Identifying Minimum Acceptable Risk and Security Baseline Definitions

Seven Domains of IT Infrastructure

Information Security Management Framework

Agenda

1. Introduction to Risk Management & Security Baselines
2. The Seven Domains Framework
3. Domain 1: User Domain
4. Domain 2: Workstation Domain
5. Domain 3: LAN Domain
6. Domain 4: LAN-to-WAN Domain

Introduction: Risk vs Security Baselines

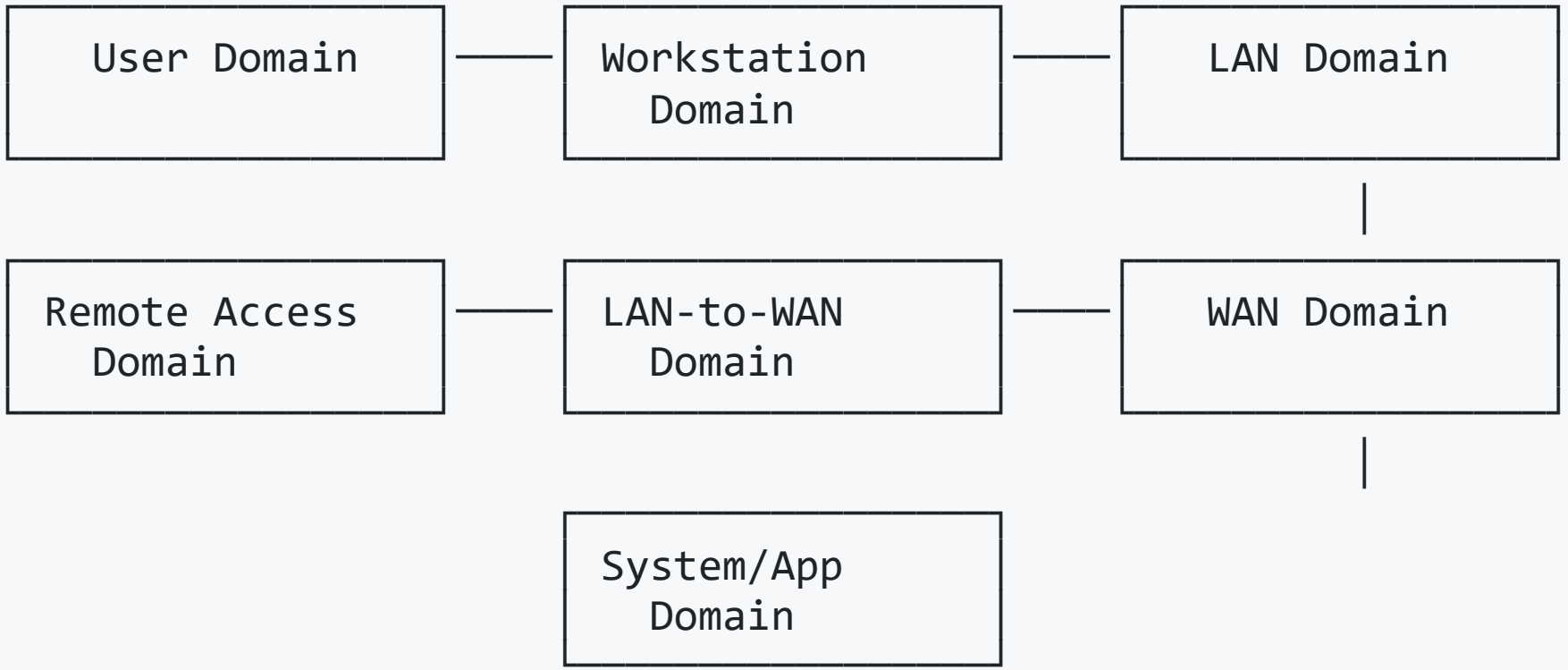
Minimum Acceptable Risk Level

- **Definition**: The lowest level of risk an organization can tolerate while maintaining operational effectiveness
- **Factors**: Business objectives, regulatory requirements, cost-benefit analysis
- **Measurement**: Quantitative (ALE, ROI) and Qualitative (High/Medium/Low)

Security Baseline

- **Definition**: Minimum security standards and controls required across all IT domains
- **Purpose**: Establish consistent security posture
- **Components**: Policies, procedures, technical controls, monitoring

The Seven Domains Framework



Domain 1: User Domain

Risk Profile

- **High Risk Areas**: Social engineering, weak passwords, insider threats
- **Impact**: Data breaches, unauthorized access, compliance violations

