The Value of an Information Security Management System (ISMS)

June 25, 2025

Burt Kim Profile

- Actively engaged in different critical infrastructure industries
- Managed and implemented 30+ project and programs across GRC and cybersecurity
- IT and OT and enterprise environments
- Started SimpliGRC with a business partner in 2023
- Located in Calgary with international reach

Common IS Scenarios and Challenges

	Common Information Security (IS) Scenarios	Common IS Challenges
1	Personnel buy-in to the strategy is low	• May cause confusion, decrease in moral, lost opportunities, personnel departures, culture barriers • Misallocated resources may trigger ineffective sunk costs and missed targets • Risks may be assessed incorrectly
2	Competing priorities for cross-functional resources	
3	Actual outcomes are below the expected outcomes	
4	Risk management is misaligned with the business	
5	Stagnant processes and / or procedures for evolved operations	
6	Portfolios are larger than allocated budgets	• Ineffective or inefficient responses to planned and unplanned events
7	Misalignment with enterprise goals and objectives	• Budgets and other resources may be reduced • Changes to the team or department
8	People, Process, Technology (PPT) controls are imbalanced	• Technology solutions are perceived to represent information security and cybersecurity programs
9	Complicated compliance programs, includes internal and external	• Lack of trust from the external stakeholders • Potential violations to legal or regulatory requirements • Negative public image
10	Leadership changes may trigger downstream impacts to the organization	• Culture and sub-cultures may impede strategy and outcomes
11	Succession plans for key Subject Matter Experts (SMEs) are insufficient	• Loss of key resources that may negatively impact operations

SIMPLI GRC

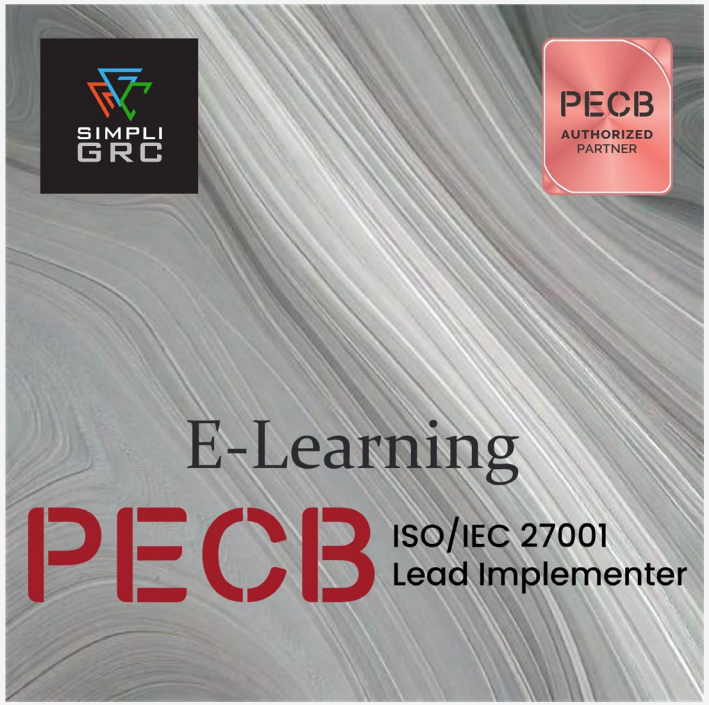
Introduction to ISMS

Information Security Management System (ISMS), as defined by ISO/IEC 27000:2012

> *part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security*

Break down the definition and the following can be interpreted as characteristics of an ISMS:

1. A risk-based approach focused on the business or segment of the business
2. Scope and authorize the ISMS program to increase the Confidentiality, Integrity, and Availability (CIA) of information security
3. A plan to implement and operate an ISMS
4. Operational governance, risk, and compliance functions through the implementation of policies, processes, procedures, guidelines, and controls
5. Monitoring, reviewing, and maintaining the authorized PPT controls
6. Continual improvement where gaps or deviations in the authorized ISMS program are discovered



Value of an ISMS

Culture eats strategy for breakfast

- Peter Drucker

Value of an ISMS

1. A strong ISMS incorporates culture
2. Supports enterprise goals and objectives
3. Synergizes PPT for expected outcomes
4. Intake almost any event and enables the organization to manage it
   - Cybersecurity incidents
   - Operational incidents
   - Emerging technologies
   - Risk responses
5. Integrates external requirements like regulations or partner agreements
6. Integrates with any risk framework
7. The people side of an ISMS include:
   - Alignment with the organization's business environment and culture
   - Needs and expectations of interested parties or stakeholders
   - Leadership demonstrates commitment to the ISMS
   - Enabling the competence, awareness, and communication of the personnel
8. Increases protection of the information assets through CIA
9. Demonstrates a strong information security program to interested parties

Value of an ISMS

Focusing on one pillar of PPT excessively can feel like a game of Whack-A-Mole.

