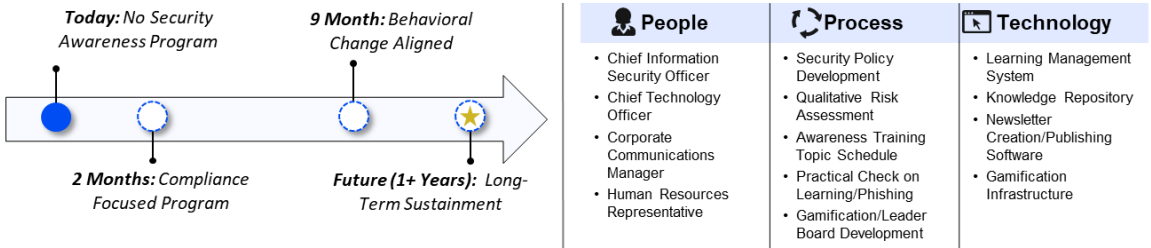


# Project Charter

Resourcing Requirements			Organizational Gaps	Project Snapshot
<b>Duration</b>	<b>Manpower</b>	<b>Funding</b>	<b>Skill:</b> <i>None</i>	<div><div><div>Cost</div><div>LowHigh</div></div><div><div>Anticipated Value</div><div>EffectivenessEfficiency</div></div></div>
<b>Build:</b> 12 Months	<b>Build:</b> 1 FTEs	<b>Build:</b> \$65,000	<b>Technology:</b> Learning Management System, Knowledge Repository, Training Modules	
<b>Run:</b> Ongoing	<b>Run:</b> 2 FTEs	<b>Run:</b> \$40,000		
<b>Project Overview</b>				<b>Priority:</b> <div>LOWMEDHIGH</div>

## Project Overview



Current State Risk Profile

1

Regulatory Risk: Non-compliance with cyber regulations around security training and awareness

2

Business Risk: Loss of proprietary or sensitive business information as a result of a cyber incident

3

Operational Risk: Inability to leverage enabling technology for day to day functions

Critical Success Factors

Success Factor 1

Compliance with all applicable regulatory standards associated with security awareness

Success Factor 2

Specialized training of high-risk groups and individuals

Success Factor 3

Cultural acceptance of security awareness across the organization

Anticipated Difficulty

High

Medium

Low

## Project Details

- Develop Foundational Policy Documents:** Revision of existing security policies to include suggested security awareness guidance.
- Qualitative Risk Analysis:** Estimating and risk ranking cyber human risks by their probability and impact to our organization
- Initial Training:** Leveraging in house or outside resources to conduct high impact initial training
- Convening Advisory Board:** Select and regularly meet with members for different business units for input and guidance into security awareness matters
- Gathering Qualitative Metrics:** Incorporate a metrics program which utilizes KPIs and KRIs
- Conduct Targeted Training:** Facilitate specialized training for high risk and privileged members of the organization
- Begin Ambassador Program:** Formally empower security ambassadors across different regions
- Push Regular Newsletters:** Begin sending out a customized security newsletter with rotating topics
- Gamification of Training:** Develop the building blocks for security awareness gamification

RACI	
<b>Responsible</b>	Chief Information Security Officer
<b>Accountable</b>	Security Awareness Officer, Security Awareness Personnel
<b>Consulted</b>	Chief Information Officer, Advisory Board
<b>Informed</b>	Department Heads, Information Technology Staff, Human Resources Managers, Ambassadors

Project Sequencing				
1 Months	3 Months	6 Months	9 Months	1+ Year
A	D		G	
B	E		H	
	F			
C			I	

Outputs
<ul style="list-style-type: none"> <li>Established Annual Training Schedule</li> <li>Formation of Security Awareness Advisory Board</li> <li>Specialized and Localized Training Modules</li> <li>Quantitative Metrics Collection and Analysis</li> <li>Adoption of Security Awareness Gamification</li> </ul>

