Top 25 Cybersecurity Frameworks.

G. M. Faruk Ahmed, CISSP, CISA, CDCP

www.gmfaruk.com

Top 25 Cybersecurity Frameworks to Consider for your cybersecurity program.

1. Australian Signals Directorate (ASD) Essential 8

ASD's Essential 8 takes a maturity model approach to cybersecurity, listing three levels. The eight essential strategies encompass:

- Setting and enforcing application controls
- Patching applications
- Configuring Microsoft Office Macro settings
- Hardening user applications
- Restricting administrative privileges
- Patching operating systems
- Using multi-factor authentication
- Ensuring daily backups

Each maturity level aligns with having specific controls within those eight strategies in place. Maturity Level One means the organization is "partly aligned." Maturity Level Two means an organization put additional controls in place to be "mostly aligned." Maturity Level Three means an organization has implemented all required controls and is "fully aligned."

2. Center for Internet Security (CIS) Controls

While some frameworks offer flexibility, others take a more prescriptive approach. Probably the cybersecurity framework most often cited by professionals, the CIS Controls framework lists twenty mission-critical controls across three categories:

- Basic
- Foundational
- Organizational

The CIS Controls framework then goes even further to define three implementation groups. Implementation Group 1 is for organizations with limited resources and cybersecurity expertise. Implementation Group 2 is for organizations with moderate resources and cybersecurity expertise. Implementation Group 3 is for mature organizations with significant resources and cybersecurity expertise.

Under each of the 20 controls, the CIS Controls framework provides a list of sub-controls, color-coded to indicate which implementation group should be using them. For example, CIS Control 1 "Inventory and Control of Hardware Assets" lists sub-control "Utilize an Active Discovery Tool" is appropriate for Implementation Groups 2 and 3 but considered too much of a burden for Group 1.

3. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Consisting of 197 control objectives organized into 17 domains, the CCM focuses solely on cloud computing. The 17 domains include:

- Audit & Assurance
- Application & Interface Security
- Business Continuity Management & Operational Resilience
- Change Control & Configuration Management
- Cryptography, Encryption & Key Management
- Datacenter Security
- Data Security & Privacy Lifecycle Management
- Governance, Risk Management & Compliance
- Human Resources
- Identity & Access Management
- Interoperability & Portability
- Infrastructure & Virtualization Security
- Logging & Monitoring
- Security Incident Management, E-Discovery, & Cloud Forensics
- Supply Chain Management, Transparency & Accountability
- Threat & Vulnerability Management
- Universal Endpoint Management

Within each domain, CCM lists controls and specifications to help organizations create a compliant security program.

4. Control Objectives for Information Technology (COBIT)

The Information Systems Audit and Control Association (ISACA) updated its COBIT framework in 2019 to create a Governance System and Governance Framework. Instead of basing compliance on individual security controls, COBIT 2019 starts with stakeholders' needs, assigns job-related governance responsibilities to each type, then maps the responsibility back to technologies. Ultimately, COBIT's goal is to ensure appropriate oversight of the organization's security posture.

The COBIT core model groups governance and management objectives into five domains:

- EDM: Evaluate, Direct, and Monitor
- APO: Align, Plan, and Organization
- BAI: Build, Acquire, and Implement
- DSS: Deliver, Service, and Support
- MEA: Monitor, Evaluate, and Assess

COBIT's design principles include:

- Understanding the enterprise strategy

- Scoping the governance system
- Refining the scope
- Completing the design

Ultimately, COBIT's focus on governance creates a security framework that streamlines audits and incorporates continuous improvement to enhance those outcomes.

