Justification – IR-1 Incident Response Policy

I chose Incident Response Policy because it ensures that SnowBe can act fast and effectively when security incidents occur. The cyber threats are increasingly daily and sensitive customer data is at high risk. This therefore need a clear incident response policy which helps to reduce damage and recovery time, while also maintaining business continuity and compliance.

Control Enhancements:

- The 1-hour response rule ensures rapid containment.
- Root cause analysis should be included since it strengthens future prevention.
- Reports should be provided without fail so as to improve visibility across departments.
- Structure the incident phases (detect, analyze, contain, recover) to match NIST guidelines.

Justification – AC-1 Access Control Policy

Access Control Policy (AC-1) is essential for ensuring only authorized users can access SnowBe’s systems. It protects data by enforcing least privilege and requiring identity verification like MFA. As we know that SnowBe has a diverse team and sensitive data, control policy will prevents misuse and unauthorized access of the systems and critical data.

Control Enhancements:

- Make enforcement to be automatic to make sure that there is consistent access to rules.
- RBAC supports access based on roles.
- Do regular reviews to identify and solve outdated permissions.
- Ensure that access is central to make management easier.