CYBERSECURITY & RISK + FINANCIAL SYSTEMS & CONTROLS

Business Account & Financial-System Security Review

A focused human review of the accounts, permissions, financial workflows, and recovery controls that can lead to financial loss, payroll disruption, sensitive-data exposure, or account takeover.

THE PRACTICAL QUESTION

Could a compromised account, weak permission, poor workflow, or missing control expose the business to financial loss or operational disruption?

WHAT THE REVIEW CAN EXAMINE

Identity & access

- MFA, administrators, privileged and shared accounts
- User permissions, stale accounts, and recovery methods
- Employee and contractor onboarding and offboarding

Financial systems & payments

- QuickBooks, payroll, banking, and processor access
- Vendor and ACH changes, approvals, and audit trails
- Segregation of duties and financial-fraud controls

Business accounts & SaaS

- Microsoft 365, Google Workspace, and cloud storage
- Critical SaaS administration, integrations, and provisioning
- Access to sensitive client and employee information

Recovery & operational readiness

- Backup access, coverage, and restoration readiness
- Account and system inventories and responsibilities
- Basic policy, continuity, and incident-readiness gaps

WHAT THE CLIENT RECEIVES

A decision-ready review - not a scanner report.

- Concise executive summary
- List of reviewed systems and accounts
- Prioritized, risk-rated findings
- Evidence supporting each finding
- Practical remediation recommendations
- Immediate, near-term, and longer-term priorities
- Management findings discussion
- Clear boundary between observed and unverified conditions

REQUEST A SECURITY REVIEW hello@lillyfinancial.net

STRUCTURED, EVIDENCE-BASED, AND REPEATABLE

A practical review of how access and financial controls operate.

01

Define the material systems

Agree on the accounts, platforms, workflows, people, providers, and evidence within scope.

02

Examine control operation

Review permissions, configurations, records, procedures, and the way critical changes actually occur.

03

Prioritize practical action

Deliver supported findings, risk levels, remediation priorities, and a management discussion.

CONDITIONS THE REVIEW IS DESIGNED TO FIND

Payment authority

One person can create a vendor, change payment details, and approve payment without independent review.

Administrative access

A critical administrator account lacks appropriate MFA or relies on an insecure recovery method.

Access lifecycle

A former employee or contractor still has access to email, files, payroll, accounting, or SaaS.

Recovery confidence

Backups exist, but their access is weakly protected or restoration has never been tested.

CLEAR SERVICE BOUNDARY

Defensive review and remediation guidance.

INCLUDED WHEN SCOPED

- Interviews and workflow review
- Account, permission, and control review
- Configuration and evidence sampling
- Risk-rated findings and recommendations

NOT INCLUDED

- Penetration testing, red teaming, or exploitation
- Malware analysis, digital forensics, or 24/7 response
- SOC or managed detection and response
- Certification, legal opinions, or security guarantees

Methodology is informed by the NIST Cybersecurity Framework and recognized internal-control practices. This does not imply NIST certification or endorsement.

REQUEST A SECURITY REVIEW lillyfinancial.net/business-account-security-review/