وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

معايير أمن المعلومات والأمن السيبراني

Information Security Standards And CYBERSECURITY STANDARDS

تعريف معايير الأمن السيبراني:

- معايير الأمن السيبراني هي مجموعة من المتطلبات والتوصيات التي تهدف إلى حماية الأصول الرقمية من الهجمات الإلكترونية.
- تحدد هذه المعايير الضوابط والإجراءات التي يجب على المؤسسات اتخاذها لتحسين أمنها السيبراني.

مهام الأمن السيبراني التي يمكن أن تساعد في تحقيقها معايير الأمن السيبراني:

- تحديد الأصول وتقييم المخاطر: تساعد معايير الأمن السيبراني المؤسسات على تحديد الأصول الرقمية التي تحتاج إلى الحماية، وتقييم المخاطر التي تتعرض لها هذه الأصول.
- تطوير وتنفيذ ضوابط الأمن: توفر معايير الأمن السيبراني مجموعة واسعة من الضوابط التي يمكن للمؤسسات استخدامها للحماية من الهجمات الإلكترونية.
- مراقبة واختبار الامتثال: تساعد معايير الأمن السيبراني المؤسسات على مراقبة واختبار امتثالها للضوابط الأمنية.
- إدارة الحوادث: توفر معايير الأمن السيبراني إرشادات حول كيفية إدارة الحوادث الأمنية.
- بشكل عام، يمكن أن تساعد معايير الأمن السيبراني المؤسسات في تحقيق الأمن السيبراني من خلال توفير إطار عمل ومجموعة من الموارد التي يمكن استخدامها لتحسين حماية الأصول الرقمية.

أهم معايير الأمن السيبراني الدولية:

- ISO/IEC 27001
- ISO/IEC 27002
- NIST CYBERSECURITY FRAMEWORK
- CIS CONTROLS
- OWASP

- ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

- معيار دولي لأنظمة إدارة أمن المعلومات
  - يوفر هذا المعيار إطارًا للمؤسسات لتطبيق ممارسات أمن المعلومات الجيد.
  - يعتمد على نظرية الدكتور دايمنق للتطوير المستمر
  - يحتوي على 11 فقرة موزعة كالاتي :

1- المقدمة
2- النطاق
3- المراجع المعيارية
4- الشروط و المصطلحات
5- السياق
6- القيادة
7- التخطيط
8- الدعم
9- التشغيل
10- تقييم الأداء
11- التحسين

- كما يحتوي على الملحق (A) الخاص بمرجع ضوابط أمن المعلومات المعيارية
- Annex A Information security controls reference
- 93 ضابط (CONTROL) مقسمة على 4 مواضيع (THEMS)
  - 37 الضوابط التنظيمية ORGANIZATIONAL CONTROLS
  - 8 الضوابط المتعلقة بالأفراد PEOPLE CONTROLS
  - 14 الضوابط المادية PHYSICAL CONTROLS
  - 34 الضوابط الفنية TECHNICAL CONTROLS

- **5.2 Policy**
- Top management shall establish an information security policy that:
- a) is appropriate to the purpose of the organization;
- b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
- c) includes a commitment to satisfy applicable requirements related to information security;
- d) includes a commitment to continual improvement of the information security management system.
- The information security policy shall:
- e) be available as documented information;
- f) be communicated within the organization;
- g) be available to interested parties, as appropriate.


Terms & Conditions 3
4 Context
5 Leadership
Normative ref. 2
6 Planning
Scope 1
Intro 0
PLAN
7 Support
10. Improvement
ACT
ISO
27001:2022
DO
CHECK
8 Operation
9 Performance Evaluation

ISO/IEC27002

Information security, cybersecurity and privacy protection — Information security controls

يوفر هذا المعيار إرشادات و افضل الممارسات لتنفيذ ضوابط الأمن السيبراني التي وردت في الملحق الخاص بالمعيار 27001

ISO/IEC 27002:2022

Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard

Bibliography

7 Physical controls

A Attributes

B Mapping to ’27002:2013

5 Organizational controls

8 Technological controls

6 People controls

Key

Formalities

Mgmt

Human

IT/cyber

Physical

Annex

N Clause №

ISO/IEC27002

5- Organizational controls

5.1 Control

Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

NIST - CYBER SECURITY FRAMEWORK

معايير الأمن السيبراني NIST هي مجموعة من المبادئ والممارسات التي تهدف إلى حماية المعلومات والأنظمة والشبكات من الهجمات الإلكترونية. تم تطوير هذه المعايير من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة، وهي معتمدة من قبل العديد من الحكومات والشركات في جميع أنحاء العالم.

