CISO and following established cybersecurity policies and procedures.

References:

- Taxare can adapt existing roles and responsibilities from its business plans to fit the context of cybersecurity.

- The NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, can provide a starting point for defining roles and responsibilities in the field of cybersecurity.

- Taxare should align with NIST's Cybersecurity Framework, which provides a clear overview of the roles and responsibilities of business owners and employees in the context of cybersecurity.

**Protect**

The "Protect" aspect of the NIST framework involves implementing controls to safeguard an organization's assets and data. In the context of the TAXARE application, which handles tax data and personal information of users and chartered accountants, here are key controls that should be in place to address the cybersecurity plan:

1. ***Access Control:***
   1. Implement strong access control measures to ensure that only authorized individuals can access the application and sensitive data.
   2. Use Role-Based Access Control (RBAC) to manage permissions for users, administrators, and chartered accountants. Using AWS Identity and Access Management (IAM) to manage access to AWS resources. Assign least privileged access to users and services to limit exposure to sensitive data.
2. ***Data Encryption:***
3. Employ encryption for data both in transit and at rest. Utilize technologies like SSL/TLS for data in transit and encryption mechanisms for stored data. Enable encryption for data at rest and data in transit. Use AWS Key Management Service (KMS) to manage encryption keys. Use Amazon RDS Encryption to Encrypt sensitive data stored in Amazon RDS databases. Enable SSL/TLS for data in transit.
4. ***Authentication and Authorization:***
5. Implement strong user authentication mechanisms, including multifactor authentication (MFA) for enhanced security.
6. Ensure that users and chartered accountants have appropriate authorizations based on their roles and responsibilities. Using IAM Control user authentication and authorization for AWS resources. Using AWS Cognito for identity management and user authentication in the application
7. ***Data Loss Prevention:***
8. Implement data loss prevention (DLP) solutions to prevent unauthorized disclosure of sensitive data, including tax information and personal details. Utilizing AWS DLP services and third-party solutions to prevent unauthorized data disclosure.
9. ***Network Security:***
10. Protect the application's network by using firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to identify and respond to network threats. Using AWS Virtual Private Cloud to isolate resources and implement network security. Using AWS WAF and AWS Shield to Protect against DDoS attacks and web application vulnerabilities.
11. ***Application Security:***
12. Conduct regular security testing, including vulnerability scanning and penetration testing, to identify and address application-level vulnerabilities. Using AWS Inspector to Automate security assessments and vulnerability scanning. Using AWS Security Hub to Centralize security findings and threat detection across the AWS environment.
13. ***Security Patch Management:***
14. Develop a robust patch management process to keep the application, operating systems, and software up to date with security patches. Using AWS Systems Manager for patch management, compliance reporting, and automation
15. ***Security Awareness Training:***
16. Train employees, users, and chartered accountants to recognize and respond to security threats, such as phishing and social engineering attacks. Utilizing AWS Training and Certification for security awareness and skills development.
17. ***Secure Coding Practices:***
18. Ensure that developers follow secure coding practices when designing, developing, and maintaining the application to minimize security vulnerabilities. Using AWS Developer Tools to Implement development and deployment best practices with AWS CodePipeline, CodeBuild, and CodeDeploy.
19. ***Incident Response Plan:***
20. Have a well-defined incident response plan to effectively respond to security incidents. This includes procedures for reporting, containing, and recovering from security breaches. Using AWS Incident Response and AWS Security Hub to create and manage an incident response plan, leveraging AWS security tools and resources.
21. ***Backup and Recovery:***
22. Regularly back up critical data and system configurations to ensure data can be restored in the event of data loss or system failure. Using Amazon S3 to Store backups of critical data and system configurations securely. Using AWS Backup to automate and centralize backup management.
23. ***Data Retention Policies:***
24. Implement data retention and data disposal policies to manage the lifecycle of user and chartered accountant data securely. Using Amazon S3 Lifecycle Policies to set up data retention and data disposal policies in S3.
25. ***Privacy Controls:***
26. Comply with data protection regulations and industry standards related to user privacy and tax data, such as GDPR or HIPAA, by implementing necessary controls. Using AWS Compliance Programs to align with AWS's compliance programs to ensure privacy and regulatory compliance.
27. ***Third-Party Risk Management:***
28. Assess and manage the security risks associated with third-party services, including cloud providers or external software components used in the application. Using AWS Artifact to Access third-party compliance reports to assess the security of AWS services and AWS Marketplace to use trusted third-party security solutions available on the AWS Marketplace.
29. ***Secure Communication:***
30. Ensure that all communications, including user interactions and data transfers, are conducted securely through encryption and secure protocols. Using AWS PrivateLink to Establish private connections for secure communication between the application and AWS services. Using AWS Certificate Manager to Secure communication with SSL/TLS certificates.
31. ***Security Monitoring and Auditing:***
32. Implement continuous security monitoring to detect and respond to security events promptly. Utilize auditing and logging to maintain a record of security-related activities. Using AWS CloudTrail to Monitor and log security-related activities for auditing and compliance. Using Amazon CloudWatch to Set up alarms and monitoring for security events.

