CANADA'S
National Research &
Education Network

INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK (CSF)

Agenda

- NIST – A brief history
- What is a Security Framework?
- NIST CSF described
- Maturity model
- Self-assessment
- Delegation

CANADA'S National Research & Education Network

CANADA'S National Research & Education Network

NIST: A Brief History

- NIST = National Institute of Standards and Technology
- Founded in 1901 to establish "an authoritative domestic measurement and standards laboratory" in the US
- NIST created standards for:
  - electricity
  - length and mass
  - temperature
  - light
  - Time
- Created the means to transfer those values to the public

THE EVENING STAR, MONDAY, MARCH 11, 1901

CORRECT MEASURES

Function of the New Bureau of Standards.

LABORATORY TO BE ERECTED

Prof. Stratton, the Director, Details Need of Establishment.

A HANDICAP REMOVED

A new bureau of the government, authorized by the last Congress, will be established in this city in the near future and will give employment to a number of persons. It is to be known as the national bureau of standards and is to be under the control of the Treasury Department. A separate building for a laboratory, to cost not to exceed $250,000, is to be erected on a site to be purchased at a cost of $25,000.

Mr. Samuel W. Stratton of Chicago has been appointed by the President to be chief of the bureau at an annual salary of $5,000. Prof. Stratton is to have the following assistants, to be appointed by the Secretary of the Treasury: One physicist, at an annual salary of $3,500; one chemist, at $3,500; two assistant physicists or chemists, each at an annual salary of $2,200; one laboratory assistant, at $1,400; one laboratory assistant, at $1,200; one secretary, at $2,000; one clerk, at $1,200; one messenger, at $720; one en-

Director Stratton.

CANADA'S National Research & Education Network

NIST began formalizing its Information Technology (IT) publications around 1977. They currently deal with...

Artificial intelligence
Biometrics
Cloud computing & virtualization
Complex systems
Computational science
Conformance testing
Cyber-physical systems
Cybersecurity
Data & informatics
Federal information standards (FIPS)
Health IT
Internet of Things (IoT)
Interoperability testing
Mobile
Networking
Privacy
Software research
Usability & human factors
Video analytics
Virtual / augmented reality
Visualization research
Voting systems

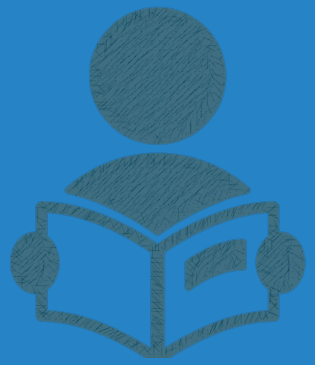
The first official Cybersecurity Publication:

Audit and Evaluation of Computer Security

OCTOBER 1, 1977

AUTHOR(S): ZELLA G. RUTHBERG, ROBERT G. MCKENZIE

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop on "Audit and Evaluation of Computer Security," held in Miami Beach, Florida on March 22-24, 1977. Its purpose was to explore the

