SUTHERLAND®

How-to Guide

INSUFFICIENT SHIELDS: ADDRESSING CYBERSECURITY FLAWS IN INSURANCE TPA

Carriers can't risk cybersecurity breaches and the serious consequences that accompany them. Learn how a Digital TPA can protect your data and operations with confidence.

Digital TPA: The Key to **Compliant Data Security**

On 2 November 2023, a cybersecurity incident at a global TPA brought multiple national retirement and insurance provider platforms to a grinding halt. Most Insureds and Participants couldn't access their accounts until the week of November 27. Even then, it took more than a month to bring systems fully back to normal.

Cybersecurity breaches take many forms: ransomware attacks, including phishing attacks, and distributed denial-of-service (DDoS) attacks - when business operations go down, and at the same time, members can't access their accounts digitally. Even after restoration, TPA platforms require weeks of catch-up cycles to be up-to-date and current.

Unsurprisingly, cybersecurity breaches come with severe consequences, including financial losses, reputation damage, legal penalties, and diminished customer trust.

A ROBUST AND SECURE TPA PLATFORM: NO LONGER A NICE TO HAVE

In today's fast-evolving insurance technology landscape, Business Process as a Service (BPaaS) solutions provide insurers with flexibility, scalability, and efficiency, enabling insurers to streamline their operations and deliver superior customer experiences. But in this digital era, having a secured Third-Party Administration (TPA) platform for BPaaS solutions is crucial to protect sensitive information and maintain regulatory compliance.

According to the guidelines set forth by the Department of Labor (DOL), all fiduciaries responsible for plans (including TPAs) are obligated to mitigate cybersecurity risks effectively. The Employee Benefits Security Administration (EBSA) has developed the following best practices for use by recordkeepers and other service providers managing plan-related IT systems and data. These guidelines also assist TPAs in making informed decisions regarding the selection of service providers[1]:

Operational Considerations	Technological Considerations
Have a formal, well-documented cybersecurity program.	Have strong access control procedures.
Ensure any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.	Implement and manage a secure system development life cycle (SDLC) program.
Have a reliable annual third-party audit of security controls.	Conduct prudent annual risk assessments.
Clearly define and assign information security roles and responsibilities.	Encrypt sensitive data, stored and in transit.
Conduct periodic cybersecurity awareness training.	Implement strong technical controls in accordance with best security practices.
Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.	Appropriately respond to any past cybersecurity incidents.

This whitepaper will explore the essential factors and optimal methodologies for constructing a resilient and secure TPA platform tailored for BPaaS solutions within the life and annuity insurance domain.

[1] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

Table of Contents

A New Framework for Keeping Your **Operations Secure**

Before diving into the specifics of building a secure TPA platform, it's crucial to grasp the unique hurdles and prerequisites of the life and annuity insurance sector.

Life and annuity products handle vast amounts of personal and financial data, including policyholder information, beneficiary details, and transaction records. Moreover, insurers must comply with rigorous regulatory mandates such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) to uphold the security and privacy of customer data. Additionally, adherence to PCI DSS standards for card-related payments is imperative.