5. Cybersecurity and Infrastructure Security Agency (CISA) Transporation Systems Sector (TSS) Cybersecurity Framework

The Department of Transportation, Transportation Security Administration, United States Coast Guard, and Transportation Systems Sector worked together to create a framework that addressed industry-specific needs. Based on NIST's Cybersecurity Framework, the TSS Cybersecurity Framework focuses on five discrete TSS strategy goals:

- Define Conceptual Environment
- Improve and Expand Voluntary Participation
- Maintain Continuous Cybersecurity Awareness
- Enhance Intelligence and Security Information Sharing
- Ensure Sustained Coordination and Strategic Implementation

It aligns each goal to the appropriate NIST categories. For example, "Ensure Sustained Coordination and Strategic Implementation" aligns with NIST's "Business Environment Governance." The TSS Cybersecurity Framework takes a risk-based and maturity model approach, allowing organizations to apply threat intelligence to determine security breach impact. By defining low, moderate, and high impact levels, organizations can prioritize the next steps to reduce the risk profile.

6. Cybersecurity Maturity Model Certification (CMMC)

The Office of the Under Secretary of Defense Acquisition and Sustainment (OUSD(A&S)) worked with Department of Defense (DoD) stakeholder, University Affiliated Research Centers (UARCs), and Federally Funded Research and Development Centers (FFRDC) to standardize cybersecurity across the Defense Industrial Base (DIB).

Unlike other maturity models, CMMC is both a set of best practices and a requirement for organizations that solicit DoD contracts. CMMC lists five maturity levels, primarily based on whether the data an organization collects, transmits, stores, and processes is Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

The five certification levels are:

- Level 1: Basic safeguarding of FCI and basic cyber hygiene
- Level 2: Documenting and processes the transition phase to prove intermediate cyber hygiene practices for FCI and CUI

- Level 3: Establishing basic CUI protections, managing processes, and developing good cyber hygiene practices
- Level 4: Increasing security over CUI, reducing advanced persistent threat (APT) risks, reviewing processes, and establishing proactive practices
- Level 5: Furthering risk reduction around APTs, optimizing processes, and establishing advanced/progressive practices

As an organization's maturity level increases, so do the required controls' number and sophistication level. At Maturity Level 1, an organization only needs seventeen practices. Meanwhile, an organization that needs to meet Maturity Level 5 compliance needs 173 practices in place.

7. European Telecommunications Standards Institute (ETSI)

ETSI is a non-profit standards organization with more than 900 members from across 65 countries and five continents. A European Standards Organization (ESO), ETSI supports European regulations and legislation by creating standards used throughout the EU.

Technical Report (TR) 103 305-1 "Critical Security Controls for Effective Cyber Defence." ETSI based the top twenty Enterprise industry level cybersecurity best practices on the Critical Security Controls (CSC) CIS established. However, unlike the CIS Critical Controls, ETSI does not divide activities into Implementation Groups. The "Critical Security Controls for Effective Cyber Defence" includes the following for each of the twenty controls:

- Control name
- Explanation of control criticality
- Table with detailed control descriptions
- Procedures and tools
- System entity relationship diagram

8. European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework

Published on December 7, 2020, the ENISA National Capabilities Assessment Framework provides the Member States a way to engage in self-assessments so that they can identify their maturity level. The framework offers a way for countries to assess their cybersecurity capabilities, ultimately giving them guidelines for setting national strategies.

The Framework outlines the following benefits that come from engaging in a national assessment:

- Useful information for developing long-term strategies
- Identifying gaps in cybersecurity programs
- Opportunities for enhancing cybersecurity capabilities
- Supporting political accountability
- Establishing public and international credibility

- Creating a public image of transparency
- Heling anticipate future issues
- Identifying lessons learned and best practices
- Providing a cybersecurity baseline across the EY
- Evaluating national cybersecurity capabilities

9. Factor Analysis of Information Risk (FAIR) Cyber Risk Framework

The FAIR Institute is a nonprofit organization whose mission is to establish and promote risk management best practices so that risk professionals can collaborate better with their business partners.