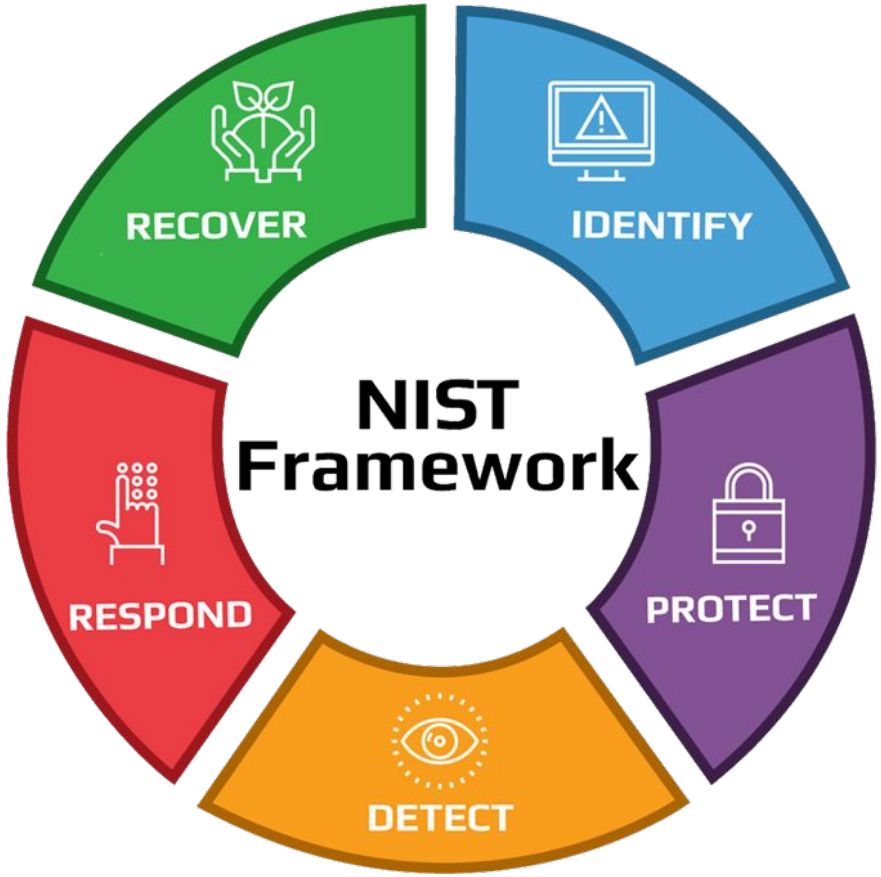


+ 340 cybersecurity-related publications providing guidance to security professionals.

https://csrc.nist.gov/publications/sp800

Why the NIST Cybersecurity Framework (CSF)?

- Selected by the National Research and Education Network
- Canadian Government includes it on their critical path towards enterprise security maturity
- Many businesses in Canada and elsewhere leverage the NIST CSF



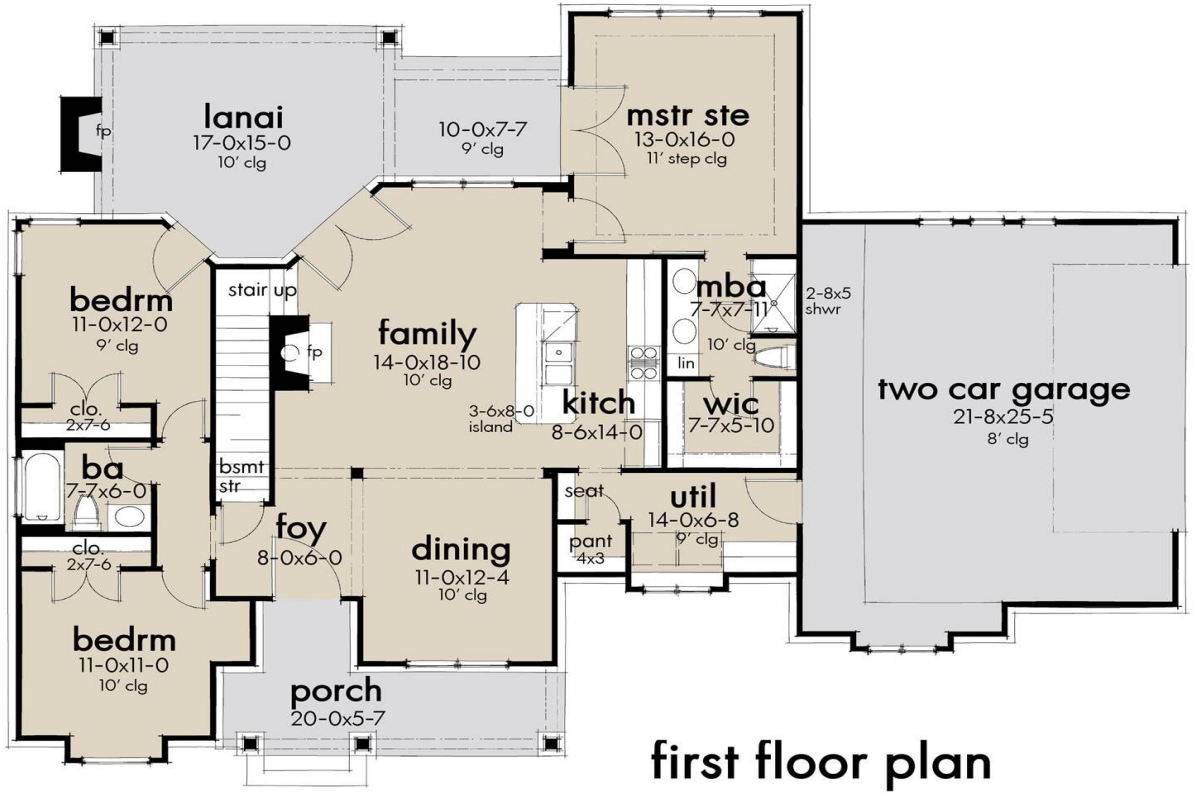
CANADA'S National Research & Education Network

WHAT IS A SECURITY FRAMEWORK?

CANADA'S
National Research &
Education Network

What is a Security Framework?

- Gives an overall view
- Provides structure
- Creates a way to measure success



HELPS IDENTIFY

- What parts are missing
- What's broken
- Which systems are functional

CANADA'S
National Research &
Education Network

HELPS IDENTIFY

- Is it too big?
- Is it REALLY expensive?
- Does it have a life of its own?

