Auditing Fundamentals

Frameworks and Maturity

Business Needs

Photo by Kindel Media from Pexels

Photo by Tom Fisk from Pexels

But how?

Frameworks

Frameworks

- ISO/IEC 27000
- COBIT
- NIST
- CIS
- CMMC
- ASD

ISO/IEC 27000

International Organization for Standardization and the International Electrotechnical Commission

- Deliberately broad in scope
- Covering more than just privacy, confidentiality and IT/technical/cybersecurity issues
- Applicable to organizations of all shapes and sizes

ISO/IEC 27000

International Organization for Standardization and the International Electrotechnical Commission

- ISO/IEC 27001
  - Information technology — Security Techniques — Information security management systems — Requirements
- ISO/IEC 27002
  - Code of practice for information security controls

COBIT

Control Objectives for Information and Related Technologies

- Created by ISACA for information technology (IT) management and IT governance
- Business focused and defines a set of generic processes for the management of IT

NIST Special Publication 800-53

National Institute of Standards and Technology

- Catalog of security and privacy controls for all U.S. federal information systems except those related to national security
- Agencies are expected to be compliant with NIST security standards and guidelines
- NIST Special Publication 800-53B provides a set of baseline security controls and privacy controls for information systems and organizations

CIS Controls and CIS Benchmarks

Center for Internet Security

- Set of 18 prioritized safeguards to mitigate the most prevalent cyber-attacks
- A defense-in-depth model to help prevent and detect malware
- Offers a free, hosted software product called the CIS Controls Self Assessment Tool (CIS-CSAT)

CMMC

Cybersecurity Maturity Model Certification

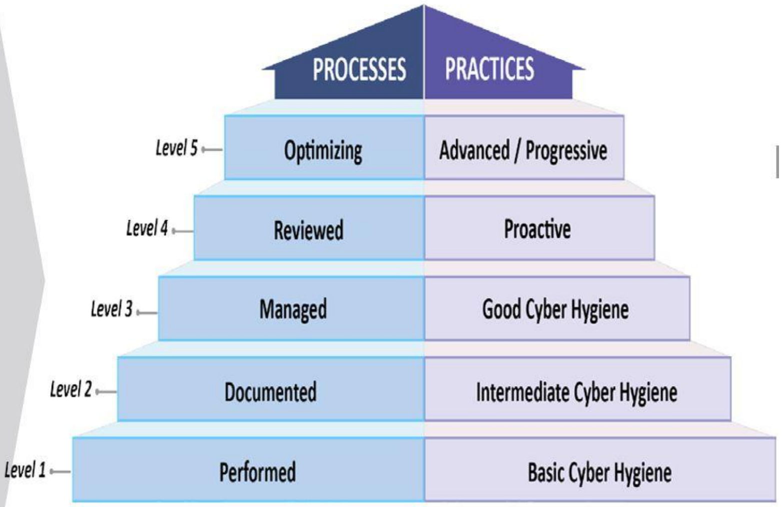
- A training, certification, and third party assessment program of cybersecurity in the United States government Defense Industrial Base
- Requires a third party assessor to verify the cybersecurity maturation level
- 5 levels

CMMC

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity



DISTRIBUTION A. Approved for public release

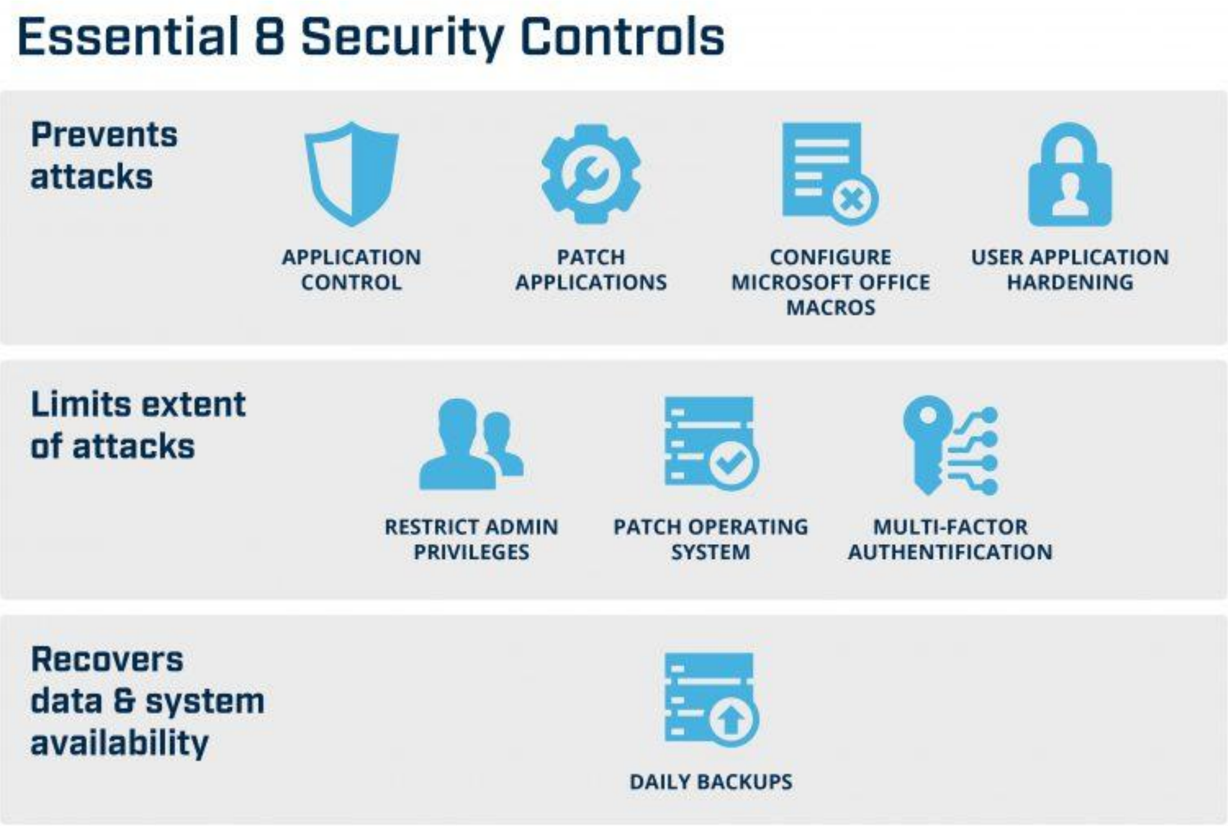
ASD Essential 8

Australian Cyber Security Centre
Essential Eight Maturity Model

- Help organisations protect themselves against various cyber threats
- Designed to protect Microsoft Windows-based internet-connected networks
- 4 maturity levels

Australian Government
Australian Signals Directorate

ASD Essential 8



Essential 8 Security Controls

Prevents attacks

- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING

Limits extent of attacks

- RESTRICT ADMIN PRIVILEGES
- PATCH OPERATING SYSTEM
- MULTI-FACTOR AUTHENTICATION

Recovers data & system availability

- DAILY BACKUPS

ASD Essential 8

The Essential Eight

- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING
- RESTRICT ADMIN PRIVILEGES
- PATCH OPERATING SYSTEM
- MULTI-FACTOR AUTHENTIFICATION
- DAILY BACKUPS

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

So What?

How to implement?