The FAIR cyber risk framework takes an explicit approach to cyber risk management so that organizations can quantify risk regardless of the cybersecurity framework they use. According to FAIR, an implicit risk management approach starts with a compliance requirement and aligns controls to it, creating a reactive risk posture. Meanwhile, FAIR's explicit approach creates a cycle of continuous improvement integrating risk targets, controls, and a proactive risk posture.

FAIR creates a risk management system focused on:

- Defining costs: the three elements of which are achievement, maintenance, and acceptable loss exposures
- Building a foundation: the five elements of which are cost-effective risk management, well-informed decisions, effective comparisons, meaningful measurements, and accurate models
- Implementing the program: the three elements of which are the risk that drives loss exposure, risk management decisions, and feedback loop for improvement

10. HITRUST Cybersecurity Framework (CSF)

To help healthcare organizations and their business associates find a more flexible way to meet Health Insurance Portability and Accountability Act (HIPAA) compliance, HITRUST offers an integrated risk and compliance approach.

Privacy, information security, and risk management leaders across the public and private sectors worked together to establish a set of safeguards for protecting the security and privacy of protected health information (PHI) and electronic PHI (ePHI). The HITRUST CSF consists of 49 control objectives across 156 control specifications, all of which fall into one of the following 14 control categories:

- Information security management program
- Access control
- Human resources security
- Risk management
- Security policy
- Organization of information security

- Compliance
- Asset management
- Physical and environmental security
- Communications and operations management
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Privacy practices

11. Information Security Forum (ISF) Standard of Good Practice for Information Security (SOGP 2020)

The ISF is a no-profit organization whose members consist of companies on the Fortune 500 and Forbes 2000 lists. The organization focuses on creating a knowledge exchange where members share security issues, experiences, and practical solutions.

The SOGP 2020 provides a set of best practices intended to:

- Improve resilience
- Provide a foundation for information risk assessments
- Validate information security across the supply chain
- Support compliance with major industry standards
- Form a basis for policies, standards, and procedures

12. International Society of Automation (ISA/IEC 62443)

Founded in 1945, ISA is a non-profit professional association that established a Global Security Alliance (GSA) to work with manufacturers and critical infrastructure providers. GSA incorporates various stakeholders, including end-user companies, automation and control systems providers, IT infrastructure providers, services providers, and system integrators.

ISA/IEC 62443 is an industrial security framework focused on both traditional IT environments and SCADA or plant floor environments and includes:

- Defining risk and vulnerability analysis methodologies
- Defense-in-depth security model
- Zone/conduit security model
- Risk mitigation techniques like anti-virus, patch management, firewalls, and virtual private networks (VPNs)

13. International Telecommunications Union (ITU) National Cybersecurity/ Critical Information Infrastructure Protection (CIIP)

Recognizing the increasing importance of information and communication technologies (ICTs) to national security, economic well-being, and social cohesion, ITU created its CIIP as a model

for sharing the responsibility between government, business, other organizations, and individual users.

The CIIP sets forth the following key elements that a national cybersecurity strategy should include:

- Government/Private Sector collaboration: Cooperate across all stages of development to share incident response information and address common concerns
- Incident management capabilities: Identify national and international public and private parties who will cooperate in developing tools and procedures for protecting cyber resources, disseminating incident management information, establishing integrated risk management processes, and assessing and re-assessing program effectiveness
- Legal infrastructure: Establish cybercrime authorities and procedures as well as any additional legal infrastructures necessary
- Culture of Cybersecurity: Implement a cybersecurity plan for government-operated systems, promote a comprehensive national awareness program, support outreach to children and individual users, enhance research, and identify training requirements

14. Internet of Things (IoT) Cybersecurity Alliance (IOTCA)

The IoTCA's mission is to forge a community that brings together cybersecurity and IoT experts so that they can address real-world IoT security issues and work to establish a security-first IoT posture.

