Approaching a CSA z246.1 Compliance Program

Comparisons with Other Programs

March 3, 2025

Introduction

- Developed with the contributions from industry experts throughout Canada
- CSA z246.1 is in its fourth edition since 2009.
  - Introduces cybersecurity measures through a Security Management Program (SMP).
  - Continues to focus on the pipeline, natural gas, hydrocarbons, petrochemical, oil & gas, oil sands, and petroleum and natural gas wells in Canada.
  - Requires security risks to be managed using risk-based and performance-based management processes.
  - Note where the requirements state “shall” versus “should”.
  - Enforceable in Alberta in May 2025 by AER under Alberta Legislation 08/2024.
  - Enforceable in BC since August 2023 by BCER.
- The organization subject to CSA z246.1:21 chooses how to develop and implement its SMP.
- Violations could result in notices of non-compliance, public letters, or suspension of the approved licenses
- BCER may request the licensee to engage a third-party review of their SMP.

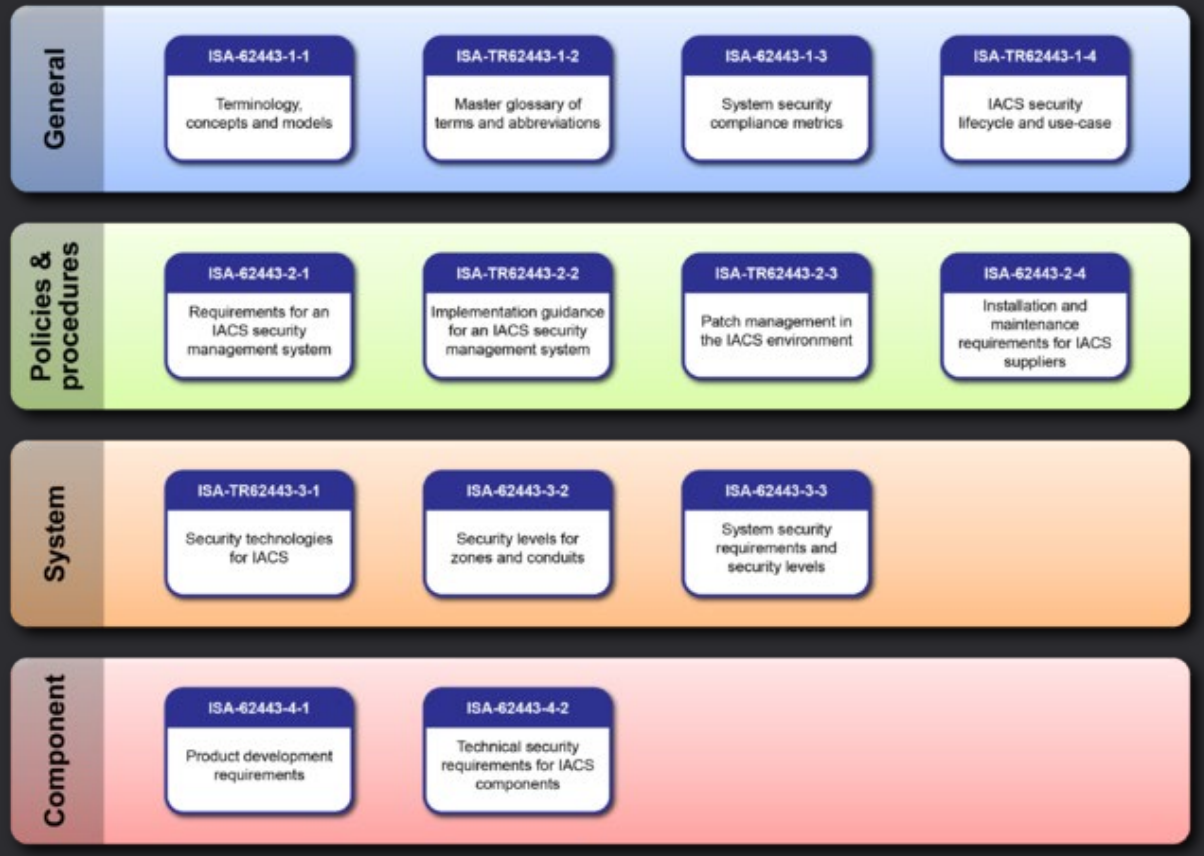
ISO/IEC 27001 Comparison

- Plan Do Check Act cycle
- Risk-based management processes
  - Natural alignment with ISO 31000 which is applicable to operational and cybersecurity risks
  - ISO/IEC 27002 Information Security (IS) Controls as a guide for IS risk response
- Performance-based management processes
- People Process Technology (PPT) focus on:
  - Information Security Management
  - Cybersecurity
  - Personnel Security
  - Physical Security Measures
  - Security Incident Management
  - Monitor and Review

NIST CSF v2.0 Comparison

- Preferred standard for cyber security capabilities in North America.
- NIST CSF v2.0 is a voluntary standard and an organization is unable to be certified.
  - Focuses on the 6 tiers: Govern, Identify, Protect, Detect, Respond, Recover.
  - Aligns naturally with NIST RMF and NIST SP 800-53.
  - Does not directly support physical security, monitoring and review, and other sub-requirements like competence and communication requirements. Requires other NIST standards or special publications to address gaps in NIST CSF.
- Risk-based management process alignment with NIST RMF.
- Performance-based management process alignment with NIST SP 800-55.