- Assume one individual holding the mallet represents one of the PPT pillars.
- As one hole or event / risk is managed, another appears and so on
- Next, assume three people holding mallets each representing all three pillars of the PPT framework. They are added to the same playing surface in the same game. This is where the strength of PPT is resembled.

Each PPT pillar holds its own benefits and when they work together, synergies are realized.

ISMS Requirements

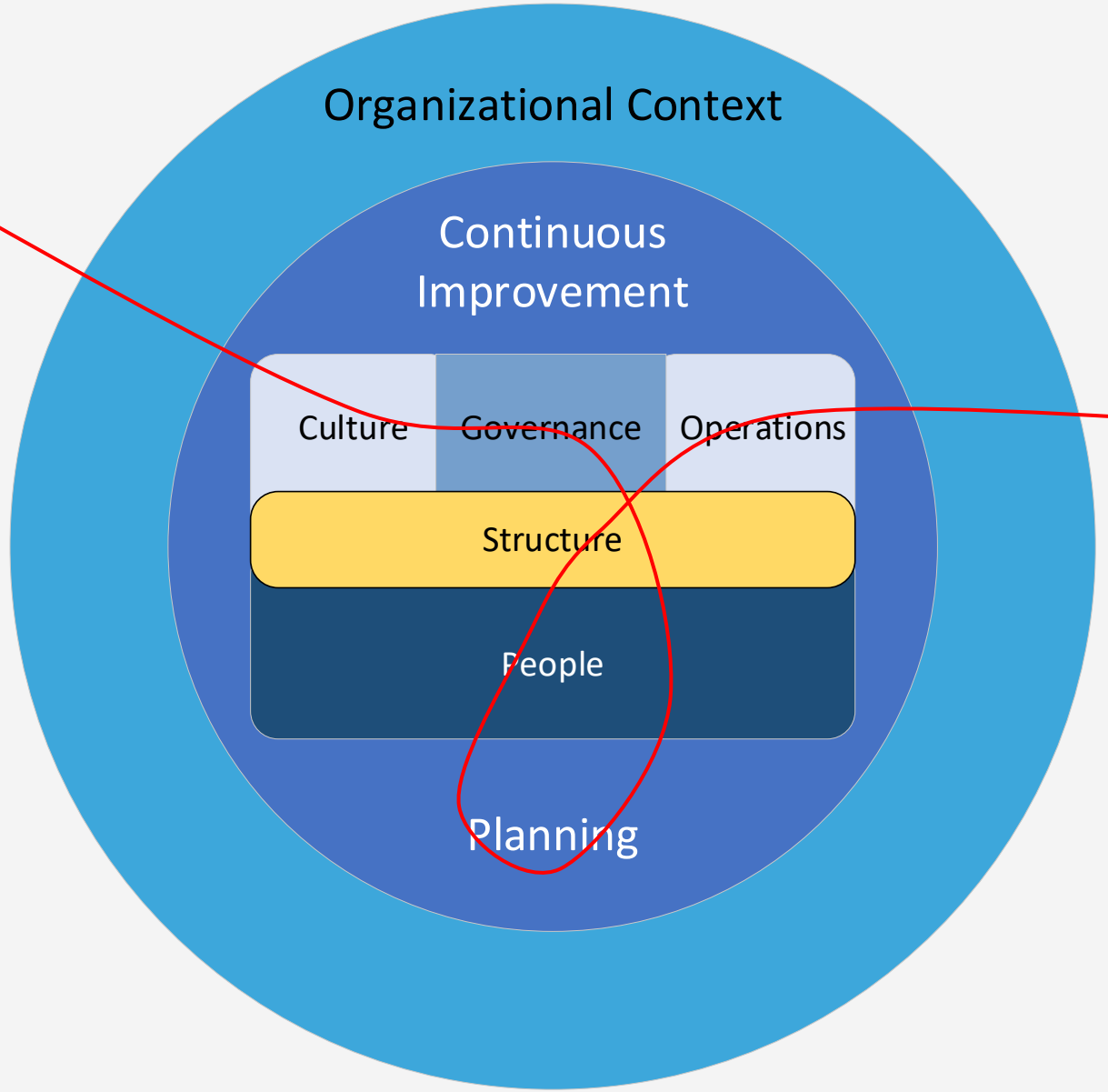
Common Requirements of an ISMS	
Context of the organization • Purpose of the organization • Enterprise goals and objectives	**Planning** • Risk management framework • Information security objectives • Program changes
Culture • Leadership • Sub-cultures	**Continuous Improvement** • Monitoring, measuring, evaluating
Governance • Policy, process, procedure	**Structure** • Roles and responsibilities
Operations • Planned outcomes • Oversight • Communication • Risk Management	**People** • Leadership • Subject Matter Experts • Interested parties • Awareness and training

