letsbloom

01

CLOUD SECURITY CONTROLS FRAMEWORK

DATA PRIVACY STANDARDS

- GDPR
- GLBA
- CCPA
- NIST Cloud Controls
- SANS Controls
- ENISA Standards
- CSA Controls Matrix
- CIS Benchmarks
- Singapore Privacy Considerations

PAYMENT STANDARDS

- PCI Standards
- Card Holder Data (CHD) Standards
- DSS 3.2
- Tokenization Security

BANKING POLICIES

- ACMG (Access Controls)
- Payment Card Data Management
- Data Loss Protection

PII* STANDARDS

- NIST SP 800-53, Rev. 5
- NIST SP 800-122

*Personal Identifiable Information

CONTROL OBJECTIVES

- Compliance and VM
- Cloud Services
- Information Classification
- Information Handling
- Network Security
- Management Security
- Logging and Monitoring

RISK MANAGEMENT | SECURE SOFTWARE DEVELOPMENT | SERVICE MANAGEMENT | RESILIENCE | AUDIT

IDENTITY & ACCESS MANAGEMENT | INFRASTRUCTURE & DATA SECURITY | CRYPTOGRAPHY | SECURITY ASSESSMENT | SECURITY OPERATIONS

letsbloom

PaaS SECURITY AND COMPLIANCE

CLOUD SECURITY REFERENCE ARCHITECTURE

GOVERNANCE & RISK MANAGEMENT

- STRATEGY
- POLICY & PROCEDURES
- TRAINING & COMMUNICATIONS
- SERVICE LEVEL AGREEMENTS
- REGULATORY COMPLIANCE
- INDUSTRY STANDARDS

1 INFRASTRUCTURE SECURITY	Core host and network
2 THREATS & VULNERABILITIES	Threat intelligence drives vulnerability and patch management
3 APPLICATION SECURITY	Across development lifecycle orchestrated through CI/CD pipeline
4 IDENTITY & ACCESS	Define and manage identities and their access, entitlements to cloud resources
5 DATA PROTECTION	For data-at-rest | data-in-transit | data-in-use | Through technology and process
6 LOGGING & MONITORING	Log and monitor to identify security events and provide incident response
7 INCIDENT RESPONSE	Proactive threat hunting and incident response orchestration to manage the security posture

letsbloom

PaaS SECURITY AND COMPLIANCE

1000+ SECURITY CONTROLS

INFRASTRUCTURE SECURITY

OS Hardening
Patch Management
Backup and Recovery Management
Configuration Management
Intrusion Detection and Prevention
Network segmentation/isolation
Firewalls and Ingress / Egress Security

DATA PROTECTION

Data-in-transit Encryption
Data-at-Rest Encryption (S3 buckets, DB, Blob)
Network isolation of sensitive data
Tokenization
Data Exfil Detective Controls
Data /input/output segregation
Valet key/temporary access tokens

APPLICATION SECURITY

Secure Code Review
Vulnerability Assessment and Remediation
(D)DoS protection
TLS Enforcement
Web Application Firewall
OWASP Top 10 and SANS Top 25 CWE Mitigation

IDENTITY & ACCESS

Role-based Access Control
Least Privilege Principle
Fine grained Entitlement Management
On-demand Privilege Access Provisioning
Access Controls for Data Stores (S3, DB, Blob)
- Object Lock
- Secure Access to resources

LOGGING & MONITORING

Network (Flow) Log Monitoring
Cloud Trail Log Monitoring
Data Store Access Log Monitoring
Cloud Watch Alarms
Config Alarms

INCIDENT RESPONSE

Incident Response
Incident Management
Response Orchestration
IOC (Indicators-of-Compromise) Checks

THREATS & VULNERABILITIES

OS and Container Vulnerability Assessment
OS and Container Security Patching
Remediation Tracking
Threat Intelligence Feeds
Threat Modelling

PaaS SECURITY AND COMPLIANCE

REGULATORY COMPLIANCE

To provide security of the platform, letsbloom implements continuously enforced security controls to demonstrate, validate and monitor that letsbloom can operate under several compliance standards and industry certifications. Following are the generally accepted regulatory control objective domains. Letsbloom implements controls across these domains to ensure compliance.

RISK MANAGEMENT

Letsbloom has established effective risk management frameworks to manage technology risks and to ensure confidentiality, integrity and availability of the platform.

Risks are identified, assessed, and treated periodically and are continuously monitored and reported.

SECURE SOFTWARE DEVELOPMENT

Letsbloom follows agile development methodology with Dev Sec Ops practices and security-by-design principles to ensure platform security.

Letsbloom processes ensure a systematic approach to Threat Modeling, Security Design and Code Reviews, Vulnerability and Penetration testing throughout the lifecycle.

SERVICE MANAGEMENT

Letsbloom implements a robust IT service management framework to support effective operations, asset tracking, change and incident management.

Framework supports Configuration, Patch, Change and Release Management processes and ensures effective incident reporting and response.

RESILIENCE

Letsbloom platform's architecture was designed with principles of IT resiliency to ensure system availability, recoverability with effective backup and recovery.

Platform's disaster recovery and business continuity requirements are built to support RTO and RPO as per supported SLAs.

AUDIT

Letsbloom has identified a comprehensive set of auditable areas for technology risk and ensures that a periodic audit is performed.

Audit frequency is commensurate with the criticality and risk of supported services and performed by accredited personnel.

IDENTITY & ACCESS MANAGEMENT

Letsbloom implements robust identify verification and establishment processes and is fully access controlled.

Letsbloom access controls are designed using principles of 'least privilege', 'segregation of duties', multi-factor authentication and 'just-in-time' privileged access provisioning to ensure effective security.

INFRASTRUCTURE & DATA SECURITY

Letsbloom secures against unauthorized access, modification, copying, or transmission of confidential data at-rest, in-transit and in-use.

Platform also implements and continuously enforces robust network and infrastructure security to protect against common attack vectors such as DDoS, MITMA, malware and spoofing attacks.

CRYPTOGRAPHY

Letsbloom platform has robust cryptography to protect data-at-rest and data-in-transit which uses well-established standard algorithms with appropriate key strength.

Platform implements an effective automated key management policy, standards and procedures.

SECURITY ASSESSMENT

Letsbloom conducts regular vulnerability assessments for operating systems, databases and platform components to identify, track and remediate risks.

Platform also conducts periodic penetration testing and cyber exercises to obtain an in-depth evaluation of its cyber security defenses and test the response and recovery procedures.

SECURITY OPERATIONS

Letsbloom has implemented a robust incident response process for prompt detection and response to cyber incidents. Platform has comprehensive security logging and monitoring implemented.

Letsbloom has defined processes to collect, process, review and retain security logs and defined roles and responsibilities for security operations.