Security Baseline Requirements

- **Authentication**: Multi-factor authentication mandatory
- **Training**: Annual security awareness training (minimum 4 hours)
- **Access Controls**: Role-based access, principle of least privilege
- **Monitoring**: User activity logging and behavioral analytics

Domain 1: User Domain - Case Study

Case: Healthcare Provider - HIPAA Compliance

Scenario: 500-employee hospital system
Risk: PHI exposure through user negligence

Baseline Implementation:

- Mandatory MFA for all systems accessing PHI
- Quarterly phishing simulation testing
- Role-based access to patient records
- Annual HIPAA training with competency testing

Results:

- 85% reduction in successful phishing attempts
- Zero PHI breaches in 18 months
- 100% compliance audit score

Domain 2: Workstation Domain

Risk Profile

- **High Risk Areas**: Malware infection, data theft, unauthorized software
- **Impact**: System compromise, data loss, network propagation

Security Baseline Requirements

- **Endpoint Protection**: Enterprise-grade antivirus with real-time scanning
- **OS Management**: Automated patching within 72 hours of release
- **Data Protection**: Full disk encryption (AES-256 minimum)
- **Application Control**: Whitelisting for approved software only

Domain 2: Workstation Domain - Example

Financial Services Firm Implementation

Environment: 200 Windows 10/11 workstations

Minimum Acceptable Risk: <5% infection rate, <24hr containment

Baseline Controls:

```
Antivirus: CrowdStrike Falcon
Encryption: BitLocker with TPM 2.0
Patching: WSUS automated deployment
App Control: Windows Defender Application Control
Backup: Daily incremental, weekly full
Monitoring: Sysmon + SIEM integration
```

KPIs: 99.5% patch compliance, 0% successful malware execution

Domain 3: LAN Domain

Risk Profile

- **High Risk Areas**: Network segmentation failures, lateral movement, data interception
- **Impact**: Network-wide compromise, data exfiltration

Security Baseline Requirements

- **Network Segmentation**: VLANs for different user groups/functions
- **Access Control**: 802.1X authentication for all connections
- **Monitoring**: Network traffic analysis and anomaly detection
- **Encryption**: WPA3 for wireless, TLS 1.3 for internal communications

Domain 3: LAN Domain - Case Study

Manufacturing Company Network Security

Challenge: Operational Technology (OT) and IT convergence
Risk Level: Critical production system availability

Baseline Architecture:

- **Segmentation**: Separate VLANs for IT, OT, Guest, BYOD
- **Firewalls**: Next-generation firewalls between segments
- **Monitoring**: Industrial control system monitoring
- **Backup Networks**: Redundant paths for critical systems

Outcome: Zero production downtime from cyber incidents, 40% reduction in network-related security events

Domain 4: LAN-to-WAN Domain

Risk Profile

- **High Risk Areas**: Firewall bypass, DDoS attacks, data exfiltration
- **Impact**: External threats penetrating internal network

Security Baseline Requirements

- **Perimeter Defense**: Next-generation firewall with IPS
- **Traffic Inspection**: Deep packet inspection for all traffic
- **Redundancy**: Dual internet connections with failover
- **Monitoring**: 24/7 SOC monitoring of perimeter events

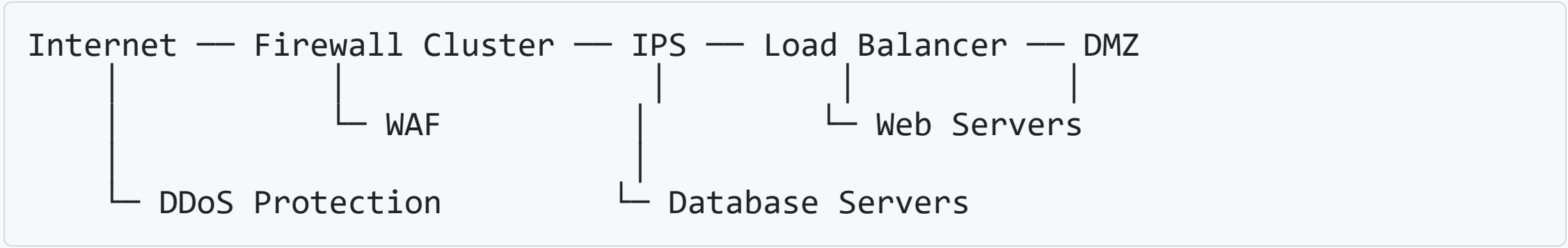
Domain 4: LAN-to-WAN - Implementation Example