Sample ISMS


Organizational Context
Continuous Improvement
Culture
Governance
Operations
Structure
People
Planning

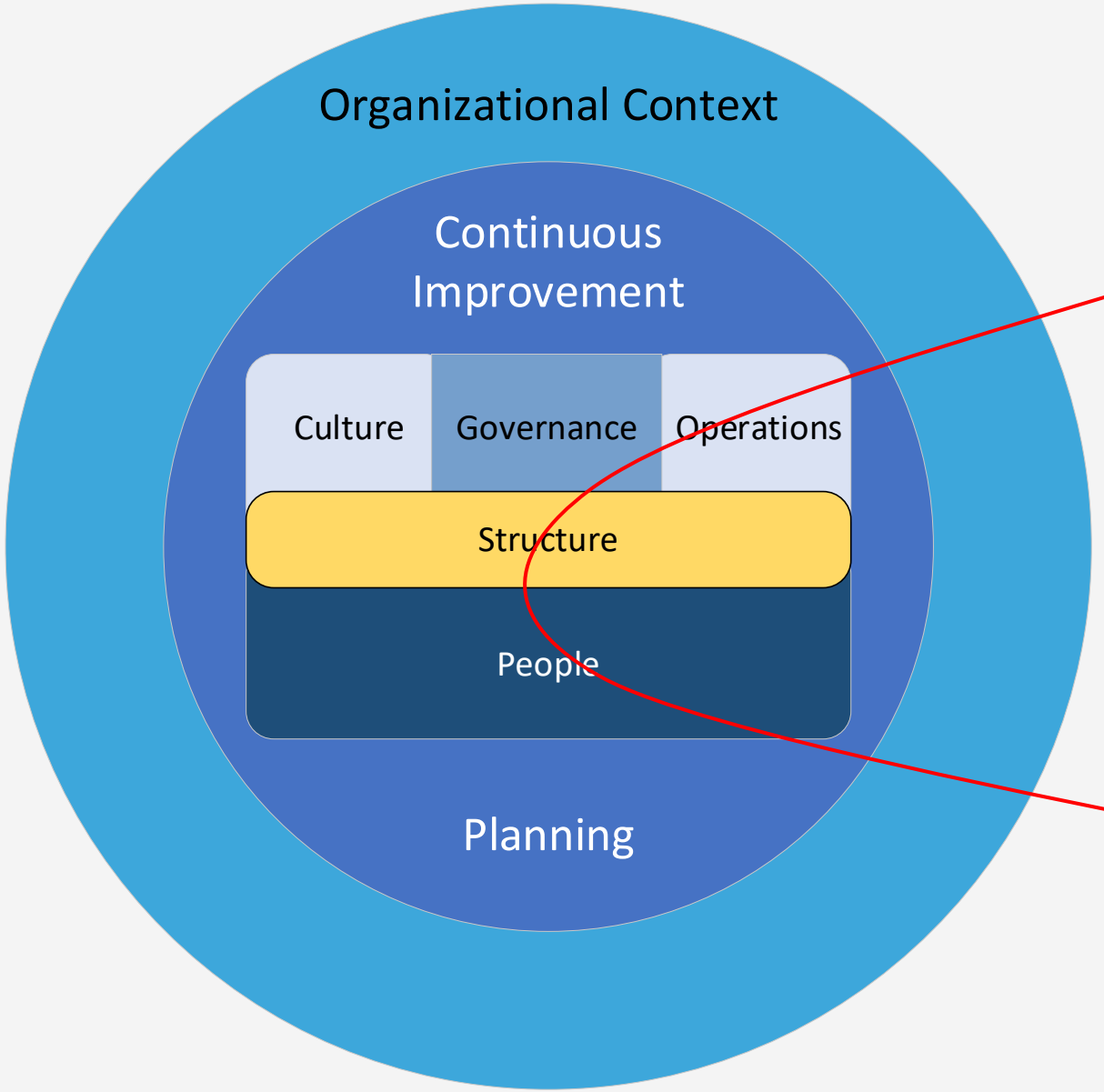
Sample ISMS

Input (Event):
Leadership Change



Output:
Operational Changes

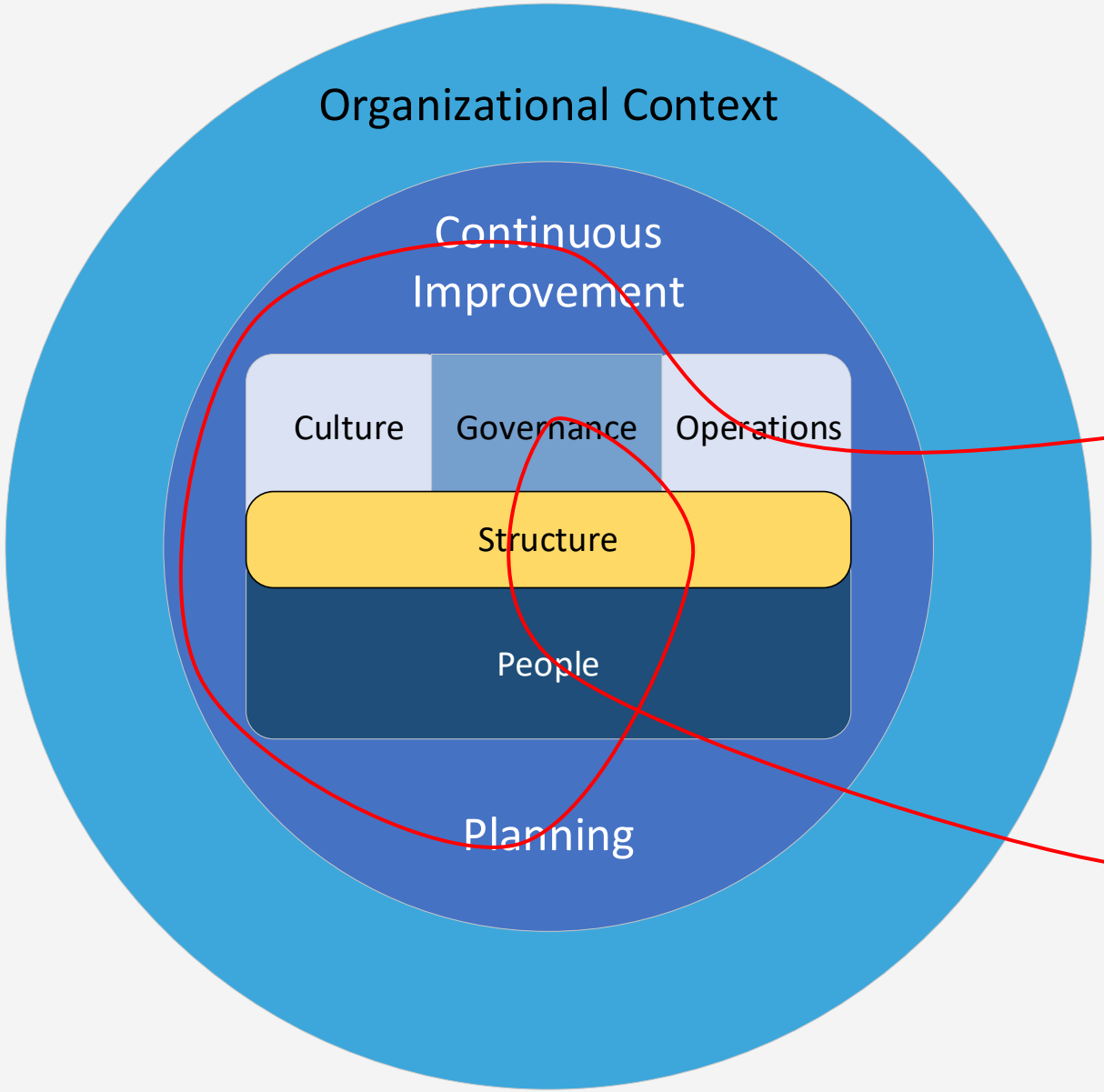
Sample ISMS



Input (Event):
Planned Operations

Output:
Expected Outcomes

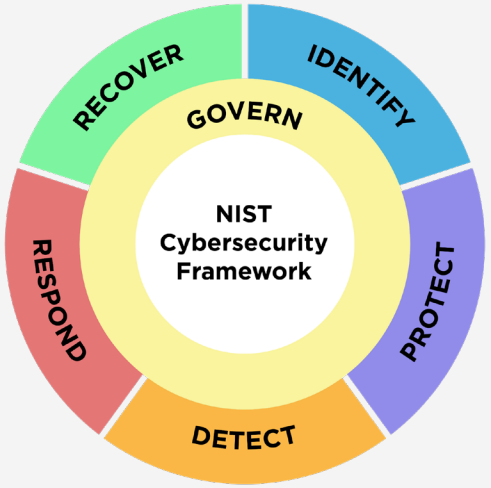
Sample ISMS



Input (Event):
New Operational Event

Output:
Updated Operations

ISMS Standards and Frameworks



Integration of Additional Requirements

- Implementing PPT makes for easier integration of additional or customized requirements that fit your organization.
    - Cultural requirements specific to your organization.
        - Changes to enterprise requirements are easier to integrate with existing alignment of business goals and objectives.
            - A properly implemented ISMS is capable to adopt requirements from external sources, including regulations, partners, customers, or internal strategies. Eg. Privacy regulations, payment card industries, OT cybersecurity, or critical infrastructure requirements.
                - Incorporate any Risk Management Frameworks (RMF) including ISO 31000, NIST RMF, or operational risk management programs.
