A10 TSA Compliance Solution Check List

Ensure the vendors you're evaluating have the critical capabilities that your organisation requires to help meet TSA compliance demands

	Vendors:				
Security Compliance Support: How effective is this solution at helping you to meet the following requirements?					
Detect threats via analytics and intrusion detection					
Mitigate risks with filtering, load balancing, and threat protection					
Enhance incident response through logging and SIEM integration					
Provide API and web application detection for threat defence					
Ensure compliance with TSA Sections 105A and 105B and enable proactive cyber threat management					
Responding to Security Compromise: Does the solution support threat mitigation capabilities?					
Multi-vector DDoS detection and mitigation at both infrastructure and application layers					
Identify zero-day threats					
Undertake behavioural analysis					
Provide AI-driven baselining, or real-time anomaly detection					
Automate policy escalation					
Distinguish between legitimate traffic and attack traffic					
Provide API and web application protection					
Integrate with SIEM and SOAR platforms					
Generate actionable insights for rapid response and post-incident analysis					
Help you meet TSA Section 2 105C–105D requirements for service availability and threat resilience. Enable compliance with CoP (Section 5) regulation 6					

A10 TSA Compliance Solution Check List

	Vendors:				
Network Oversight and Architecture: Does the solution secure network architecture and ensure service continuity?					
Enable zone segmentation to limit incident impact					
Enforce management control with MFA and encryption					
Protect oversight functions: load balancing and traffic steering					
Deliver automated failover, redundancy and smart load distribution					
Help you meet TSA CoP sections 2 and 8					
Supply Chain and Third-party Control: Does the solution adhere to best practices?					
Ensure software integrity, secure updates and vulnerability management					
Provide signed firmware, regular patches, hardening guides					
Support testing protocols to ensure equipment integrity, resilience and operational readiness					
Support compliance with TSA CoP Sections 11 and 13 and regulations 7 to 9					
Protection of Data and Functions: Does the solution help protect data and critical functions in your network?					
Ensure encrypted traffic inspection					
Deliver robust access control and secure communications					
Enable role-based access					
Secure administration, user activity logging					
Integrate with identity management and MFA systems					
Has an available TSA Security Declaration					