EXECUTIVE RISK SUMMARY
Governance, Risk & Compliance Assessment – Social Services Cloud Environment

Overview
This executive summary presents key risk findings identified during a governance, risk, and compliance assessment of a cloud-supported social services environment handling sensitive PII/ SPII data. The assessment evaluated application security, identity management, vendor exposure, endpoint risk, and governance processes to determine the organization's current risk posture and recommended mitigation priorities.

Risk Posture Summary
The organization demonstrates foundational security controls such as password policies, VPN access, email filtering, and audit logging. However, several high-priority gaps exist that may increase the likelihood of data exposure, operational disruption, or regulatory impact. The highest risks are associated with identity access management, phishing susceptibility, and endpoint vulnerability management.

Top Enterprise Risks

1. Unauthorized Access to Case Management System (Risk Score: 20)
   Weak MFA enforcement and excessive permissions create risk of unauthorized access to sensitive client records. Identity compromise remains the most critical exposure due to direct impact on regulated data.

2. Phishing Leading to Credential Compromise (Risk Score: 20)
   High likelihood of social engineering attacks against staff increases the probability of data breach through compromised identities. Limited user awareness training elevates this risk.

3. Endpoint Vulnerabilities and Patch Gaps (Risk Score: 16)
   Legacy devices and lack of centralized patch reporting increase exposure to known CVE exploitation and automated attack tools.

Moderate Risks
• Vendor cloud storage misconfiguration could expose sensitive files if periodic configuration audits are not implemented.
• Insider misuse risk exists due to limited user behavior analytics and broad data access permissions.
• Lack of formal incident response documentation may delay breach containment and recovery.
• Absence of a defined data classification policy increases risk of accidental data exposure across collaboration platforms.

Business Impact
Failure to address these risks may result in unauthorized disclosure of protected information,

regulatory non-compliance, reputational damage, and disruption of critical social services operations. Identity-based attacks and human error present the greatest threat to operational continuity.

Recommended Strategic Actions

- Enforce multi-factor authentication (MFA) and conduct role-based access reviews across core applications.
- Implement structured phishing awareness and simulation training for staff.
- Deploy centralized vulnerability management and patch reporting capabilities.
- Establish formal incident response playbooks aligned with NIST 800-61 guidance.
- Develop and enforce a data classification standard to strengthen governance.

Conclusion

The organization maintains a functional security baseline but requires targeted governance and risk management improvements to strengthen resilience against identity-driven threats and data exposure risks. Addressing the prioritized recommendations will significantly reduce overall risk and improve compliance alignment.