Cybersecurity Program Proposal

PRESENTED BY

Kelly Sophia Camacho

PRESENTED TO

Lemonade

Business Objective

Data Security

Protect essential assets and reduce risk

Business Continuity

Ensure operational resilience for critical business functions

Regulation Compliance

Comply with industry specific regulations

GDPR | HIPAA | CCPA | EU AU Act

Increase Automation

Improve efficiency and decrease intensive process

Security Plan Objectives

- Data Security
- Regulation Compliance
- Business Continuity
- Increase Automation

Establish strong and resilient security posture that safeguards organization's assets, while enabling business growth

Protect Sensitive Data

Mitigate Cyber Threats

Foster Security-Conscious Culture

Enhance Security Posture

Risk Identified

01 Regulatory Compliance

Non-compliance to data protection laws and industry specific regulations

02 Third Party + Cloud

Security risks associated with third party vendors and cloud service providers

03 Asset Management

Security vulnerabilities and poor process of identifying, classifying, and protecting assets

04 Artificial Intelligence

Security risks from internal (model vulnerabilities) and external sources abusing the model

Risk Assessment – High Priority

ID NO.	RISK or HAZARD DESCRIPTION	RESOURCES IMPACTED	PROBABILITY LEVEL	IMPACT LEVEL	PRIORITY VALUE
Regulaton Requirement					
1	Data Privacy (regulatory non-compliance)	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	High	High	9
2	Data Retention and Destruction (regulatory non-compliance)	- Financial Loss (fines, legal fees) - Operational Efficiency	High	High	9
Third Party + Cloud					
3	No vender risk management	- Company Reputaion - Data (PHI and PII) - Financial Loss (legal fees, loss of business)	High	High	9
4	Supply Chain Attack (Vendor Compromise)	- Data (PHI and PII) - Operations - Financial Loss	Medium	High	6
5	Supply Chain Discruption	- Data (PHI and PII) - Operations - Financial Loss	Medium	High	6
6	CSP Vulnerabilities (like misconfigurations)	- Data (PHI and PII) - Technology (applications and systems)	Medium	High	6
7	CSP Breach	- Data (PHI and PII) - Technology (applications and systems) - Company Reputation - Financial Loss	Medium	High	6

Risk Assessment – High Priority

ID NO.	RISK or HAZARD DESCRIPTION	RESOURCES IMPACTED	PROBABILITY LEVEL	IMPACT LEVEL	PRIORITY VALUE
AI					
8	AI Fairness	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Operational Efficiency	Medium	High	6
9	Privacy Violations (AI)	- Regulatory Compliance - Company Repuation (customer trust/loyalty)	Medium	High	6
10	Model Bias (AI)	- Regulatory Compliance - Company Repuation (customer trust/loyalty) - AI Model Accuracy	Medium	High	6
11	Model Exploitaiton and Manipulation (AI)	- AI Model Accuracy - Company Reputation (customer trust)	Medium	High	6
Asset Management					
12	Lack of Structured Risk Management	- Data (PHI and PII) - Operations - Technology (applications and systems)	Medium	High	6
13	Legacy Applications/Systems	- Data (PHI and PII) - Operations - Company Reputation	Medium	High	6
14	Data Breach	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	Medium	High	6
15	Data Loss	- Financial Loss (fines, legal fees) - Company Reputation (customer trust/loyalty) - Customer Data (PHI and PII)	Medium	High	6

Solution - Policy and Procedures

Access Control

- Enhance data confidentiality
- Reduce unauthorized access

Implementations include:
MFA, PoLP, RBAC, IAM

Data Protection

- Enhance data integrity
- Prevent data loss

Implementations include:
Data Retention and Destruction, Data Encryption, Regular Audits

Incident Response

- Faster incident detection
- Reduced downtime

Implementations include:
Communication Procedures, Monitoring and Detection

Risk Management

- Prioritize risk mitigation
- Proactively identify threat/risk

Implementations include:
Risk Monitoring, Threat Modeling, Regular Assessments

Vender Management

- Reduced supply chain risks
- Secure third-party relationship

Implementations include:
Vendor Assessment, Continuous Monitoring

Security Awareness

- Improved security culture
- Reduce human error

Implementations include:
Employee Training, Tabletop Exercise, Phishing Simulations

Solution - Security Controls

Network

- Enhance confidentiality
- Reduce risk of breach

Implementations include:
IDS/IPS, NAC, Firewall

Application

- Ensure data protection
- Protect from attacks

Implementations include:
WAF, Input Validation, Output Encoding, PenTesting

AI Model

- Privacy preservation
- Protect from attacks

Implementations include:
Adversarial Training, Version Control, Fairness and Bias Testing