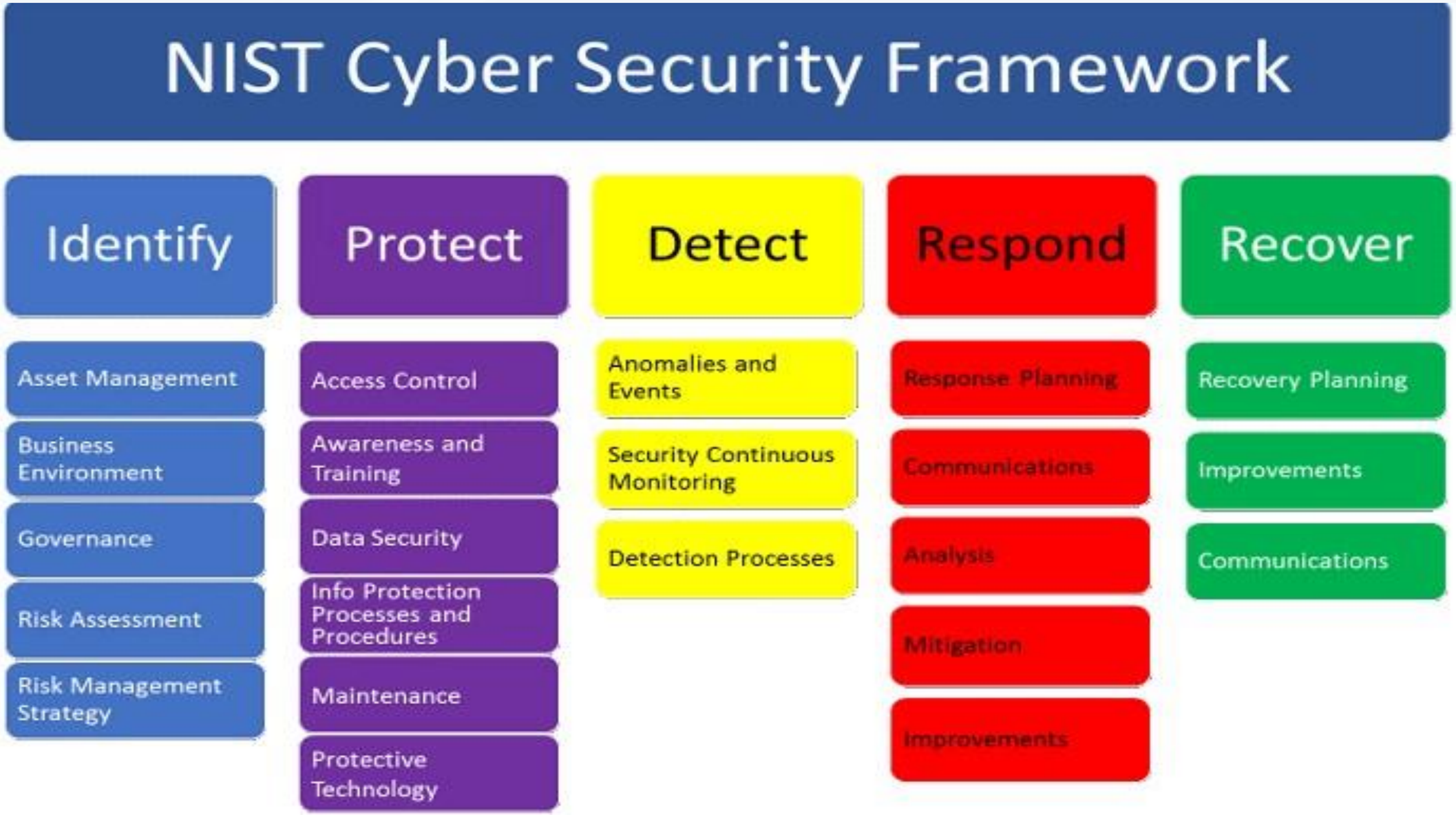
يوفر هذا المعيار إطارًا شاملًا يمكن استخدامه من قبل أي مؤسسة لتحسين أمنها السيبراني. فهي مرنة بما يكفي للتكيف مع أي حجم أو صناعة، وهي سهلة الفهم والتنفيذ.