These controls collectively form the foundation of a comprehensive cybersecurity plan for the TAXARE application, helping to protect sensitive tax data, personal information, and overall system integrity from cyber threats. Regularly assess and update these controls to adapt to evolving security challenges and regulations.

***Account Management:***

***Action/Control***: Implement robust account management practices.

Explanation: Effective account management is essential to prevent unauthorized access and misuse of accounts. In the context of Taxare:

All employees and contractors shall have their own accounts: This ensures accountability and tracks individual actions on the system.

Normal, day-to-day accounts shall not be given administrator access: Restricting administrative access to only those who require it prevents accidental or intentional system-wide changes.

Accounts should be deleted, and credentials revoked when an employee leaves: This practice minimizes the risk of former employees retaining access to Taxare's systems.

Logging of usage shall be enabled for all accounts: This includes logging user and administrator logins, which is crucial for auditing and detecting misuse.

Account audits shall be conducted on a regular basis: Regular audits help identify any unauthorized or rogue accounts.

***References:***

- These practices align with the Center for Internet Security (CIS) Controls 4 and 16, which provide best practices for account management in the cybersecurity context.

- The NIST SP 800-181 offers guidelines on the roles and responsibilities for account management, which can be a helpful reference for Taxare.

***Authentication and Password Management***

***Action/Control:*** Implement secure authentication and password management practices.

***Explanation:*** Proper authentication and password management are critical for preventing unauthorized access to Taxare's systems and data. In the context of Taxare:

Employees and contractors shall enable authentication on all devices: This ensures that all devices connecting to Taxare's network require user authentication.

Enable multi-factor authentication (MFA) on sensitive accounts: MFA adds an additional layer of security, making it harder for unauthorized users to gain access.

Use a password manager for all Taxare accounts or services: Password managers promote the use of strong, unique passwords for each account.

Never use or reuse the same passphrase on two or more systems: Reusing passwords can be a security risk, as a breach in one system can lead to unauthorized access to others.

Never share Taxare accounts: Sharing accounts violates security policies and reduces accountability.

***References:***

- These practices align with the Center for Internet Security (CIS) Control 4, which discusses best practices for passwords.

- The NIST Interagency Report 7621 Revision 1 provides guidelines for using passwords and password managers.

- The Global Cyber Alliance's Cybersecurity Toolkit offers practical guidance on creating strong passwords, enabling MFA, and using password managers.

***Data Backups and Disposal***

***Action/Control:*** Establish data backup and disposal policies.

***Explanation:*** Data backups and disposal are essential components of protecting data. In the context of Taxare:

Employees and contractors shall enable automatic data backup on all devices: Automatic backups ensure that data is regularly and securely saved.

Critical data shall be backed up according to a “3-2-1” principle: This ensures that data is redundantly stored in different locations to minimize the risk of data loss.