Cloud

- Ensure data protection
- Maintain compliance

Implementations include:
DLP, CSPM, Data Encryption

Roadmap

Year 1

Foundation and Implementation

Establish a strong security foundation

Implement core security controls and policies

Raise security awareness

Year 2

Expansion and Risk Management

Implement advanced security controls

Optimize risk management

Enhance comprehensive security plans

Year 3

Maintenance and Continuous Improvement

Maintain and enhance security posture

Optimize security operations for efficiency and effectiveness

Milestones Year 1

Risk Reduction: ~30%

Unauthorized Access
Data Breaches
Network Attacks
Human Error

Q1

Implement IAM

Begin implementing RBAC and PoLP principles

Conduct security awareness training for all employees

Q2

Complete RBAC and PoLP principles

Implement data retention and destruction policies and procedures

Conduct phishing simulation exercise

Implement MFA for all user accounts

Q3

Implement data encryption for data at rest and in transit

Implement patch management to address vulnerabilities promptly

Q4

Deploy network security controls (firewalls, IDS/IPS)

Implement NAC

Conduct tabletop exercise to test incident response procedures

Establish communication procedures for an incident response

Milestones Year 2

Risk Reduction: ~40%

Cloud Security Vulnerabilities
Third-Party Risks
AI Model Bias and Vulnerabilities
Data Loss and Exposure
Web Application Attacks

Q1

Deploy WAF to protect Web Application

Implement input validation and output encoding controls for applications

Conduct vulnerability assessment and penetration testing (VAPT)

Q2

Conduct security awareness training

Implement CSPM to monitor cloud security posture

Implement DLP

Establish regular AI fairness and bias testing

Q3

Implement AI model security controls (transparency, version control and adversarial training)

Implement regular risk assessment and monitoring process

Implement vendor risk management program (vendor assessments)

Q4

Develop and implement comprehensive incident response plan (IR) + business continuity and disaster recovery plan (BCDR)

Conduct full security audit to assess overall security posture

Conduct a compliance audit

Milestones Year 3

Risk Reduction: ~30%

Regulatory Non-Compliance
Zero-Day Exploits
Advanced Persistent Threats
Ineffective Security Controls

Q1

Enhance incident response capabilities (improved monitoring and detection tools)

Conduct red team + blue team exercises to test security defenses

Q2

Implement advanced threat protection technologies, including Endpoint detection and response (EDR)

Conduct security awareness campaign focused on emerging threats

Q3

Review and update security policies and procedures based on evolving threats and regulations