E-commerce Platform Security

Traffic Volume: 10Gbps peak, 50,000 concurrent sessions

Risk Tolerance: 99.9% availability, <1% false positive rate

Technical Implementation:



Metrics: 99.95% uptime, blocked 15M malicious requests/month

Domain 5: Remote Access Domain

Risk Profile

- **High Risk Areas**: VPN vulnerabilities, unsecured endpoints, data leakage
- **Impact**: Unauthorized network access, data breaches

Security Baseline Requirements

- **VPN Security**: IPSec or SSL VPN with certificate authentication
- **Endpoint Compliance**: Device health checks before connection
- **Data Protection**: DLP policies for remote data access
- **Session Management**: Automatic timeout and re-authentication

Domain 5: Remote Access - Case Study

Law Firm Remote Work Security

Challenge: COVID-19 remote work transition for 150 attorneys
Compliance: Attorney-client privilege protection

Zero Trust Implementation:

- **Identity Verification**: MFA + device certificates
- **Network Access**: Micro-segmentation based on role
- **Data Protection**: Document watermarking and access logging
- **Monitoring**: User and entity behavior analytics (UEBA)

Results: Maintained confidentiality standards, enabled 100% remote work capability

Domain 6: WAN Domain

Risk Profile

- **High Risk Areas**: Data interception, service provider vulnerabilities, connection failures
- **Impact**: Business continuity disruption, data exposure

Security Baseline Requirements

- **Encryption**: End-to-end encryption for all WAN traffic
- **Redundancy**: Multiple service providers and connection types
- **SLA Management**: Defined uptime and response requirements
- **Monitoring**: Real-time performance and security monitoring

Domain 6: WAN Domain - Example

Multi-Site Retail Chain

Infrastructure: 50 retail locations + 2 data centers
Requirements: 99.5% uptime, PCI DSS compliance

WAN Security Design:

- **Primary**: MPLS network with end-to-end encryption
- **Secondary**: Internet-based SD-WAN with IPSec tunnels
- **Backup**: 4G/5G cellular connections for failover
- **Monitoring**: Centralized network operations center (NOC)

Performance: 99.7% average uptime, sub-100ms latency between sites

Domain 7: System/Application Domain

Risk Profile

- **High Risk Areas**: Application vulnerabilities, database breaches, privilege escalation
- **Impact**: Data theft, service disruption, compliance violations

Security Baseline Requirements

- **Secure Development**: SAST/DAST testing in CI/CD pipeline
- **Access Controls**: Database-level encryption and access logging
- **Vulnerability Management**: Regular penetration testing and remediation
- **Backup & Recovery**: Tested disaster recovery procedures

Domain 7: System/Application - Case Study

SaaS Platform Security Implementation

Application: Customer relationship management system
Users: 10,000+ across multiple tenants

Security Architecture:

```
Application Layer:
  - Input validation and sanitization
  - Session management with tokens
  - API rate limiting and throttling

Database Layer:
  - Transparent data encryption (TDE)
  - Column-level encryption for PII
  - Database activity monitoring (DAM)

Infrastructure:
  - Container security scanning
  - Kubernetes network policies
  - Infrastructure as code security
```

Risk Assessment Methodology

Quantitative Risk Analysis

```
Risk = Threat × Vulnerability × Impact
ALE = SLE × ARO
```

Risk Matrix Framework

Impact →	Low	Medium	High	Critical
High	Medium	High	High	Critical
Medium	Low	Medium	High	High
Low	Low	Low	Medium	Medium

Acceptance Criteria

- **Critical**: Immediate action required
- **High**: Action required within 30 days
- **Medium**: Action required within 90 days
- **Low**: Monitor and review quarterly

Implementation Strategy Framework

Phase 1: Assessment (Months 1-2)

- Current state analysis across all seven domains
- Gap analysis against security baselines
- Risk quantification and prioritization

Phase 2: Foundation (Months 3-6)

- Core infrastructure hardening
- Identity and access management implementation
- Basic monitoring and logging

Phase 3: Enhancement (Months 7-12)

- Advanced threat detection
- Automation and orchestration
- Continuous monitoring implementation

Measuring Success: KPIs and Metrics

Technical Metrics

- **Mean Time to Detection (MTTD)**: <15 minutes for critical threats
- **Mean Time to Response (MTTR)**: <1 hour for security incidents
- **Patch Management**: 95% compliance within SLA timeframes
- **Vulnerability Remediation**: Critical vulns fixed within 72 hours