Data, especially customer data, shall be retained and disposed of according to relevant laws: Compliance with laws like the Federal Trade Commission's (FTC) Disposal Rule ensures that customer data is handled appropriately.

References:

- These practices align with the Center for Internet Security (CIS) Control 10, which provides guidelines for data backup and recovery.

- The NIST Interagency Report 7621 Revision 1 offers guidance on data backup and recovery.

- The FTC's Disposal Rule provides information on how to comply with data disposal requirements.

***Vulnerability Management***

***Action/Control:*** Implement a vulnerability management plan.

***Explanation:*** Vulnerability management is essential to identify and address security weaknesses. In the context of Taxare:

Enable automatic updates on all devices that connect to Taxare’s network: This ensures that devices receive security updates promptly.

Install updates within 24 hours unless otherwise directed by the CISO of Taxare: Timely installation of updates reduces the risk of exploitation.

Not disable or interrupt automated vulnerability scanning: Regular vulnerability scanning helps detect potential security issues.

Coordinated Vulnerability Disclosure Policy: Establishing a VDP ensures that ethical hackers can responsibly report vulnerabilities, reducing the risk of exploitation and enhancing security.

References:

- These practices align with the Center for Internet Security (CIS) Controls 3 and 8, which provide best practices for vulnerability management.

- The NIST SP 800-161, Revision 2 offers guidance on creating an incident response

plan, including the Coordinated Vulnerability Disclosure Policy.

**Detect**

Achieving the "Detect" aspect of the NIST framework for the TAXARE application involves setting up mechanisms to identify and detect security incidents or anomalies in real-time. AWS provides several services and features that can assist in implementing effective detection controls. Here's how you can achieve this:

1. ***Log and Event Collection:***

Implement AWS CloudTrail to capture AWS API activity and AWS Config for tracking changes to AWS resources. These services provide a detailed audit trail of actions and configurations in your AWS environment.

1. ***Security Information and Event Management (SIEM):***

Utilize AWS Partner solutions or third-party SIEM platforms to centralize and analyze logs and events from various sources, including AWS services and application logs. AWS provides integration with popular SIEM tools.

1. ***Intrusion Detection and Prevention:***

Set up intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic and detect suspicious or malicious activities. AWS offers services like Amazon GuardDuty and VPC Flow Logs.

1. ***Security Automation:***

Use AWS Lambda for automated responses to detected events or incidents. Lambda can execute predefined scripts or actions in response to specific triggers or alerts from your detection systems.

1. ***Threat Intelligence Feeds:***

Subscribe to threat intelligence feeds and integrate them with your detection systems to stay updated on emerging threats and vulnerabilities.

1. ***Behavior Analytics:***

Implement behavior analytics solutions to detect anomalies in user behavior and system activities. AWS Partner solutions can help you achieve this.

1. ***Real-time Monitoring:***

Set up real-time monitoring with Amazon CloudWatch Alarms to detect specific threshold breaches or patterns indicative of security incidents.

1. ***Custom Alerts:***

Define custom alerts based on application-specific security events or scenarios. You can use CloudWatch Alarms and Simple Notification Service (SNS) for alerting.

1. ***Incident Detection Workflow:***

Develop an incident detection workflow that outlines how alerts and events are categorized, prioritized, and handled, including incident escalation and response procedures.

1. ***Machine Learning for Anomaly Detection:***

Explore AWS machine learning services like Amazon SageMaker for building custom anomaly detection models that can help identify unusual patterns and behaviors.

1. ***Security Analytics:***

Leverage AWS services like Amazon QuickSight for creating security analytics dashboards to visualize and analyze security-related data.

1. ***Regular Monitoring and Review:***

Continuously monitor and review detection rules, thresholds, and alerts to ensure they remain relevant and effective in identifying security incidents.

1. ***Incident Response Drills:***

Conduct incident response drills and tabletop exercises to test your detection and response capabilities. These drills help you identify weaknesses and areas for improvement.

1. ***External Threat Feeds:***

Integrate external threat intelligence feeds into your detection systems to stay updated on known threats and vulnerabilities.