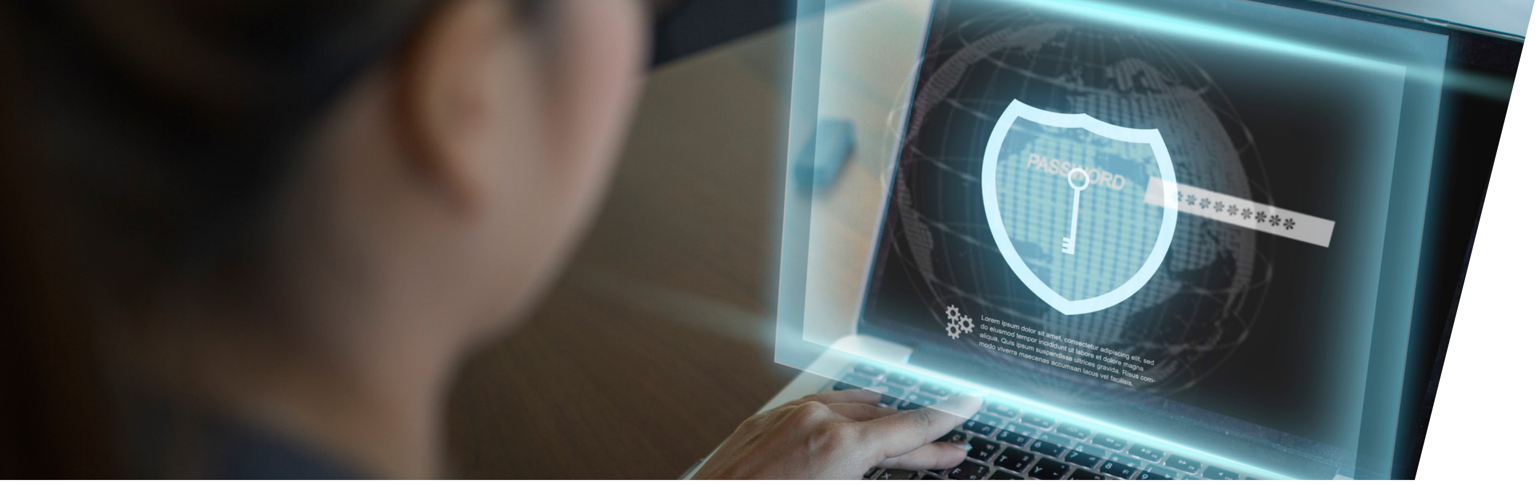
This is a complex operating environment with many moving parts. L&A carriers, therefore, need a TPA that not only delivers on cybersecurity but does so with a keen understanding and application of relevant regulations.

KEY CONSIDERATIONS FOR TPA SECURITY

Carriers today need a TPA with a security framework that encompasses multiple layers and various components and practices designed to protect data, applications, and infrastructure in cloud environments. Here are some key guiding principles for TPA platform security architecture[2]:

- **Strong Identity Foundation.** Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize identity management and aim to eliminate reliance on long-term static credentials.
- **Enable Traceability.** Monitor, generate alerts, and audit actions in real time. Integrate log and metric collection with systems to automatically investigate and take necessary action.
- **Security at all Layers.** Apply a defense-in-depth approach with multiple types of controls to all layers, including edge of network, virtual private cloud (VPC), load balancing, instance and compute services, operating system, application configuration, and code.
- **Automated Best Practices.** Automated, software-based security mechanisms improve your ability to scale rapidly, securely, and cost-effectively. Create secure architectures and implement controls that are defined and managed in version-controlled templates.
- **Protect Data in Transit and at Rest.** Classify your data into sensitivity levels and use mechanisms such as encryption, tokenization, and access control where appropriate.
- **Reduce Manual Intervention.** Use mechanisms and tools to reduce or eliminate the need to access or manually process data directly. This reduces the risk of mishandling or modification and human error when handling sensitive data.
- **Prepare for Security Events.** Prepare for incidents through incident management and investigation policies and processes that align with your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

[2] https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/foundations.html



The Way Forward: **A Multi-layer Security Architecture**

Knowing what to look for in a TPA is one thing, but understanding the ins and outs of security architecture is another. Here are some of the key components you should look for in a TPA's security architecture:

NETWORK SECURITY

- Segmentation of network resources using virtual private clouds (VPCs), subnets, and security groups.
- Network monitoring and intrusion detection/prevention systems (IDS/IPS) to detect and respond to suspicious activities.

IDENTITY AND ACCESS MANAGEMENT (IAM)

- Centralized management of user identities, roles, and permissions.
- Multi-factor authentication (MFA) for added security.
- Role-based access control (RBAC) to enforce the principle of least privilege.

APPLICATION SECURITY

- Secure coding practices to prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and insecure deserialization.
- Regular security testing, including static code analysis (SAST), dynamic application security testing (DAST), and penetration testing.

DATA SECURITY AND ENCRYPTION

- Encryption of data at rest and in transit using strong cryptographic algorithms.
- Key management to securely generate, store, and rotate encryption keys.

LOGGING AND MONITORING

- Centralized logging of events and activities for auditing and forensic analysis.
- Real-time monitoring of system metrics, logs, and user activities for detecting and responding to security incidents.

COMPLIANCE AND GOVERNANCE

- Adherence to industry-specific regulations (PCI, HIPAA) and compliance standards (e.g. SOC 2, ISO 27001).
- Regular audits and assessments to validate compliance and identify areas for improvement.

