j.e.m.z technology

VULNERABILITY ASSESSMENT

JUNE 9, 2025

J.E.M.Z TECHNOLOGY
Preparer: Andrea Jared
IT Tech Support | Junior Network Admin | Security Analyst

j.e.m.z technology

Vulnerability Assessment Report

Assessment ID: VA-2025-Q1
Assessment Type: Organizational Risk & Security Controls Evaluation
Preparer: Andrea Jared
Assessment Date: June 9th 2025
Classification: Internal

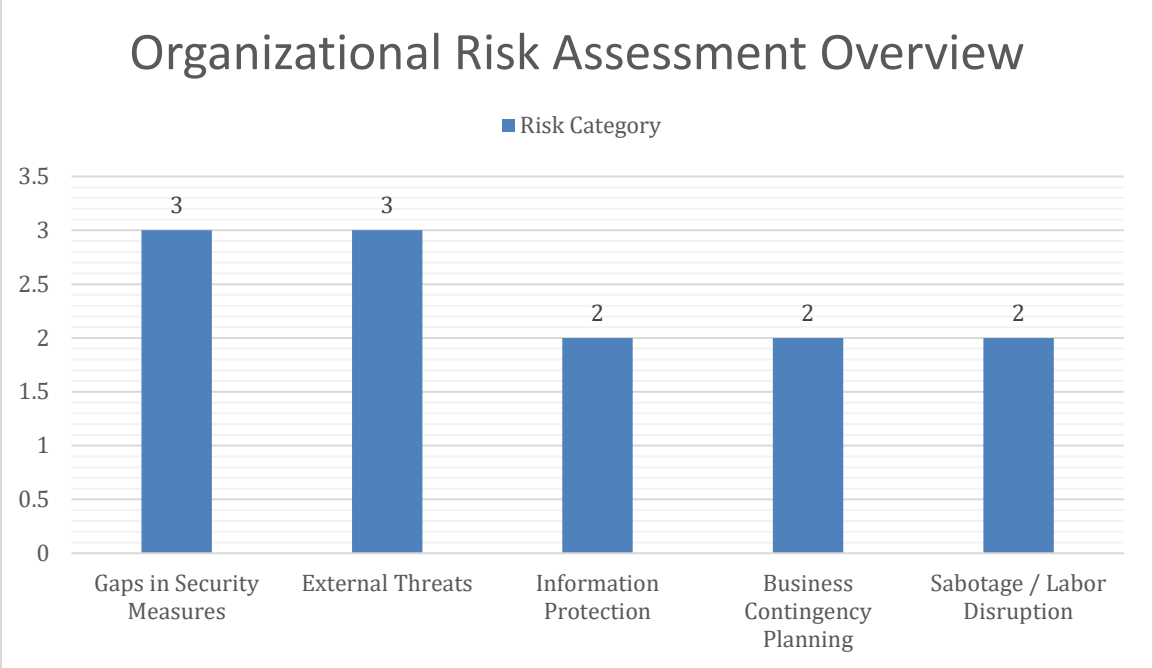
Executive Summary

This assessment evaluated organizational security controls, operational resilience, and exposure to internal and external threats. The review identified moderate-to-high risk exposure in areas of security control gaps, business contingency planning, and information protection standards.
Several opportunities for improvement were identified that will reduce operational disruption risk, protect organizational assets, and improve regulatory alignment.

Scope of Assessment:

- Physical and logical security controls
- External threat exposure
- Data protection practices
- Business continuity planning
- Organizational resilience to sabotage or labor disruption

Risk Category	Level of Concern	Priority	Operational & Financial Impact
Gaps in security measures	High	**Immediate**	Increased risk of breach & financial liability
External Threats	High	High	Potential Service disruption
Information Protection	Moderate	High	Risk of data loss or regulatory penalties
Business Contingency Planning	Moderate	Medium	Operational downtime risk
Sabotage / Labor Disruption	Low-Moderate	Medium	Temporary productivity impact



Detailed Findings:

Gaps in Security Measures

Level of Concern: High
Priority Setting: Immediate

Observations:

- Inconsistent multi-factor authentication enforcement
- Limited centralized logging and monitoring
- Infrequent access review processes

Operational & Financial Implications:

- Increased likelihood of unauthorized access
- Regulatory non-compliance exposure
- Potential financial penalties and reputational damage

Property Value Impact:

High-value intellectual property and customer data are exposed due to insufficient access control enforcement.

Challenges:

- Budget constraints for security tool implementation
- Change management resistance

Opportunities:

- Implement organization-wide MFA
- Deploy centralized SIEM monitoring
- Conduct quarterly access audits

Detailed Findings:

External Threats

Level of Concern: High
Priority Setting: High

Observations:

- Increased phishing campaign targeting employees
- Public-facing web services with limited WAF protection
- No formal threat intelligence monitoring program

Operational & Financial Implications:

- Service disruption
- Credential compromise
- Potential ransomware infection

Property Value Impact:

Critical infrastructure and digital assets at risk of compromise.

Opportunities:

- Deploy Web Application Firewall
- Implement phishing simulation program
- Integrate threat intelligence feeds

Detailed Findings:

Information Protection

Level of Concern: Moderate
Priority Setting: High

Observations:

- Data classification framework partially implemented
- No formal encryption policy for removable media
- Backup encryption inconsistently enforced

Operational & Financial Implications:

- Potential data leakage
- Regulatory compliance risk

Property Value Impact:

Sensitive customer and internal operational data exposed to confidentiality risks.

Opportunities:

- Full data classification rollout
- Enforce encryption for portable devices
- Implement DLP solution

Detailed Findings:

Business Contingency Planning

Level of Concern: Moderate
Priority Setting: Medium

Observations:

- Business Continuity Plan not tested in last 18 months
- Recovery Time Objectives (RTO) not clearly documented
- Disaster recovery roles not formally assigned

Operational & Financial Implications:

- Prolonged downtime in major incident
- Revenue loss during disruption

Property Value Impact:

Operational systems critical to revenue generation lack validated recovery processes.

Opportunities:

- Conduct annual disaster recovery simulation
- Document RTO/RPO metrics
- Assign recovery leadership roles

Detailed Findings:

Acts of Sabotage or Labor Disruption

Level of Concern: Low–Moderate
Priority Setting: Medium

Observations:

- Limited monitoring of privileged user behavior
- No formal insider threat awareness training

Operational & Financial Implications:

- Potential intentional service interruption
- Insider data exfiltration

Property Value Impact:

Intellectual property and confidential records vulnerable to internal misuse.

Opportunities:

- Implement User Behavior Analytics (UBA)
- Develop insider threat awareness training
- Enhance privileged account monitoring

Overall Risk Rating

Based on aggregated scoring and exposure:

Overall Organizational Risk Posture: Moderate–High

Immediate remediation should focus on:

1. Closing access control gaps
2. Strengthening external threat defenses
3. Improving monitoring and detection capabilities

Strategic Recommendations

- Implement Zero Trust access principles
- Establish continuous vulnerability management program
- Deploy centralized logging and SIEM
- Formalize business continuity testing schedule
- Conduct quarterly security governance reviews

Conclusion

While foundational security controls are present, several high-priority improvements are required to reduce exposure to external and internal threats. Addressing identified gaps will significantly reduce operational risk, improve regulatory compliance posture, and protect high-value organizational assets.