Control ID	Control Name	Category	Description	Current State	Target State	Gap Summary	Recommended Actions	Priority	Status
A.5.1	Information Security Policies	Governance	Policies for information security are documented, approved, communicated, and reviewed	Partial	Full	Policies outdated and not reviewed annually	Implement annual policy review cycle; update Acceptable Use, Password, and Remote Work policies	High	Open
A.6.1	Information Security Roles & Responsibilities	Organization	Security roles are formally assigned and communicated	Minimal	Full	No formal RACI or documented security responsibilities	Create a RACI matrix; document responsibilities for IT, HR, and business units	Medium	In Progress
A.8.1	Asset Management	Asset Management	Information assets are identified and ownership assigned	Partial	Full	No centralized asset inventory or owner assignment	Deploy asset management tool; assign owners for each asset category	High	Open
A.9.2	User Access Management	Access Control	User provisioning, modification, and removal are controlled	Minimal	Full	Inconsistent user access reviews; no formal offboarding process	Implement IAM workflow; quarterly access reviews; standardized offboarding checklist	High	Open
A.10.1	Cryptographic Controls	Cryptography	Use of cryptographic solutions and key management is defined	Minimal	Full	Data at rest not encrypted; no documented crypto standards	Enable full-disk encryption; create cryptographic control policy; secure key storage	High	Open
A.12.4	Logging and Monitoring	Operations	Security events and logs are collected, retained, and reviewed	Partial	Full	Logging enabled but not centralized; no review process established	Deploy SIEM; create log review procedures; set retention policies	Medium	Not Started
A.17.1	Business Continuity Planning	Business Continuity	Information security continuity is integrated into business continuity	Partial	Full	BIA incomplete; no recovery testing conducted	Complete BIA; test recovery procedures quarterly	Medium	In Progress

ISO 27001 Control Maturity Rating Guide:				
Rating	**Description**			
None	No control exists			
Minimal	Control exists but is informal or inconsistent			
Partial	Control partially implemented or missing documentation			
Defined	Control is documented and approved but not fully followed			
Managed	Control is implemented and monitored			
Optimized	Control continuously improved with metrics			

ISO 27001 Annex A Gap Assessment — Executive Summary

This gap assessment evaluates Gladden Tech's current alignment with ISO/IEC 27001:2022 Annex A controls. The goal is to identify strengths, weaknesses, and the steps required to reach an audit-ready security posture.

Key Findings:

- Security policies require updates and an annual review cycle to meet ISO requirements.
- Roles and responsibilities are not formally documented, impacting governance.
- Asset inventory is incomplete and lacks assigned owners.
- Identity and access management processes are inconsistent and not regularly reviewed.
- Data encryption is not consistently applied across endpoints or storage systems.
- Logging and monitoring capabilities are limited without centralized SIEM visibility.
- Business continuity processes are partially implemented but require testing.

Overall Maturity Summary:

Domain	Maturity
Governance	Partial
Access Control	Minimal–Partial
Asset Manageme	Partial
Operations	Partial
Cryptography	Minimal
Business Continu	Partial

Top 3 Remediation Priorities:

1. Establish formal IAM processes (MFA, access reviews, offboarding).
2. Implement encryption standards for data at rest and key management.
3. Deploy centralized logging and define monitoring procedures.

Conclusion:

Gladden Tech demonstrates foundational information security controls but must strengthen governance, access control, monitoring, and data protection to reach ISO 27001 readiness.