Phase 1: Gap Assessment
1-2 Months

Connect & Determine Scope
- Team introductions
- Kickoff meeting
- Determine scope, including assessment criteria

Assess the Client
- Walkthroughs and interviews
- Document reviews
- System observation and inspection

Debrief
- Prioritized gaps and recommendations
- Initial set of controls
- High-level scope definition

Prepare & Finalize Deliverables
- Present deliverables to client
- Communicate Phase 2 budget

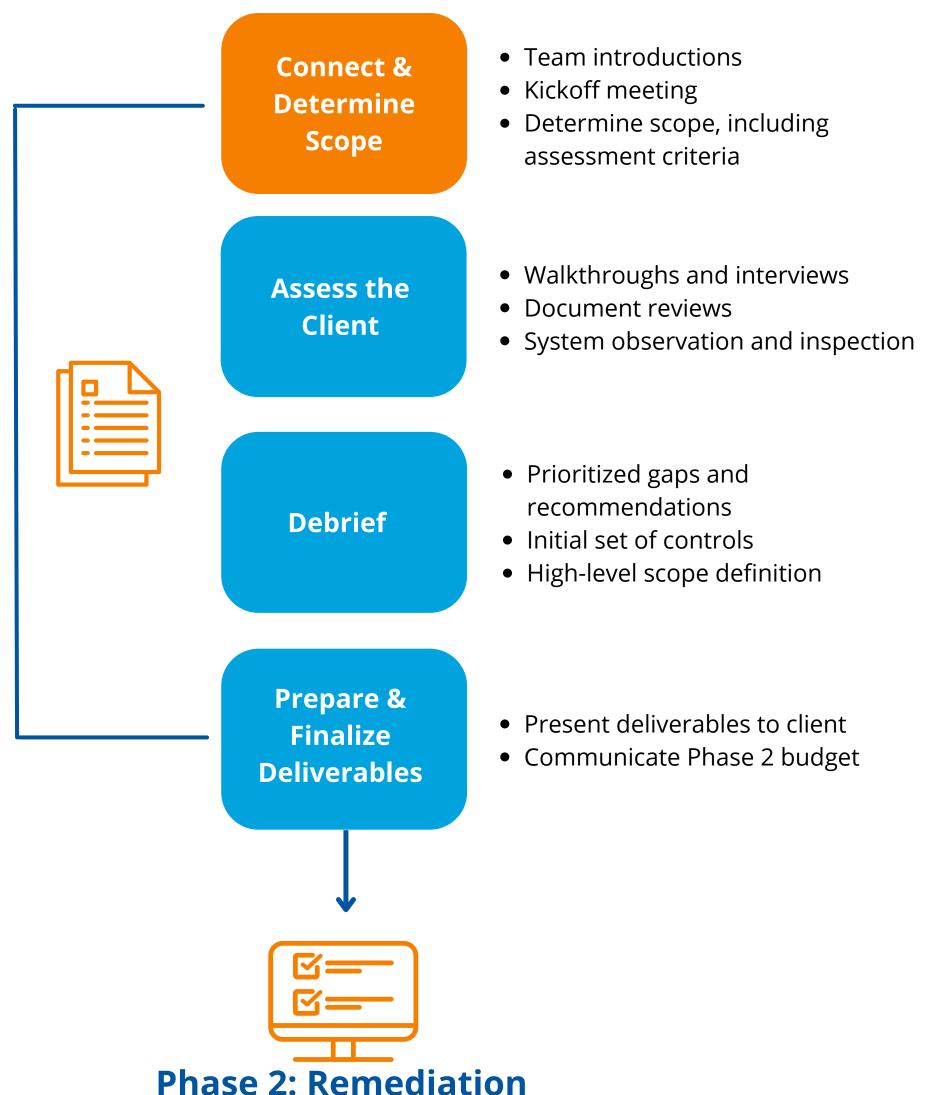## Phase 2: Remediation
1-3 Months

Establish Security Committee
- Form a security team
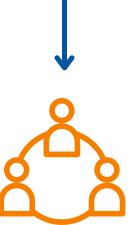- Document team members' responsibilities

Project Management
- Security team documents
- Information security policies and procedures
- Final set of controls mapped to in-scope framework

Phase 2 Deliverables
- Ensure all gaps and recommendations progress toward remediation

Determine Phase 3 Approach
- Define security plan
- Roadmap for sustainable long and short-term information security management program
- Communicate Phase 3 budget estimates

Phase 3: Continuous Management

Ongoing CISO Advisory services:
- Customer compliance questionnaires
- Risk assessments
- Vendor evaluations
- Internal audits
- Security awareness training
- Penetration tests
- Reviews and updates of policies and procedures
- InfoSec KPIs