SECURITY AUTOMATION AND ORCHESTRATION

- Integration of security tools and processes into automated workflows for rapid response and remediation.
- Continuous security monitoring and automated incident response to reduce manual intervention and improve efficiency.

EMPLOYEE TRAINING AND AWARENESS

- Regular training programs to educate employees about security best practices, phishing awareness, and the importance of data protection.

The Sutherland TPA security framework encompasses multiple layers and various components and practices designed to protect data, applications, and infrastructure in cloud environments

/ **VPC, VPN gateway, Private/Public Subnets,** Unique Security Groups for each resource.

/ **AWS Shield** is utilized for DDoS protection, and **AWS WAF** for Web APP and APIs.

/ **VPC Endpoints** leveraged for images access.

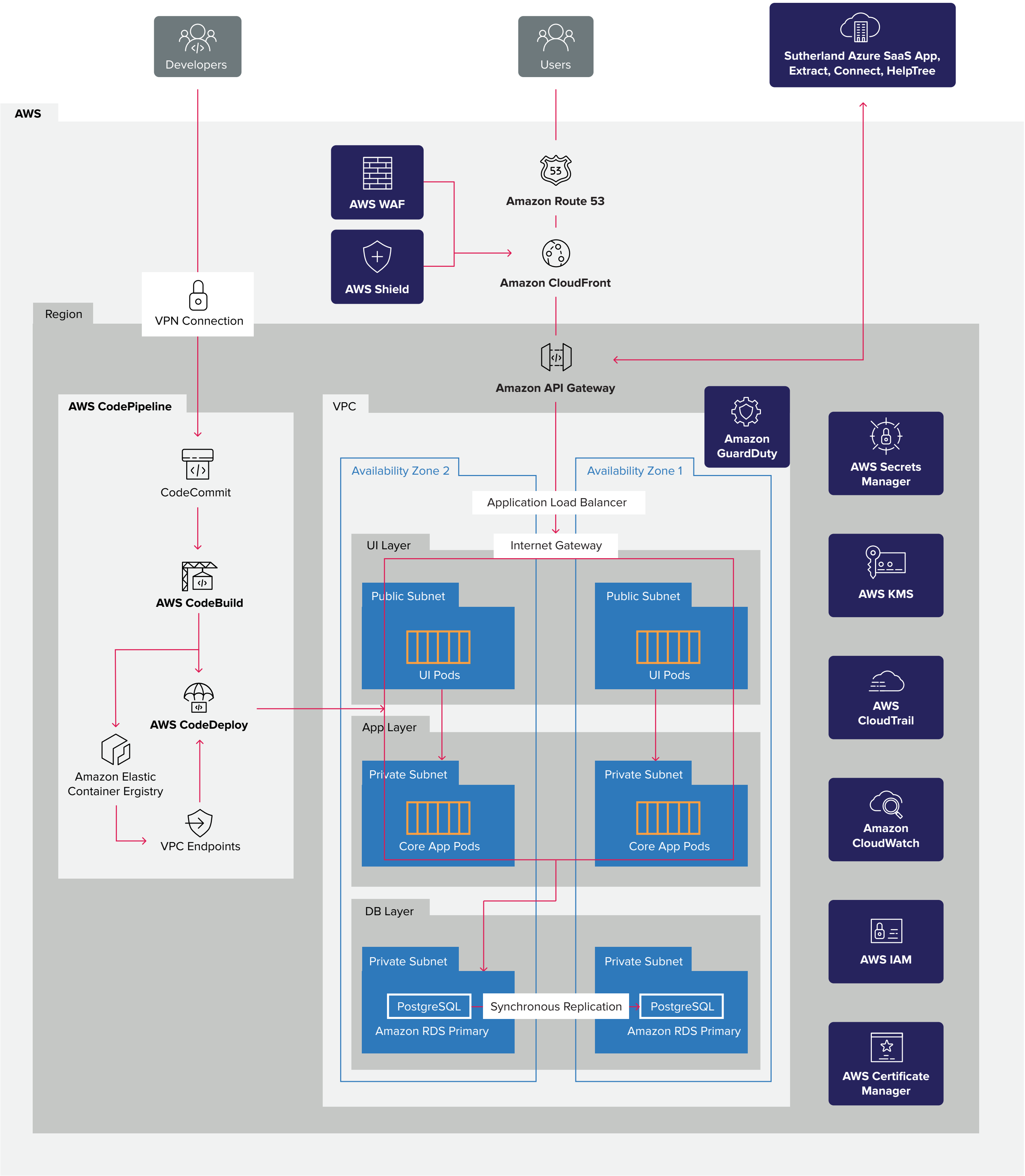
/ All the UI components (Aura and NewGen) internet-facing and will be deployed on a **public subnet.**

/ The App layer and DB layer to be hosted on **private subnets.**

/ All the **Docker images** to be stored in a private repository using AWS ECR within Sutherland cloud infrastructure.