Their framework takes a multi-layered approach to create end-to-end security, taking into account all connected devices and their associated applications. The framework includes:

- Endpoint layer: devices/connected objects, short-range networks
- Network layer: communications network
- Data/App layer: applications

Their goal is to mitigate risks such as:

- Resource limitations
- Malware
- Device cloning
- Lak of monitoring
- Protocol tampering
- Man-in-the-middle attack
- Denial of Service
- Unauthorized software
- Unauthorized access

15. Internet of Things (IoT) Security Foundation (IoTSF) Security Compliance Framework

The IoTSF is a non-profit international organization that brings together IoT security professionals, IoT hardware and software product vendors, network providers, system specifiers, integrators, distributors, retailers, insurers, local authorities, and government agencies.

They focus on securing IoT during the design phase to mitigate financial and brand reputation risk. The IoTSF Security Compliance Framework released in May 2020 takes a risk-based approach to compliance and focuses on six key issues:

- Management governance
- Engineered for security
- Fit for purpose cryptography
- Secure network framework and applications
- Secure production processes and supply chains
- Safe and secure for the customer

16. International Office of Standardization (ISO) 27001

ISO represents one of the oldest standards organizations. Founded in 1947, this non-governmental organization has members from 165 countries. ISO sets standards for various technologies, including several security standards. The ISO/IEC 27000 "family" boasts over a dozen standards, but ISO 27001 sets the foundation for establishing an information security management system (ISMS).

ISO 27001 includes requirements for establishing, implementing, maintaining, and continually improving an ISMS influenced by the organization's needs, objectives, security requirements, processes, size, and structure. Its best practices include setting controls and processes based on:

- Organization context
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

As part of establishing an ISMS, organizations need to consider additional ISO 27000 family standards such as:

- ISO/IEC 27002:2013 - Code of practice for information security controls
- ISO/IEC 27003 - Information security management system implementation guidance
- ISO/IEC 27004 - Information security management - Measurement
- ISO 31000:2009 - Risk Management - Principles and guidelines

17. MITRE ATT&CK

The non-profit, federally funded MITRE is a cybersecurity-focused research and development center. When MITRE began documenting common cyberattack tactics, techniques, and procedures (TTPs) used against Windows enterprise networks, ATT&CK became the baseline acting as a common language for offensive and defensive researchers. MITRE is responsible for establishing and trademarking the Common Vulnerabilities and Exposures (CVE) list.

MITRE Enterprise has 14 tactics commonly used when malicious actors set up advanced persistent threats (APTs) within a corporate ecosystem. Each of the following 14 tactics is then broken down into specific activities:

- Reconnaissance
- Resource development
- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and control
- Exfiltration
- Impact

In response to the increasing use of mobile devices, MITRE created the Mobile matrix to help security staff better track emerging threats. The 14 MITRE mobile tactics, again divided into sub-categories, are:

- Initial access
- Execution
- Persistent
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and control
- Exfiltration
- Impact

18. National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)

The United Kingdom's NCSC launched in 2016 and brings together SMEs, enterprise organizations, government agencies, the general public, and departments to address cybersecurity concerns.

Its CAF provides guidance for UK Critical National Infrastructure (CNI), organizations subject to the NIS Directive cyber regulation, and organizations managing cyber-related risks to public safety. CAF guides organizations toward establishing a cyber resiliency program, focusing on outcomes rather than checklists.

It has four primary objectives:

- A: Managing security risk
- B: Protecting against cyber attacks
- C: Detecting cybersecurity events
- D: Minimising the impact of cybersecurity incidents

It embeds 14 subparts within these four primary objectives, many aligned with other international standards. These subparts are:

- A.1: Governance
- A.2 Risk management
- A.3: Asset management
- A.4: Supply chain risk management
- B.1: Service protection policies and processes
- B.2: Identity and access control
- B.3: Data security
- B.4 System security
- B.5: Resilient networks and systems
- B.6: Staff awareness and training
- C.1: Security monitoring
- C.2: Practice security event discovery
- D.1: Response and recovery planning
- D.2: Lesson learned

19. New Zealand Protective Security Requirements (PSR)

New Zealand's PSR creates a policy framework for how organizations should manage security governance (GOVSEC), personnel (PERSEC), information (INFOSEC), and physical security (PHYSEC) across the public and private sectors.