Business Metrics

- **Security Investment ROI**: Cost avoidance vs security spending
- **Compliance Score**: Percentage of regulatory requirements met
- **Business Continuity**: RTO/RPO objectives achievement
- **User Productivity**: Security friction impact measurement

Real-World Case Study: Healthcare System

Organization Profile

- **Size**: 3,000 employees, 5 hospitals, 20 clinics
- **Compliance**: HIPAA, HITECH, state regulations
- **Challenge**: Legacy systems, limited budget, diverse user base

Risk Assessment Results

Domain	Risk Level	Primary Concerns
User	High	Phishing susceptibility, password reuse
Workstation	Medium	Unpatched systems, legacy applications
LAN	High	Flat network, limited segmentation
LAN-to-WAN	Medium	Single firewall, limited monitoring
Remote Access	Critical	No VPN, unsecured remote access
WAN	Low	Managed MPLS service
System/App	High	Legacy EHR, database vulnerabilities

Healthcare Case Study: Implementation

Year 1 Priorities (High/Critical Risks)

1. **Remote Access Security**
    - Deployed Cisco AnyConnect VPN with MFA
    - Cost: $150K, Risk Reduction: 85%
2. **Network Segmentation**
    - Implemented micro-segmentation for clinical systems
    - Cost: $300K, Risk Reduction: 70%

3. **User Security Training**
    - Monthly phishing simulations + targeted training
    - Cost: $50K, Risk Reduction: 60%

Results After 18 Months

- Zero successful ransomware attacks (industry average: 34%)
- 95% reduction in successful phishing attempts
- Passed HIPAA audit with zero findings

Financial Services Case Study

Organization Profile

- **Size**: Regional bank, 500 employees, 25 branches
- **Regulations**: SOX, PCI DSS, GLBA, FFIEC guidelines
- **Assets**: $2B in assets, 100K+ customer records

Security Baseline Requirements

```
User Domain:
  - Hardware security keys for all privileged users
  - Quarterly security awareness training
  - Background checks and insider threat monitoring

Workstation Domain:
  - NIST 800-171 hardening standards
  - Application whitelisting
  - USB device controls

Network Domains:
  - Zero-trust network architecture
  - 24/7/365 SOC monitoring
  - Quarterly penetration testing
```

Financial Services: ROI Analysis

Investment vs. Risk Mitigation

Initial Security Investment: $2.1M

- Infrastructure: $800K
- Staff training: $200K
- Technology licenses: $600K
- Professional services: $500K

Risk Mitigation Value: $8.4M

- Prevented data breach costs: $5.2M
- Avoided regulatory fines: $2.1M
- Business continuity protection: $1.1M

Net ROI: 300% over 3 years

Common Implementation Challenges

Technical Challenges

- **Legacy System Integration**: 40% of organizations struggle
- **Skills Gap**: Shortage of qualified security professionals
- **Tool Proliferation**: Average of 47 security tools per organization

Organizational Challenges

- **Budget Constraints**: Security often seen as cost center
- **Change Resistance**: User adoption and workflow disruption
- **Compliance Complexity**: Multiple overlapping regulations

Solutions

- Phased implementation approach
- Automation and orchestration tools
- Executive sponsorship and clear communication

Future Considerations

Emerging Threats

- **AI-Powered Attacks**: Sophisticated phishing and deepfakes
- **Supply Chain Attacks**: Third-party risk management
- **IoT Security**: Expanding attack surface

Technology Evolution

- **Zero Trust Architecture**: Identity-centric security model
- **SASE (Secure Access Service Edge)**: Cloud-native security
- **XDR (Extended Detection and Response)**: Unified security operations

Regulatory Trends

- **Privacy Regulations**: GDPR, CCPA expansion
- **Critical Infrastructure**: Increased government oversight
- **AI Governance**: Emerging regulations for AI systems

Key Takeaways

Risk Management Principles

1. **Context is Critical**: Risk tolerance varies by industry and organization
2. **Defense in Depth**: Multiple layers across all seven domains
3. **Continuous Improvement**: Regular assessment and adaptation
4. **Business Alignment**: Security as business enabler, not impediment

Implementation Success Factors

- Executive support and adequate funding
- Clear communication of business value
- Phased approach with quick wins
- Regular measurement and reporting

Final Recommendation

Start with high-impact, low-cost controls and build systematic coverage across all seven domains