1. Risk Management Framework (ISO 31000 Applied)

Key Terms Applied

- Asset: User credentials and project data.
- Threat: Phishing attack, DoS attempt.
- Vulnerability: Weak passwords, unpatched systems.
- Control: MFA, logging, encryption, backups.

Governance Structure

- CISO: Oversees risk management.
- IT Security Team: Implements technical controls.
- Incident Response Lead: Manages breach handling and escalation.
- Escalation Procedures: Incidents reported → IR Lead → CISO → Executive board (if high-impact).

Regulatory Compliance Matrix (HIPAA Example)

Control Area	HIPAA Requirement	Project Implementation
Access Control	Unique IDs, role-based access	MFA + least privilege access policies
Encryption	Encrypt PHI data at rest & transit	AES + SSL/TLS on sensitive data
Breach Notification	Report breaches within 60 days	IR plan includes notification protocol

Visual Framework (Alignment)

- ISO 31000 framework connects risk identification → assessment → evaluation → mitigation → monitoringdirectly into project lifecycle.

---

2. Risk Assessment Techniques

Identification Methods

- Brainstorming: Security team identifies phishing and malware risks.
- Checklists: Use NIST controls list for standard threats.
- SWOT Analysis:
    - Strengths: Encryption, MFA.
    - Weaknesses: Limited user awareness.
    - Opportunities: Better automation.

    - Threats: Phishing campaigns.

Qualitative Analysis – 5x5 Risk Matrix

- Likelihood (1–5) × Impact (1–5).
- Example: Phishing → Likelihood = 4, Impact = 4 → Score = 16 (High).

Quantitative Analysis

- EMV (Expected Monetary Value): $100,000 potential loss × 0.3 probability = $30,000 risk exposure.
- ALE (Annualized Loss Expectancy): If one phishing breach costs $20,000 and happens twice yearly, ALE = $40,000.

Threat/Vulnerability Assessment Findings

- Threat: Phishing. Vulnerability: Weak passwords. Asset: Credentials. Control: MFA.

Risk Register (Excerpt)

Threat	Likelihood	Impact	Risk Score	Control	Status
Phishing	4	4	16 (High)	MFA, training	Active
DoS	3	5	15 (High)	Rate-limiting	Active

---

3. Risk Evaluation

Multi-Criteria Model
Weights: Financial (30%), Operational (25%), Compliance (25%), Reputation (20%).

Business Impact Analysis (BIA)

- RTO (Recovery Time Objective): 12 hours.
- RPO (Recovery Point Objective): 1 hour of data loss acceptable.
- MTD (Maximum Tolerable Downtime): 48 hours.

Critical Asset Register

Asset	Threat	Vulnerability	Dependency	Exposure
Credentials	Phishing	Weak passwords	Authentication system	High

Availability	DoS	Lack of scaling	Web server	High

---

4. Risk Mitigation Planning

Controls (ISO 27001/NIST CSF)

- Technical: MFA, IDS, encryption.
- Administrative: Security policies, training.
- Physical: Secure server storage.

Treatment Options

- Mitigate: MFA reduces phishing risk.
- Avoid: Eliminate unused admin accounts.
- Transfer: Cyber insurance.
- Accept: Low-impact risks with minimal exposure.

Residual Risk
Phishing reduced from High to Medium with MFA + training.

---

5. Risk Communication

Executive Risk Report (Key Findings)

- High risk of phishing mitigated with MFA.
- DoS risks addressed with rate-limiting.
- ALE for phishing: $40,000 → reduced to $10,000 post-controls.

Stakeholder Communication Plan

- Audience: Executives, IT staff, users.
- Message: Tailored — executives get financial impact, IT staff get technical details, users get awareness training.
- Schedule: Monthly reports + immediate breach notifications.

Visual Dashboard

- Metrics: # of incidents, detection time, downtime, ALE reduction.
- Automated alerts: Sent when thresholds exceeded.

---

6. Risk Management Implementation

Program Plan

- Phase 1: Identify & assess risks.
- Phase 2: Apply controls & mitigation strategies.
- Phase 3: Continuous monitoring.

Framework Used: ISO 31000 customized for project scope.

Gap Analysis: Weak user training → add awareness program.

Continuous Monitoring

- Automated IDS alerts.
- Risk register updated quarterly.
- KPIs track response times, incident frequency, financial losses.

Final Wrap-Up

This single document combines:

- Incident Response Plan
- Security Policies & CIA Triad Protections
- Encryption/Hashing Demonstrations
- Legal & Ethical Compliance
- Full Risk Management Program (ISO 31000)

The mini threat model project is now tied directly to professional cybersecurity standards, risk management practices, and compliance requirements, creating a polished package suitable for executive review or academic grading.
