NZ INFOSEC
SECURITY COMPLIANCE

ISO 27001

INFORMATION SECURITY MANAGEMENT SYSTEM

INTRODUCTION

- ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements.”
- ISO 27001 was developed to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).
- There are 114 controls in in ISO 27001:2013 standard
- ISO – International Organization for Standardization
    - An independent and non-governmental organization with 164 member countries.
    - World's largest developer of voluntary international standards.
    - Developed more than 20,000 standards for all industries e.g., manufacturing, technology etc.

ISO 27001:2013 BENEFITS

Comply with legal requirements
Laws, regulations and contractual requirements - can be resolved by implementing ISO 27001

Achieve marketing advantage
Advantage in the eyes of the customers who are sensitive about keeping their information safe
Increase in Trust with respect to partners, customers and public

Lower costs
By minimizing incidents and by mitigating the risks

Better organization
Process improvement e.g., HR security, secured development, physical security, assets control, information classification, proper inventory, Business Continuity planning and tests etc.

Minimization of IT risks and possible damage

Systematic detection of Vulnerabilities

REQUIREMENTS AND CONTROLS

ISO/IEC 27001 requirements	
4	Context of the organisation
5	Leadership
6	Planning
7	Support
8	Operation
9	Performance evaluation
10	Improvement

Annex A Controls (total 114 controls) – 14 Domains	
A5	Information security policies
A6	Organization of information security
A7	Human resource security
A8	Asset management
A9	Access control
A10	Cryptography
A11	Physical and environmental security
A12	Operations security
A13	Communications security
A14	System acquisition, development & maintenance
A15	Supplier relationships
A16	Information security incident management
A17	Information security aspects of BCM
A18	Compliance

CERTIFICATION STEPS / PLAN

1. Secure top management support
2. Buy the ISO 27001:2013 from ISO website
3. Appoint a staff for implementation of the ISO
4. Define the Context, Scope (Location, processes, products etc.),
5. Define objective of ISMS
6. Develop and publish information security policy
7. Conduct a risk assessment and risk mitigation plan
8. Complete the Statement of applicability
9. Conduct security awareness training for staff
10. Review and update the required documentation
11. Measure, monitor and review the effectiveness of the controls
12. Conduct internal audit and management review
13. Certification audit – by a Certified ISO 27001 Lead auditor

Steps 1 – 12 can take 1-3 months depending upon your company size and speed

CERTIFICATION AUDIT PROCESS

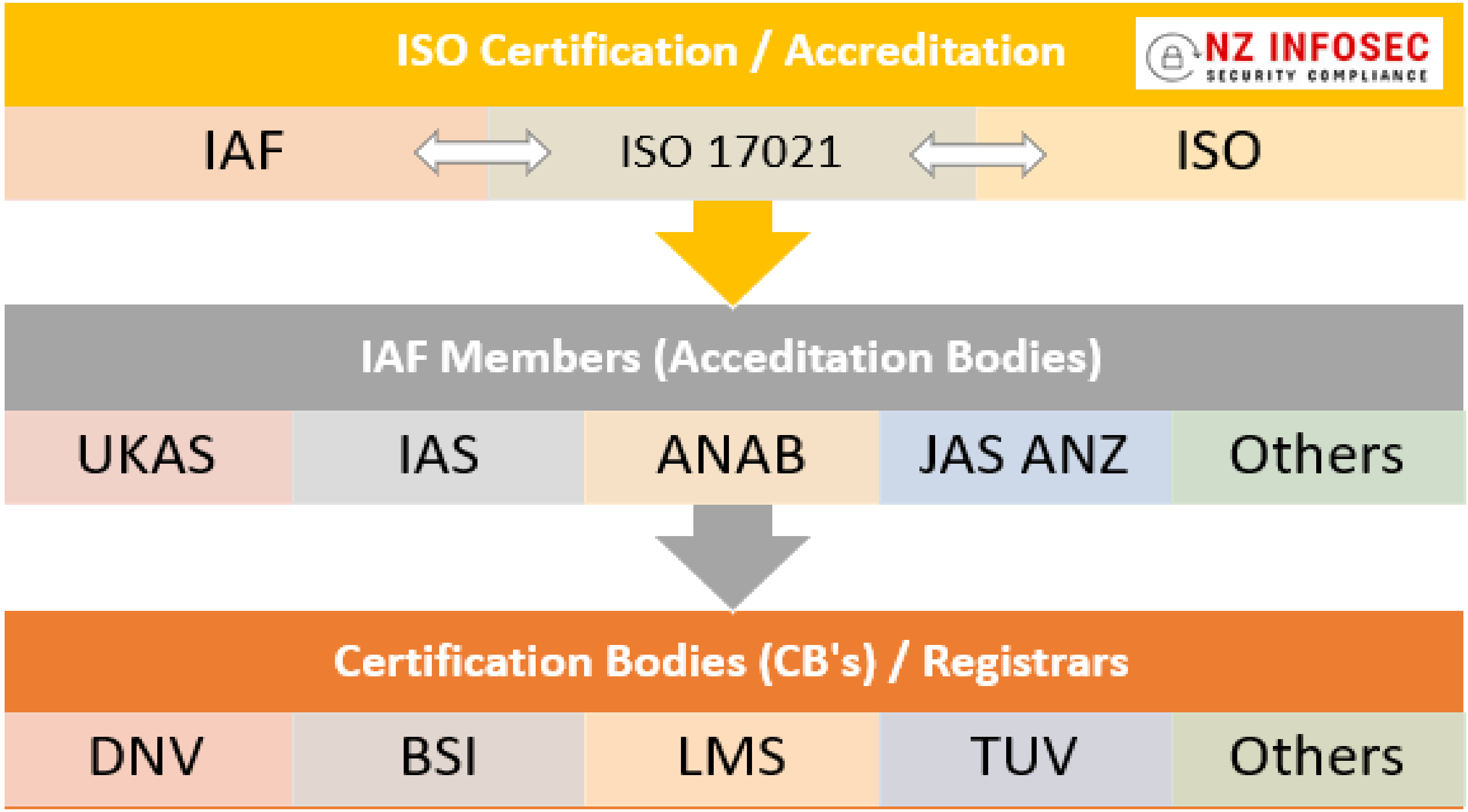
- ISO audits are done by IRCA UK Certified Lead Auditors / Certification Bodies.
- First stage audit - initial check on documentation, process, product and organisation information.
- Second stage audit - to check the implemented controls and its effectiveness.
- Both stage audits can be done online/remote or onsite.
- After the final audit, the certificate is issued by an accredited certification body, based in UK.
- All ISO certifications can be verified from the website of the certification body or registrar.
- ISO certification is valid for 3 years and re-certification is required every three years.
- Surveillance audit is required every year for the next two years.

Documents are not enough

RECORDS required

Training, operations, security, HR, networks, logs, suppliers etc.

CERTIFICATION PROCESS



ISO Certification / Accreditation

NZ INFOSEC SECURITY COMPLIANCE

IAF ⟺ ISO 17021 ⟺ ISO

IAF Members (Acceditation Bodies)

UKAS	IAS	ANAB	JAS ANZ	Others

Certification Bodies (CB's) / Registrars

DNV	BSI	LMS	TUV	Others

Thank You

Information Security Is Everyone’s Responsibility

www.nzinfosec.co.nz