PILLAR THREE

Identity

Strong identity management ensures the right people have the right access to the right resources at the right time for the right reasons.

SCENARIO

A staff member leaves the organisation but still has access to critical systems.

Another employee shares their login details with a contractor.

A hacker uses stolen credentials to access sensitive information.

Weak identity management can lead to data breaches, fraud, and loss of public trust.

WHAT IS IDENTITY?

Identity is the digital representation of a person or entity that is used to verify who they are and determine what they can access.

Effective identity management ensures identities are unique, verified, secure, and governed throughout their lifecycle.

QUESTIONS EVERY ORGANISATION SHOULD ASK

- How do we create and verify identities for users?
- How do we ensure the right access for the right role?
- How do we remove or disable access when needed?
- Are we using strong authentication methods?
- How do we monitor and review access regularly?
- How do we manage identities for third parties?
- Do we have clear policies and responsibilities?

HOW TO BUILD STRONG IDENTITY MANAGEMENT

1. **Define Identity Requirements** — Identify who needs access, what they need access to, and why.
2. **Verify Identities Strongly** — Use reliable methods to verify identities before granting access.
3. **Apply Least Privilege Access** — Grant the minimum access necessary to perform job responsibilities.
4. **Use Strong Authentication** — Implement multi-factor authentication and strong password practices.
5. **Monitor and Review Access** — Regularly review access rights and monitor for unusual activities.
6. **Manage Identity Lifecycle** — Create, update, and remove identities promptly and consistently.
7. **Enforce Policies and Awareness** — Establish clear policies and train staff on identity security best practices.

GOOD PRACTICE CHECKLIST

- [x] We verify identities before granting access.
- [x] We use multi-factor authentication.
- [x] We apply role-based access and least privilege.
- [x] We review access rights regularly.
- [x] We promptly remove access when no longer needed.
- [x] We log and monitor identity-related activities.
- [x] We educate staff on identity security.

WARNING SIGNS

- Shared or generic accounts are in use.
- Users have more access than they need.
- Former staff or inactive users still have access.
- No multi-factor authentication in place.
- Access reviews are not done regularly.
- Unusual access activity is not investigated.
- No clear identity management policy.