Conduct security audit for implemented controls effectiveness

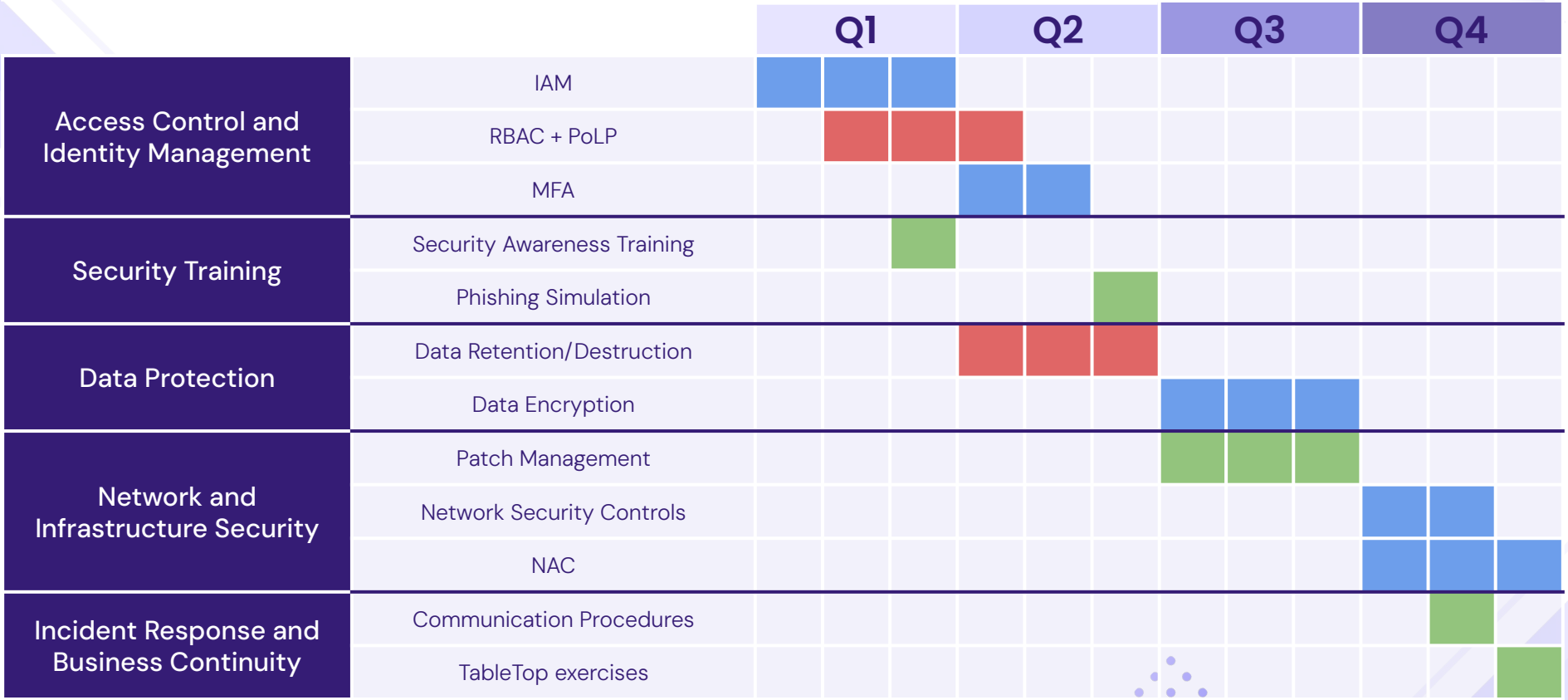
Q4

Conduct final security audit and review the overall security posture

Conduct a compliance audit

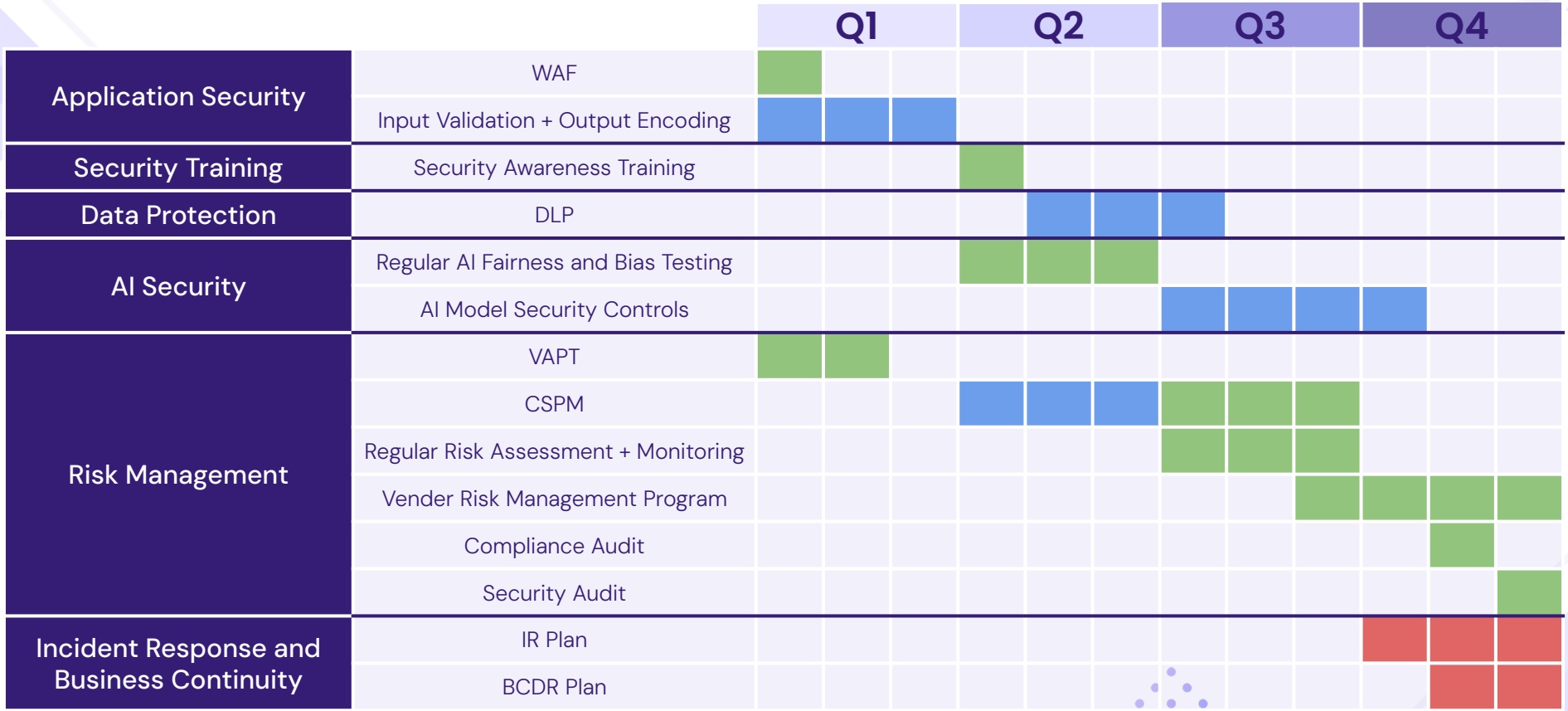
Technology Policy Process

Year 1 Timeline



Technology Policy Process

Year 2 Timeline



Technology Policy Process

Year 3 Timeline

Anticipated Challenges

Challenge	Mitigation Strategies
Technical Complexity	- Ensure compatibility between tools - Conduct small scale to test new technologies before full deployment - Hire external consultants such as security experts/consultants
Regulatory Compliance	- Stay updated on regulatory changes and adjust as needed - Engage with legal and compliance experts - Conduct regular audits to assess compliance
Emerging Threats	- Stay informed and updated on latest security trends/threats - Conduct regular security assessments
Employees Resistance to Change	- Clear communication behind change reasons - Provide training to help employees understand security measures - Roll out changes gradually to minimize disruption

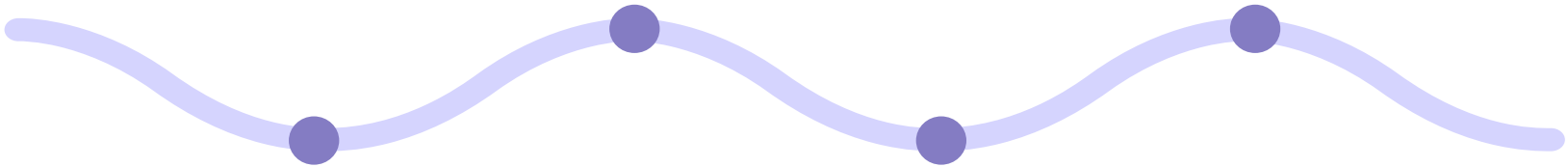
Feedback Loop

Security Committee Meetings (Quarterly)

Ensure security measures are held to standard and decisions are made in timely manner

Metrics and KPI Reviews (Quarterly/Annually)

Assess the overall progress the security program in a timely manner



Security audits and assessments (Biannual)

Assess effectiveness of security controls and measure compliance