1. ***Documentation and Reporting:***

Document detected incidents, the actions taken, and the lessons learned from each incident. Use these reports to improve your detection and response capabilities.

By implementing these measures and using AWS services such as CloudTrail, GuardDuty, CloudWatch, and Lambda, you can effectively achieve the "Detect" aspect of the NIST framework for the TAXARE application. It's essential to regularly review and update your detection mechanisms to stay ahead of evolving threats and vulnerabilities.

***Execution of the Vulnerability Management Plan***

***Action/Control***: Audit the execution of the vulnerability management plan.

***Explanation:*** Auditing the execution of the vulnerability management plan ensures that the plan is effectively implemented and that vulnerabilities are actively addressed. This is accomplished through tabletop and functional exercises that simulate potential vulnerabilities and responses.

**References:**

- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, provides information on conducting incident exercises.

**Respond:**

Respond principle of the NIST Cybersecurity Framework can be achieved in the context of the Taxare application.

1. ***Incident Response Plan on AWS:*** Develop a comprehensive incident response plan specific to the AWS environment. Document the roles and responsibilities of AWS users, including charted accountants, and outline the procedures for detecting, containing, and mitigating incidents.
2. ***Preparation on AWS***: Ensure AWS users, including the development and operations teams working on Taxare, are well-trained in AWS security best practices and incident response procedures. AWS provides training resources, such as AWS Security Certification courses, to help prepare your team.
3. ***Detection and Analysis on AWS***: Utilize AWS services like AWS CloudTrail for logging and AWS Config for configuration monitoring to detect unusual activities and changes in the AWS environment. Implement Amazon GuardDuty for threat detection and response.
4. ***Containment on AWS***: AWS Identity and Access Management (IAM) can be used to limit access during an incident. You can also employ AWS VPC (Virtual Private Cloud) and Security Groups to isolate affected resources and limit the incident's scope.
5. ***Eradication and Recovery on AWS:*** Use AWS backup and snapshot features for data recovery and Amazon Machine Images (AMIs) to rebuild affected instances. Ensure that all software and applications are updated with the latest patches.
6. ***Communication on AWS***: AWS provides communication tools like Amazon SNS (Simple Notification Service) and Amazon Chime for real-time incident communication. Develop communication plans to notify affected parties, including tax claimers and charted accountants.
7. ***Lessons Learned on AWS:*** After an incident, perform a thorough analysis using AWS CloudWatch Logs and Amazon S3 for log storage. Use AWS CloudFormation templates to replicate the infrastructure and test different incident response scenarios.
8. ***Documentation on AWS:*** AWS services like AWS CloudTrail and AWS Config automatically log and store activity data, which can serve as essential documentation for incident response. Use AWS CloudWatch Logs and Amazon S3 for centralized log storage.

References :

1. Amazon Web Services. (n.d.). AWS Identity and Access Management (IAM). <https://aws.amazon.com/iam/>
2. Amazon Web Services. (n.d.). AWS Security Best Practices. <https://aws.amazon.com/whitepapers/aws-security-best-practices/>
3. Amazon Web Services. (n.d.). AWS Well-Architected Framework - Security. <https://aws.amazon.com/architecture/well-architected/security/>
4. Amazon Web Services. (n.d.). AWS Incident Response. <https://aws.amazon.com/compliance/incident-response/>
5. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Retrieved from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
6. NIST Cybersecurity Framework - Respond. (n.d.). NIST. Retrieved from: <https://www.nist.gov/cyberframework/respond>
7. CERT Division, Software Engineering Institute, Carnegie Mellon University. (2017). Computer Security Incident Handling Guide. Retrieved from: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=669498>

**Recover**

The Recover principle in the NIST Cybersecurity Framework focuses on developing and implementing activities to restore services, minimize business impact, and prevent future incidents. In the context of the Taxare application, achieving the Recover principle involves creating a strategy to recover from cybersecurity incidents and minimize disruption to services. Here's how this can be achieved:

1. ***Backup and Data Recovery:*** Implement regular and automated backups of critical data and system configurations. Utilize AWS services like Amazon S3 for data storage and Amazon RDS for database backups. Ensure that data is backed up in a secure and geographically redundant manner to prevent data loss.
2. ***Redundancy and Failover:*** Design the Taxare application with redundancy in mind. Utilize AWS's high availability features such as Auto Scaling and Elastic Load Balancing to ensure that the application can continue to operate even if one component fails.
3. ***Incident Recovery Plan:*** Develop a comprehensive incident recovery plan specific to the Taxare application hosted on AWS. The plan should outline procedures for system recovery, data restoration, and service resumption. Test the plan periodically through tabletop exercises and real-world scenarios.
4. ***Patch and Configuration Management:*** Implement a robust system for patch management and configuration control. Regularly update and patch software components to address vulnerabilities. Utilize AWS Systems Manager for centralized patch management and compliance checks.
5. ***Incident Response Integration:*** Ensure that the incident response plan integrates with the recovery plan. This means that actions taken during incident response should feed into the recovery process, ensuring a smooth transition from incident containment to service restoration.
6. ***Testing and Validation:*** Regularly test the recovery plan through simulated exercises to validate its effectiveness. AWS provides services like AWS Disaster Recovery Testing to facilitate these tests and assess the readiness of recovery strategies.
7. ***Communication and Notification:*** Establish communication channels for notifying stakeholders, including tax claimers and charted accountants, about the recovery process. Timely and transparent communication is critical for maintaining trust.

**References:**

1. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Retrieved from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
2. Amazon Web Services. (n.d.). AWS Disaster Recovery. Retrieved from: <https://aws.amazon.com/disaster-recovery/>
3. Amazon Web Services. (n.d.). AWS Well-Architected Framework - Reliability. Retrieved from: <https://aws.amazon.com/architecture/well-architected/reliability/>
4. Amazon Web Services. (n.d.). AWS Systems Manager. Retrieved from: <https://aws.amazon.com/systems-manager/>

**Architecture and Services**

A screenshot of a computer

Description automatically generated

Please find the Architecture and Services document attached here.