فيما يلي بعض من أهم مزايا معايير الأمن السيبراني NIST:

- الشمولية: تغطي معايير الأمن السيبراني NIST جميع جوانب الأمن السيبراني، من تحديد المخاطر إلى الاستجابة للهجمات.
- القابلية للتطبيق: يمكن استخدام معايير الأمن السيبراني NIST من قبل أي مؤسسة، بغض النظر عن حجمها أو صناعتها.
- السهولة في الاستخدام: تم تصميم معايير الأمن السيبراني NIST لتكون سهلة الفهم والتنفيذ.

يمكن أن تساعد معايير الأمن السيبراني NIST المؤسسات على تحقيق الأهداف التالية:

- حماية المعلومات الحساسة من الهجمات الإلكترونية.
- الامتثال للقوانين واللوائح التنظيمية.
- تحسين الكفاءة التشغيلية.
- تعزيز الثقة لدى العملاء والشركاء.


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

Center of Internet Security - مركز أمن الانترنت

- هو منظمة غير ربحية تُعنى بتطوير وتعزيز أفضل الممارسات للأمن السيبراني. يُعرف مركز امن الانترنت بمجموعة التحكمات الأمنية 18 (CIS Controls)، وهي مجموعة من 18 إجراءً أمنيًا يتم اعتمادها على نطاق واسع من قبل المنظمات من جميع الأحجام.
- يطور مركز امن الانترنت وينشر أيضًا معايير CIS، وهي توصيات تكوينية وصفية لأكثر من 25 عائلة من منتجات البائعين. تساعد معايير CISالمنظمات على تقوية أنظمتها وتقليل مخاطرها من الهجمات الإلكترونية.

CIS CONTROLS

CONTROL		SAFEGUARDS	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	2/5	2/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Manager	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

OWASP : وهي منظمة غير ربحية مكرسة لتحسين أمن تطبيقات الويب

. تقدم OWASP مجموعة متنوعة من الموارد والأدوات والبرامج التعليمية لمساعدة المطورين والشركات على حماية تطبيقات الويب الخاصة بهم من الهجمات الإلكترونية.

تشمل بعض الموارد التي تقدمها OWASP ما يلي:

- **OWASP Top 10**: قائمة بالأهم عشرة مخاطر أمنية لتطبيقات الويب.
- **OWASP Application Security Verification Standard (ASVS):** معيار لاختبار أمن تطبيقات الويب.
- **OWASP Cheat Sheet Series:** مجموعة من النشرات الإرشادية التي توفر نصائح وحيل لتحسين أمن تطبيقات الويب.
- **OWASP Developer Guide:** دليل للمطورين لإنشاء تطبيقات ويب أكثر أمانا

OWASP Top 10 - 2021

A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A010:2021	Server-Side Request Forgery

الخلاصة

من خلال دراسة معايير الامن السيبراني المختلفة نلاحظ ما يلي:

1) الامن السيبراني موضوع اداري وتنظيمي قبل ان يكون فني.
2) يجب ان تلتزم الإدارة العليا في جميع الجهات برعاية برنامج الامن السيبراني وتبين ذلك بالأدلة والدعم والا لن ينجح برنامج الامن السيبراني في تلك الجهة.
3) الامن المادي (العام) وامن الموارد البشرية جزء لا يتجزأ من الامن السيبراني في أي جهة.
4) يجب اعتماد مفهوم التحسين والتطوير المستمر عند اعداد وتنفيذ برنامج الامن السيبراني.
5) التعاون بين الجهات مع بعضها فيما يخص الامن السيبراني وتبادل الخبرات عامل مهم في نجاح برنامج الامن السيبراني العام للحكومة.
6) التدريب والتوعية من اهم ضوابط الامن السيبراني وعامل حاسم في نجاحه.