Phase	Topic	Details and examples	Schedule s
Assess	Stakeholders meetings	Conduct meetings with crucial stakeholders, including the Chief Technology Officer (CTO), Chief Financial Officer (CFO), Data Protection Officer/Legal (DPO/Legal), IT, HR, Research and Development (R&D), DevOps, Quality Assurance (QA), and Sales/Marketing, as well as Operations personnel. During these meetings, focus on eliciting valuable insights through the following inquiries: 1. Obtain a comprehensive overview of each manager's domain. 2. Gain a deep understanding of the business aspects within each department. 3. Identify and prioritize key objectives for each manager. 4. Address any concerns they may have. 5. Establish success criteria for the security program. Additionally, it is crucial to comprehend the business side of operations and establish points of contact. This understanding will prove invaluable in responding to security incidents such as ransomware recovery, business email compromise, compromised web application servers, and other potential threats.	
Assess	Review Past Infosec activities such as:	1. Awareness Program 2. Pentests 3. Vulnerability management program 4. Tools and configurations 5. Incidents/ Breaches 6. Privacy and compliance assessments	
Assess	Gather existing InfoSec materials such as:	1. Policies 2. Diagrams 3. Risk Assessments 4. Business Impact analysis 5. Assets list 6. Security Plan/roadmap 7. Controls list 8. Historical Pen Tests 9. Strategic plan 10. Work Plans 11. Incidents list 12. 3rd parties and supply chain data 13. Hardening procedures 14. Data mapping and classification 15. Compliance processes 16. Knowledge management system 17. Awareness training materials and campaigns	

Phase	Topic	Details and examples	Schedule s
Assess	identify all Assets:	1. Identify all platforms that store, process or transmit data: 2. IT management systems 3. Security tools and platforms 4. Devops and CI/CD platforms 5. DBA tools, platforms and Databases 6. RND development environment and management 7. Code repository and SBOM 8. Knowledge and LMS 9. Financial platforms: CRM/ERP/Bookkeeping/payments 10. Marketing and SD	
Assess	Assess to all systems	1. Directory and content management environments 2. EDR 3. CRM 4. Cloud services 5. ERP 6. network devices 7. Code Review system 8. CSPM/SSPM/ASPM 9. SIEM/SOC 10. Data centers 11. On prem components 12. Development management frameworks 13. code repositories 14. Dec and code management tools (JIRA) 15. Knowledge and content management environments (LMS, confluence etc.)	
Assess	Define initial budget	Make sure you are fully aligned with management about the budget for the rest of the year.	
Assess	Identify 5 Strategic Gaps:	Identify the 5 most critical security GAPs that needs to be handle as top priority.	
Assess	Define Roles and responsibilities:	Define the following roles and responsibilities for: 1. Physical security 2. Business continuity and disaster recovery (BC/DR) 3. Privacy 4. Compliance 5. IT risk 6. Risk governance 7. Security operation	

Phase	Topic	Details and examples	Schedule s
Understand	BIA- Business impact analysis	Business Impact Analysis (BIA) is a crucial component of business continuity planning that assesses the potential consequences of disruptions to key business operations.	
Understand	Maturity assessment	1. Use Best Practice questionnaire. 2. identify Resources, Budget, Risk Processes, & Technology. 3. Perform Gap Analysis (Interviews, Assessments, etc.) 4. Meet with Critical Vendor Partners 5. Validate Ransomware Readiness (Risk of Interruption to Business Operations) 6. Review Security Technical Controls (Identify, Protect, Detect, Respond, Recover) 7. identify the Top 3 Risks and Options to Address (Business Plan Components) **Assessments Scope**: 1. Risk Register 2. Audits, Compliance & Regulatory Reports 3. Controls Maturity Frameworks - e.g., ISO, NIST, CIS 4. Threat & Vulnerability assessments 5. Penetration tests & other Risk Assessments 6. Phishing tests	
Understand	Threat assessment	**Define Scope of Threat Assessment** A successful threat assessment begins with defining scope. This stage of the pre-planning should provide a clear roadmap for what a successful threat analysis looks like and what's involved at every stage. **Build Processes and Procedures Needed to Perform Threat Assessment** If the scope has been properly outlined, defining goals, what's to be covered and what's required to meet these analysis goals, the processes and procedures should easily fall into place. **Define a Rating System for Threats** Defining a rating system for threats identified in a threat analysis can help communicate the severity of threats, risks, and vulnerabilities to all key stakeholders in an approachable and easy-to-understand format. **Perform Threat Analysis** Lastly, once the scope, processes and procedures and rating system are in place, it's time to perform the threat analysis.	
Understand	Risk Assessment	Use Best Practice questionnaire based on threat analyses	

Phase	Topic	Details and examples	Schedule s
Prepare	Priorities	1. Identified urgent issues and longer terms strategic issues to be addressed. 2. Can the initiative be achieved within three months? 3. Will you have the required executive support, resources and budget? 4. Is the initiative linked to cyber-risk reduction? 5. Is the risk of failure is relatively low?	
Prepare	Security Strategy	**Strategic Plan Scope**: 1. Security Program Vision & Strategy 2. Regulatory & Industry Benchmarks 3. Security Scorecard & Top Risks 4. Gap Analysis, Quantified Recommendations, Budget, People, Skills, Investments (sometimes called a "Business Plan") 5. Delivery Roadmap 6. Performance Metrics	
Prepare	Adopt a relevant security framework	1. NIST 2. ISO 27001 3. PCI DSS 4. SOC1/2 5. MITRE ATT&CK	
Prepare	KPI	Agreed at least three key issues (quick wins) to close out over the next two months	
Execute	Inform:	1. Gain approval for the information security program, interim strategy and vision - socialize with key stakeholder: 2. Schedule bi-weekly meetings with key employees and managers 3. Meet with executive management at least once a quarter.	
Execute	Assign projects ownerships	Make sure all tasks' owners are fully aware to their duties.	
Execute	Refine roles and responsibilities	1. Ensure that all security managers roles and responsibilities are well-defined roles and responsibilities. 2. Make clear what each security manager is accountable for, and how their performance will be assessed. 3. Ensure that all line-level security staff have clear job descriptions and responsibilities that clearly reflect the work each employee actually does.	
Execute	Workplan execution	Start with the strategic goals and KPI that were defined in earlier stages.	
Execute	Test BCP, DRP and IRP		
Execute	Budget	Planned operational security budget for the following year , based on the results of your workplan and tests.	