External Security Assessments (Annually)

Validate effectiveness of internal security controls and asses security posture from a different perspective

KPIs

Security Posture		Security Awareness		Operational Efficiency		Incident Response + Business Continuity	
Quarterly							
Vulnerability Assessment	Measure the number of critical vulnerabilities	**Phishing Simulation Success Rate**	The percentage of employees who click on phishing links	**Security Tools Utilization**	Measure the usage and effectiveness of security tools	**Mean Time To Detect (MTTD)**	Measure time taken to detect a security incident
				Risk Mitigation Effectiveness	Measure the percentage of identified risks that are mitigated or transferred	**Mean Time To Respond (MTTR)**	Measure efficiency of incident response team in resolving incidents alerts
Annual							
Compliance Adherence	Measure compliance with relevant regulations and industry standards	**Employee Security Behavior**	Measures employee adherence to security policies and procedures	**Budget Utilization**	Measure efficiency of budget allocation	**Disaster Recovery Time Objective (RTO)**	Measure time taken to restore critical systems and services after a disaster
				VAPT Findings	The amount and severity of vulnerabilities identified	**Disaster Recovery Point Objective (RPO)**	Measure the amount of data loss tolerated

Budget and Resources Allocation

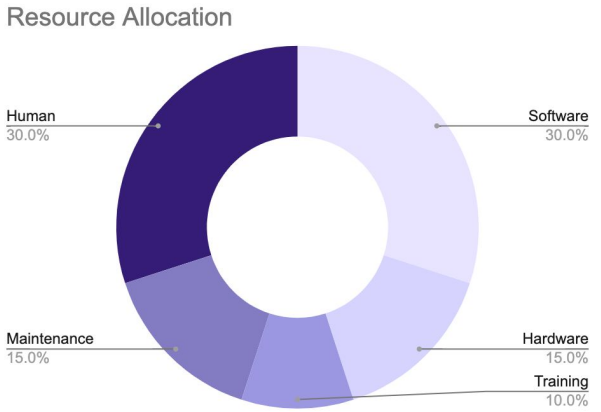
Software ~ $3M
For needed software and licensing fees for security software, tools, and platforms