/ **AWS Certificate Manager, Secrets Manager, and KMS** leveraged fully for application security and Data encryption.

SUTHERLAND TPA SECURITY FRAMEWORK



Disaster Recovery Planning and Implementation

Sutherland TPA-EDGE has high availability with robust Disaster Recovery leveraging Active-Active sync using AWS native services. This ensures that any data loss is limited to one to four hours and that entire systems are backed up in four to eight hours. In case both primary and DR sites are under attack, system restoration from backup files is done within 24 hours.

Our core platform has 24x7 online availability with behind-the-scenes on-demand batch capabilities, enabling multiple catch-up cycles to be run throughout the day.

Cloud DR Strategy	Sutherland TPA Solution
Primary Site	US East Data center leveraging all 3 Availability Zone
DR Site	US West Data center leveraging all 3 Availability Zone
RTO	4 - 8 Hrs
RPO	4 - 8 Hrs
Availability	99.99%

ENSURING CONTINUOUS OPERATIONS AND KEEPING YOU ONLINE, ALWAYS

Sutherland has a fully documented continuity of business disaster recovery (COB DR) plan in place that adheres to the internationally recognized NFPA1600 standard. The standard recovery time objective (RTO) is 25% of seats in 72 hours or less.

We perform at least one test annually for each program and use our facilities as alternate disaster recovery sites. Sutherland boasts over 60 facilities in 17 countries that are used as alternate business recovery sites and have a 4 phased approach to crisis management, including disaster recovery.

Key Security Practices for Implementation

SECURE DEVELOPMENT PRACTICES

- Follow secure coding practices and guidelines to minimize vulnerabilities in the TPA platform's codebase.
- Conduct regular code reviews and security testing throughout the development lifecycle to identify and address security issues early.
- Follow best-in-class SAST and DAST methodology and tools.

VENDOR MANAGEMENT AND DUE DILIGENCE

- Perform thorough due diligence when selecting third-party vendors and service providers for hosting, infrastructure, and security services.
- Ensure vendors adhere to industry-standard security practices and have appropriate certifications and compliance measures in place.

EMPLOYEE TRAINING AND AWARENESS

- Provide comprehensive security awareness training to employees to educate them about security best practices, phishing threats, and data protection policies.
- Foster a culture of security awareness and vigilance among employees to mitigate the risk of insider threats and social engineering attacks.

INCIDENT RESPONSE AND REMEDIATION

- Develop a comprehensive incident response plan outlining procedures for detecting, analyzing, and mitigating security incidents.
- Establish clear escalation paths and responsibilities to facilitate timely response and remediation of security incidents.

Keep Your Insurance Operations Safe With **Sutherland TPA-EDGE**

Crafting a secure TPA platform for BPaaS solutions in life and annuity products demands a proactive, multi-layered cybersecurity approach.

By integrating stringent security measures, following industry standards, and remaining vigilant against evolving threats, insurers establish a resilient, compliant, and trustworthy platform.

In today's digital era, prioritizing security isn't merely obligatory; it's a strategic necessity to instill confidence and trust among policyholders and stakeholders.

Explore how Sutherland TPA EDGE can keep your data and operations secure in the digital era.

We make digital
human™

sutherlandglobal.com
sales@sutherlandglobal.com
1.585.498.2042

Sutherland is an experience-led digital transformation company.

Our mission is to deliver exceptionally designed and engineered experiences for customers and employees. For over 35 years, we have cared for our client's customers, delivering measurable results and accelerating growth. Our proprietary, AI-based products and platforms are built using robust IP and automation. We are a team of global professionals, operationally effective, culturally meshed, and committed to our clients and to one another.

We call it One Sutherland.

SUTHERLAND®