**Cloud Services**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AWS Service | AWS Service Description | NIST Category | NIST Subcategory | Why did you include the service? | What purpose does it serve? |
| VPC | Virtual Private Cloud: Private network within AWS, divided into two Availability Zones. | Infrastructure | Network Architecture | For network separation and resource organization. | Provides a private space in AWS for resources, enhances security and segmentation. |
| Availability Zones | Zones within VPC to ensure high availability. | Infrastructure | Network Architecture | To ensure high availability. | Provides redundancy and ensures uptime in case one zone fails. |
| Public Subnet | Areas of VPC accessible from the internet. | Infrastructure | Network Architecture | For hosting resources like ALB that need internet access. | Allows resources to be accessed from the internet. |
| Private Subnet | Zones for resources that shouldn't be directly accessible from the internet. | Infrastructure | Network Architecture | For enhanced security and privacy. | Hosts resources that shouldn't be exposed to the internet like EC2 and RDS. |
| Route 53 | DNS service that routes users' requests. | Infrastructure | DNS | To manage DNS and route requests. | Directs traffic to appropriate AWS resources. |
| AWS Shield | Protection against DDoS attacks. | Security | Threat Protection | To protect architecture from DDoS attacks. | Provides DDoS protection. |
| AWS WAF | Web Application Firewall protects applications. | Security | Threat Protection | To protect from web threats. | Secures applications by filtering malicious web traffic. |
| AWS CloudFront | Content Delivery Network that accelerates content delivery. | Infrastructure | Content Delivery | For faster content delivery. | Accelerates delivery of websites, APIs, and content to users. |
| ALB | Application Load Balancer: Distributes incoming application traffic across multiple targets. | Infrastructure | Load Balancing | To manage web traffic distribution and ensure high availability. | Distributes incoming application traffic for better load management. |
| EC2 Instances | Virtual servers in AWS. | Compute | Server | To run the application. | Provides compute resources to run applications. |
| RDS Databases | Relational Database Service: Managed relational database service. | Storage | Database | For structured data storage and management. | Provides a managed relational database environment. |
| AWS S3 Buckets | Scalable storage service. | Storage | Object Storage | For scalable data storage. | Offers a place to store and retrieve any amount of data at any time. |
| Cognito | Provides user authentication and identity services. | Security | Identity and Access | For user management and authentication. | Allows secure access to the application and manages user identities. |
| Security Groups | Virtual firewalls for instances to control inbound and outbound traffic. | Security | Firewall | To protect against unauthorized access. | Regulates inbound and outbound traffic to instances. |
| CloudWatch | Monitors AWS resources and applications, providing metrics and logs. | Monitoring | Performance Monitoring | For monitoring and alarms. | Collects and tracks metrics, collects and monitors log files, and sets alarms. |
| CloudTrail | Logs all AWS activity. | Monitoring | Auditing | For tracking AWS activity and ensuring compliance. | Provides event history of AWS account activity for security analysis and auditing. |
| GuardDuty | Continuous security monitoring service. | Security | Threat Detection | To scan for suspicious activity. | Analyzes and monitors VPC flow logs, AWS CloudTrail event logs, and DNS logs. |
| IAM | Identity and Access Management: Controls permissions in AWS environment. | Security | Identity and Access | To ensure proper access control and manage permissions. | Allows management of users and their access to AWS resources. |
| AWS CloudFormation | Provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. | Infrastructure | Infrastructure As Code | For automating infrastructure provisioning and management. | Allows creation of a collection of related AWS resources and provision them in an orderly and predictable fashion. |
| AWS Trusted Advisor | Analyzes your AWS environment and compares it against best practices, providing recommendations to save costs, boost performance, or close security gaps. | Monitoring | Best Practices | For insights on AWS best practices. | Assists in optimizing AWS resources, cutting costs, increasing performance, and improving security. |
| AWS Config | Provides resource inventory, configuration history, and configuration change notifications to enable security and governance. | Monitoring | Configuration Management | For tracking resource configurations and changes. | Gives a detailed view of the configuration attributes of AWS resources and can evaluate configurations for desired settings. |

**References:**

1. Overview of Amazon Web Services. (2019). <https://d1.awsstatic.com/whitepapers/aws-overview.pdf>

**Summary**

1. ***Summary of the Plan:***  
   The "Taxare Application Cybersecurity Plan" is a comprehensive strategy that underscores the organization's commitment to enhancing its security infrastructure. The plan is designed to safeguard the organization from an array of cyber threats, protect sensitive data, uphold the operational integrity, and instill unwavering confidence among clients, partners, and stakeholders. Various facets of the plan encompass backup and recovery, data retention policies, privacy controls, and third-party risk management.
2. ***Strategy for Implementation:***  
   To implement the cybersecurity plan, the organization heavily leverages Amazon Web Services (AWS) solutions. Key strategies include regular backups of crucial data using Amazon S3, centralized backup management with AWS Backup, and enforcing data retention and disposal policies using Amazon S3 Lifecycle Policies. Furthermore, the organization adheres to essential data protection regulations like GDPR and HIPAA, with the support of AWS Compliance Programs, and manages third-party risks through AWS Artifact and AWS Marketplace.
3. ***Evolution of the Plan:***  
   While the specific details about how the plan will evolve with the changing business environment were not overtly mentioned in the sections reviewed, a robust cybersecurity plan like this typically evolves by continually assessing emerging threats, updating technologies, and refining strategies. The use of AWS tools suggests a flexible approach, where new services and features can be integrated as AWS evolves and as the organization's needs change.
4. ***Next Steps:***  
   The document culminates with references, pointing to the reliance on established sources to inform the plan. The immediate next steps, though not explicitly detailed, could involve a thorough review of the current security posture, ongoing monitoring, regular updates to the plan based on feedback and changing threat landscapes, and continuous training and awareness programs for staff.