                    - Risk practitioners certified in CRISC, CISM, or ISO 27005 can integrate additional requirements into the RMF.

ISMS Pros and Cons

ISMS Characteristics	Pros	Cons
Risk Management	• Integrates with other risk-related standards and frameworks • Requirements to align with enterprise goals and objectives	• Deep learning curve and experience required to implement or assess
Enhanced Security of CIA	• Reduces information security risks by safeguarding valued assets • Integrates with standards and frameworks • Internationally recognized	• Less specialized than specific standards or frameworks (e.g. PCI, ISA/IEC 62443, NERC CIP, etc.)
An ISMS Plan	• An integrated plan to implement ISMS requirements • Integrates with other management systems like ISO and NIST standards	• Deep learning curve and experience required to implement or assess
Operational GRC Functions	• Plan-Do-Check-Act cycle is applicable to all GRC functions with integration • Incorporates cultural requirements	• Risk of resistance from the culture and / or sub-cultures
Monitoring and Controlling PPT	• PPT approach strengthens sustainability and comprehensive information security • Reduces compliance risks with non-technical controls • Structured auditing practices from authorized auditors	• Larger investment and more time required
Continual Improvement	• Controls and checks to measure operational performance and correct deficiencies	• Increased resources to monitor and correct gaps in the ISMS

Value of Certifying Your ISMS

1. The certification process increases awareness
2. Enhances reputation and trust
3. Promotes comprehensive and applicable planning
4. Increases competitive advantage using credible industry standards
5. Reduces risk of security incidents
6. Reduces compliance risk and with legal and regulatory requirements
7. Strengthens capabilities to respond to unplanned events
8. Stronger information security with proven requirements
9. Embeds ISMS activities into the culture
10. Continual improvement measures are mandatory

How SimpliGRC Can Support

Certified staff in a number of ISO and ISACA certifications

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

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

Experienced in Business Impact Analysis and Risk Assessments

Senior analysis and project management services

IT / OT convergence services in complex environments

Strategy development and implementation

Process development and re-engineering

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

Local to Calgary and Edmonton in Alberta, Canada

THANK YOU

info@simpligrc.com

https://simpligrc.com/about/contact/