CANADA'S
National Research &
Education Network

HELPS YOU GET WHAT'S:

- Right-sized
- Functional
- Needed

CANADA'S
National Research &
Education Network

NIST CSF

- Cybersecurity incidents directed at critical infrastructure revealed a weakness.
- On February 12, 2013, President Obama signed Executive Order 13636, “Improving Critical Infrastructure Cybersecurity.”
- Initiated NIST to work with private sector to develop consensus standards and industry best practices and create a Cybersecurity Framework.

CANADA'S
National Research &
Education Network

CANADA'S
National Research &
Education Network

What is NIST CSF?

- A set of activities designed to achieve specific cybersecurity outcomes
- NOT a checklist, but a roadmap
- Made up of four elements:

NIST CSF Functions (5)

Aid an organization in its management of cybersecurity risk:

- Organizing approach
- Enabling risk decisions
- Identifying areas of potential threat

CANADA'S National Research & Education Network

NIST CSF Categories (23)

IDENTIFY

- Asset Management (ID.AM)
- Business Environment (ID.BE)
- Governance (ID.GV)
- Risk Assessment (ID.RA)
- Risk Management Strategy (ID.RM)
- Supply Chain Risk Management (ID.SC)

DETECT

- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)
- Detection Processes (DE.DP)

RECOVER

- Recovery Planning (RC.RP)
- Improvements (RC.IM)
- Communications (RC.CO)

PROTECT

- ID MGMT, Auth. & Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Info Protection Proc. & Procedures (PR.IP)
- Protective Technology (PR.PT)

RESPOND

- Response Planning (RS.RP)
- Communications (RS.CO)
- Analysis (RS.AN)
- Mitigation (RS.MI)
- Improvements (RS.IM)

CANADA'S
National Research &
Education Network

NIST CSF Subcategories (108)

- Further divides a Category into specific outcomes of technical and/or management activities
- Provides a set of results to support the achievement of outcomes in each Category

NIST CSF: IDENTIFY

SAMPLE

SUBCATEGORY: Governance (ID.GV) 1 of 6

- **ID.GV-1**: Organizational cybersecurity policy is established and communicated
- **ID.GV-2**: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
- **ID.GV-3**: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
- **ID.GV-4**: Governance and risk management processes address cybersecurity risks

NIST CSF References (504)

Sections from other published standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each subcategory

Examples:

- CIS CSC
- COBIT
- ISO 27001
- NIST SP 800-53
- ISA 62443

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

The Capability Maturity Model Integration (CMMI)

- A process and behavioural model that helps organizations:
  - streamline process improvement
  - encourage productive, efficient behaviour that decreases risk
- Developed by the Software Engineering Institute at Carnegie Mellon University
- Currently administered by the CMMI Institute, which was purchased by the ISACA in 2016

CANADA'S
National Research &
Education Network

Maturity Model Levels

The CMMI model breaks down organizational maturity into six levels:

- **Maturity Level 0 – Incomplete**: Work may or may not get completed
- **Maturity Level 1 – Initial**: Processes are viewed as unpredictable and reactive
- **Maturity Level 2 – Managed**: There's a level of project management achieved
- **Maturity Level 3 – Defined**: Organizations are more proactive than reactive
- **Maturity Level 4 – Quantitatively managed**: Measured and controlled
- **Maturity Level 5 – Optimizing**: Processes are stable and flexible

Maturity Model

CANADA'S National Research & Education Network

Questions in the assessment are in increasing maturity order

- Partly why "N/A" is not an option

The "Target" maturity will be set to 3 (Defined)

Questions MUST be answered as honestly as possible

- If the answer lies between two options, always choose the lower of the two

Self-Assessment

- Self-Assessment against an established cybersecurity framework allows for an organization to:
  - Identify any gaps (things they are not doing)
  - See how well they are performing
- Undertaken by answering a specific set of control questions that are aligned to the desired framework
- Aggregate answers provide a view into the overall picture of the organization's cybersecurity program

CANADA'S
National Research &
Education Network

Delegation

The ability to assign someone specific question(s) to get the best possible answer.

Delegation

- One person “owns” a question at a time; once delegated, it will not be accessible to answer by the person who delegated it
- Delegated questions can be retrieved
- Plan any delegation that is intended
  - Let the delegate know in advance
  - Explain they will get a signup e-mail for the system
  - Remind the delegate that the questions need to be answered as honestly as possible. If in between two answers – choose the lower of the two.

CANADA'S
National Research &
Education Network

QUESTIONS & SUPPORT:

nca@nren.ca