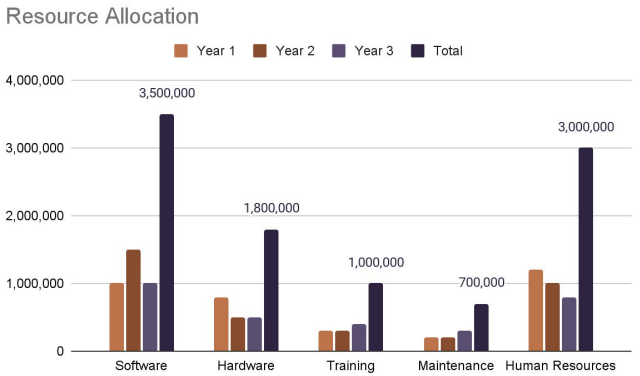
Hardware ~ $1.5M
For purchasing and maintenance of security hardware, including servers, network devices, and security applications

Training ~ $1M
For training for awareness and security best practices for employees

Maintenance ~ $1.5M
For ongoing maintenance including security consulting services, and operational costs

Human Resources ~ $3M
For employment of security team and external experts such as auditors, consultants, and pentesters





Internal VS External Budget

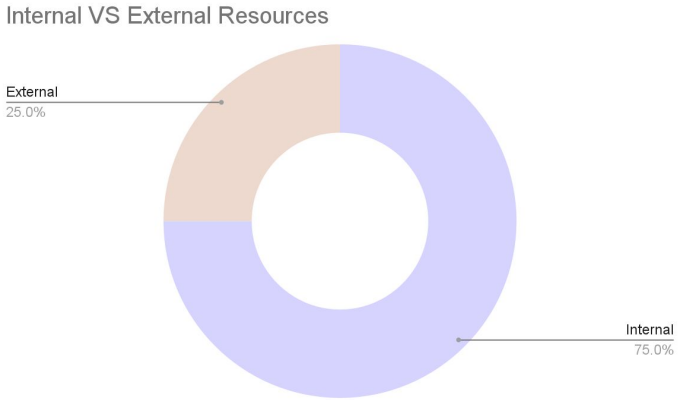
Internal ~ $7.5M (75%)
For employment and maintenance of security team

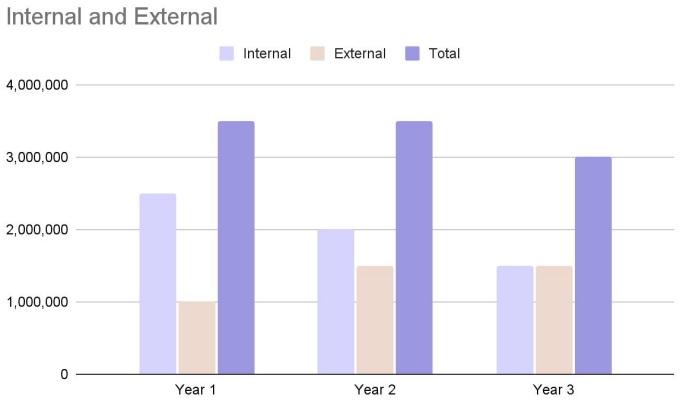
External ~ $2.5M (15%)
For external security consultants, penetration testing services, and other specialized experts

Year 1
High allocation to internal resources to build core security team and invest in initial training while leveraging external resources for specialized expertise.

Year 2
Lower allocation to internal resources needed due to investing in advanced security technology and using external resources for specialized expertise and consulting services.

Year 3
Balance between internal and external resources due to organization effectively managing security programs in place and being able to mitigate risks while leveraging external resources for ongoing assessments and emerging technologies





Conclusion

This security program outlines a comprehensive approach to enhancing Lemonade's security posture.

By meeting these security objectives, Lemonade will be able to protect its critical assets, maintain regulatory compliance, and support its business growth.

Objective Alignment

- Protect sensitive data
- Adherence to industry regulations/standards
- Comprehensive incident response and business continuity plan
- Foster security-conscious culture
- Enhance security posture
- Mitigate cyber threats
- Continuous improvement