ISA/IEC 62443 Comparison



- Preferred standard for cyber security in OT environments.
- Incorporates a structured approach with proven standards developed over decades.
- Aligns with many of the CSA z246.1 requirements
- Incorporates Maturity Levels and Security Levels
- Engineering-focused approach
- Performance-based security standard
- Globally accepted standard

Comparison with CSA z246.1

- Other standards and frameworks can be compared but the purpose of this presentation will focus on the mentioned.
- Each standard or framework holds its own pros and cons which may go beyond the scope of CSA z246.1 or be short of the full requirements.
- Mapping comparisons shown below will vary with your organization. As each standard or framework is interpreted or implemented with unique requirements, consider the following as a guide.

CSA z246.1 Requirements	ISO/IEC 27001	NIST CSF v2.0	ISA/IEC 62443
Security Management Program	Clause 4: Context of the Organization Clause 5: Leadership	Govern	ISA-62443-2-1
Security Risk Management	Clause 6: Planning	Identify	ISA-62443-3-2
Information Security Management	Clause 5: Leadership	Protect	ISA-62443-3-3
Cybersecurity	Annex A8: Technological	Protect & Detect	ISA-TR62443-3-1
Personnel Security	Annex A6: People	Protect	ISA-62443-2-1
Physical Security Measures	Annex A7: Physical	Protect	ISA-62443-3-3
Security Incident Management	Annex A5: Organization	Respond & Recover	ISA-62443-2-1
Monitoring and Review	Clause 9: Performance Evaluation Clause 10: Improvement	Detect	ISA-62443-2-1

Implementation Approach

- Any standard or framework should work. Where one is not fully matched with CSA z246.1, customizations will be required.
- Secure senior management support.
- Align with your enterprise goals .
- Practice documentation for your SMP and decisions.
- Consider a common program for all regions if possible.
    - Multiple programs may get confusing and over-allocated costs.
- Try to generate evidence that will convince the auditor you've completed the right decisions.
- Use the right terminology.
- Leverage existing controls if possible, don't reinvent the wheel.
- Convergence between IT and OT departments may be required depending upon your organization's structure and business requirements.

Dependencies

- Apply your Business Impact Analysis (BIA) and Business Continuity Plan (BCP) to your CSA z246.1 program.
- Integrate your risk management framework.
- Consolidate your risk management processes where possible.
- Update your policies to govern priorities and resources for your SMP.
- Identify and categorize your critical processes.
    - Associate interested parties, internal and external.
    - Identify impacted systems and cyber assets.

Risk Management

- Any risk management process is acceptable
- Considerations:
  - Risk processes are to be applied to people, process, and technology in CSA z246.1. Examples: personnel, physical security, cybersecurity.
  - Leverage what works in your organization to introduce less change.
  - Use ISO 31000 / ISO/IEC 27005 if a new reference point is required.
- Options
  - Practice a dedicated risk process for the z246.1.
  - Integrate with OT risk management processes.
  - Integrate with ERM.

External Relationship Impacts

- *Section 4.5 External Relationships*

  The operator should establish external relationships that

  a) *Include contracts and agreements with security partners and third parties that address the organization's security processes; and*

  b) *Ensure other security partners and third-party processes are aligned with the operator's SMP, where applicable*

- This requirement may vary with each permit holder and their relationship with each external relationship. Considerations include, but are not limited to:
  - The roles and responsibilities for vendors or suppliers to the permit holder's critical processes
  - Response to risk assessments may bring into scope an external relationship with strategic or critical partners
  - Requirements from any contracts or agreements
  - Requirements from the SMP

8) How SimpliGRC Can Support

GRC solutions across regulations, frameworks, and standards

Successfully completed several assessments and audits including NIST CSF, CIP, CIS, ISO, TSA

Diverse range of different IT and OT environments and industries

Expert process development and re-engineering

Senior analysis and project management services

Softening silos and sub-cultures to achieve enterprise or project goals

Strategy development and implementation

Experienced in Business Impact Analysis and Risk Assessments

The managing directors deliver the services to offer the direct experience and competencies

Local to Calgary and Edmonton in Alberta, Canada

Contact Us

For more information:

visit https://simpligrc.com

OR

email: info@simpligrc.com

THANK YOU