The four-tiered, hierarchical structure requires organizations to:

- Establish a strategic security directive
- Set core policies and mandatory requirements

- Follow protocols and best-practice guidance
- Establish and review organizational policies, plans, and procedures

Across the four key areas it lays out 32 focus areas:

- GOV 1 - Establish and maintain the right governance
- GOV 2 - Take a risk-based approach
- GOV 3 - Prepare for business continuity
- GOV 4 - Build security awareness
- GOV 5 - Manage risks when working with others
- GOV 6 - Manage security incident
- GOV 7- Be able to respond to increased threat levels
- GOV 8 - Assess your capability
- PERSEC 1 - Recruit the right person
- PERSEC 2 - Ensure their ongoing suitability
- PERSEC 3 - Manage their departure
- PERSEC 4 - Manage national security clearances
- PHYSEC 1 - Understand what you need to protect
- PHYSEC 2 - Design your physical security
- PHYSEC 4 - Keep your security up to date
- INFOSEC 1 - Understand what you need to protect
- INFOSEC 2 - Design your information security
- INFOSEC 3 - Validate your security measures
- INFOSEC 4 - Keep your security up to date

20. National Institute of Technologies (NIST) Cybersecurity Framework (CSF)

NIST is a US non-regulatory government agency that sets standards across the physical sciences. Originally intended for critical infrastructure owners and operators, NIST CSF can be used by any organization. Many companies outside of the critical infrastructure industry also use the CSF, especially if they need to meet other US federal data protection requirements.

The CSF consists of three sections:

- Framework Core
- Implementation Tiers
- Framework Profiles

The Framework Core consists of five functions with categories and subcategories embedded within them. The Framework Core Functions are:

- Identify (ID): develop a cybersecurity risk management approach that identifies all systems, people, assets, data, and capabilities.
- Protect (PR): Develop and implement safeguards to ensure critical services delivery
- Detect (DE): Develop and implement activities that identity a cybersecurity event occurrence

- Respond (RS):
- Recover (RC)

The four Implementation Tiers are:

- Tier 1: Partial
  - Ad hoc risk management practices
  - Organizational-level cybersecurity risk awareness
  - No sense role within the larger ecosystem
- Tier 2: Risk-Informed
  - Management approved risk management processes but not set as organizational policy
  - Organizational-level cybersecurity risk awareness but no organization-wide risk management approach
  - Understands role either of its own dependencies or dependents within the ecosystem
- Tier 3: Repeatable
  - Formally approved risk management practices expressed as policy
  - Organization-wide risk management policies, processes, and procedures
  - Understands role, dependencies, and dependents in the larger ecosystem and collaborates with other entities
- Tier 4: Adaptive
  - Adapts cybersecurity practices based on cybersecurity activities including lessons learned and predictive indicators
  - Organization-wide risk management policies, processes, and procedures that address potential cybersecurity events
  - Understands role, dependencies, and dependent within the larger ecosystem and contributes to broader community understanding of risks

21. NIST Special Publication (SP) 800-82 Guide to Industrial Control Systems (ICS) Security

In order to address the unique cybersecurity concerns facing ICS, NIST SP 800-82 provides guidance for supervisory control and data acquisition (SCADA) systems, distributed control systems (IDS), and other control system configurations found in the industrial control sectors, like Programmable Logic Controls (PLC).

To protect ICS, NIST suggests a defense-in-depth strategy, including:

- ICS specific security policies, procedures, and training
- Policies and procedures aligned with Homeland Security Advisory System Threat Level
- ICS lifecycle security considerations across architecture design, procurement, installation, maintenance, and decommissioning
- Logical separation between corporate and ICS networks
- DMZ network architecture
- Critica component redundancy across redundant networks
- Graceful degradation (fault-tolerant) critical system design

- ICS device unused port and services disablement
- ICS network and device physical access restrictions
- ICS user privileges restricted according to the principle of least privilege
- Separate authentication and user credentials for ICS and corporate network access
- Modern technology such as a smart card for Personal Identity Verification (PIV)
- Security control implementation including intrusion detection, anti-virus, and file integrity checking software
- Security techniques for ICS data storage and communications, such as encryption or cryptographic hashes
- Audit trail documentation for ICS critical areas
- Reliable and secure network protocols and services

22. North American Electric Reliability Corporation (NERC)

NERC is a non-profit international regulatory authority focused on effectively and efficiently reducing risks facing the grid system. Its jurisdiction includes bulk power system users, owners, and operators.

NERC currently has 19 approved security guidelines across the following areas:

- Cloud computing
- Control systems electronic connectivity
- Open-source software
- Physical security
- Physical security response
- Provenance
- Risk management life cycle
- Secure equipment delivery
- Cloud solutions and encrypting
- Vendor incident response
- Vendor risk management lifecycle

23. OASIS Security Assertion Markup Language (SAML)

OASIS Open is a community where experts can advance projects, including open source projects, for cybersecurity, blockchain, IoT, emergency management, cloud computing, and legal data exchange.

SAML is a standard that defines a framework for exchanging security information between online business partners. Developed by the Security Services Technical Committee, SAML is an XML-based framework that supports business communications for user authentication, entitlement, and attribute information. Organizations can apply it to human and machine entities, partner companies, or other enterprise applications. Organizations most often use SAML for web single-sign-on (SSO), attribute-based authorization, and securing web services.

SAML consists of four main components:

- Assertions: Information that includes authentication, attribute, and authorization decisions
- Protocols: Request/response protocols that help identity providers manage user requests to resources
- Bindings: Mappings of request-response message exchanges to standard messaging or communication protocols
- Profiles: Definitions that show how SAML can be used within a particular application as a way to promote interoperability

24. Payment Card Industry Data Security Standard (PCI DSS)

Founded in 2006 as a response to increased credit card fraud, the Payment Card Industry Security Standards Council (PCI SSC) consists of the five major credit card companies, American Express, Discover, JCB International, Mastercard, and Visa, Inc. The Payment Card Industry Data Security Standard (PCI DSS) is a prescriptive security compliance requirement for merchants and financial services providers.

PCI DSS contains 5 categories of controls:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Within those 5 categories, PCI DSS then sets out 12 detailed requirements:

- Install and main a firewall configuration
- Do not use vendor-supplied defaults
- Protect stored cardholder data
- Encrypt cardholder data transmissions across open, public networks
- Protect all systems again malware
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need to know
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain an information security policy

25. Saudi Arabian Monetary Authority (SAMA) Cybersecurity Framework

In May 2017, the Saudi Arabian Monetary Authority (SAMA) issued Version 1.0 of its Cyber Security Framework (SAMA CSF). In the introduction, SAMA noted that applying new online services and new developments, such as fintech, and blockchain, require additional regulatory standards to protect against continuously evolving threats.

SAMA explained its Framework's objectives as:

1. To create a common approach for addressing cybersecurity within the Member Organizations.
2. To achieve an appropriate maturity level of cybersecurity controls within the Member Organizations.
3. To ensure cybersecurity risks are properly managed throughout the Member Organizations.

The SAMA CSF defines its scope as:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services, and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment, and communication networks (technical infrastructure).

Additionally, it focuses more broadly than other financial cybersecurity frameworks by incorporating applicability to the following industries:

- All Banks operating in Saudi Arabia;
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia;
- All Financing Companies operating in Saudi Arabia;
- All Credit Bureaus operating In Saudi Arabia;
- The Financial Market Infrastructure