CYBERSECURITY RISK POST COVID-19

STRENGTHENING YOUR DEFENCES

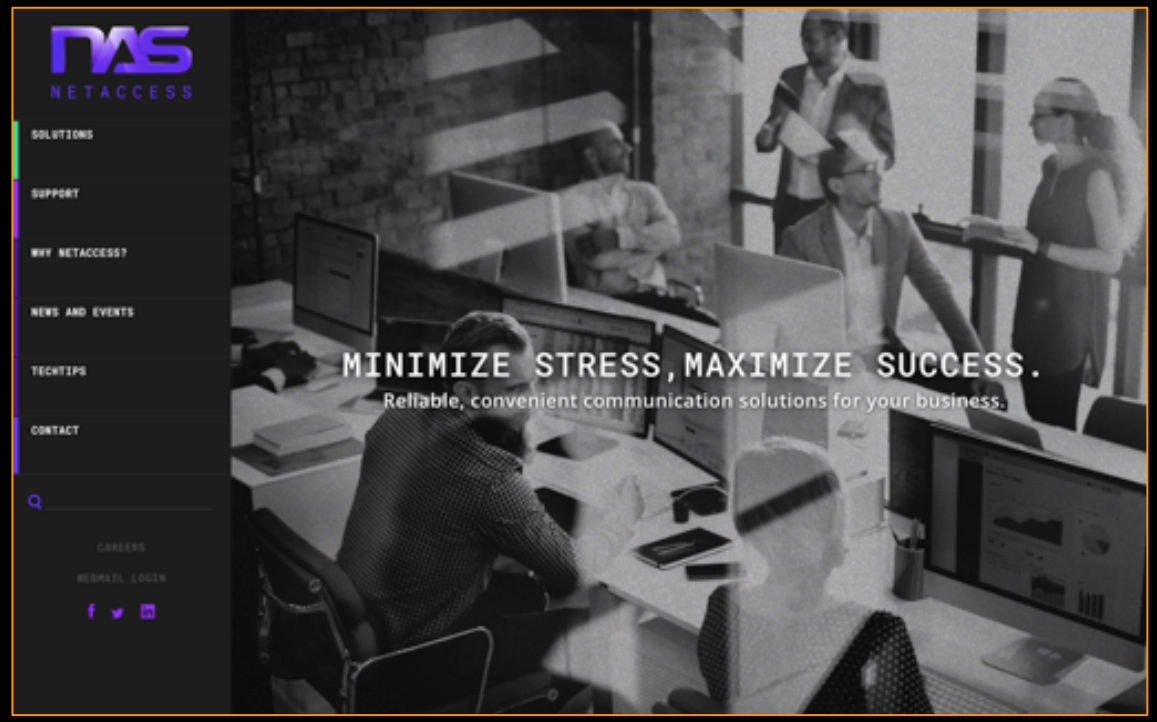
Raimund Laqua, PMP, P.Eng
ray.laqua@leancompliance.ca



CYBERSECURITY RISK POST COVID-19

Introductions

Net Access

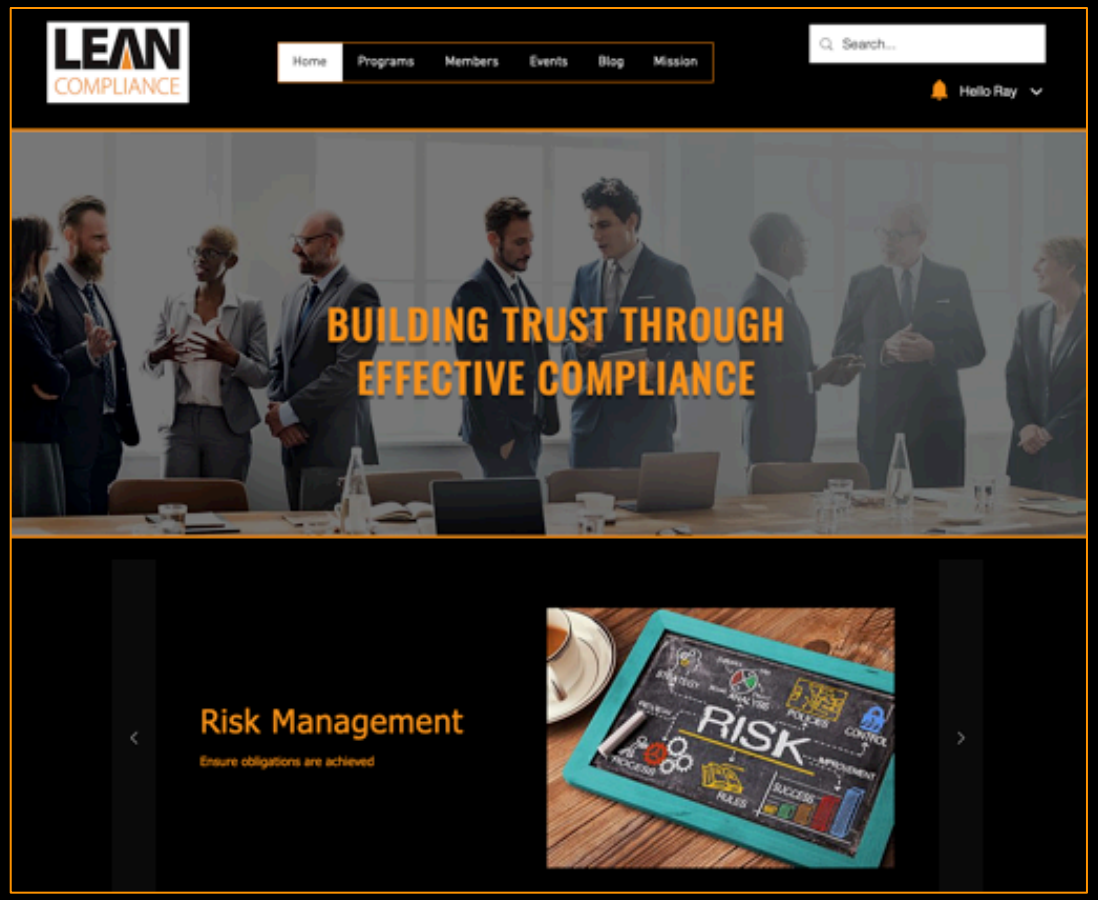


NetAccess strives to empower businesses to achieve success through the effective use of ICT. Our culture is one where reliable and personalized service comes standard, and where innovation is nurtured. We aim to transform the way our clients do business so they can stop worrying about technology and concentrate on using it to drive growth.

CYBERSECURITY RISK POST COVID-19

Introductions

Lean Compliance

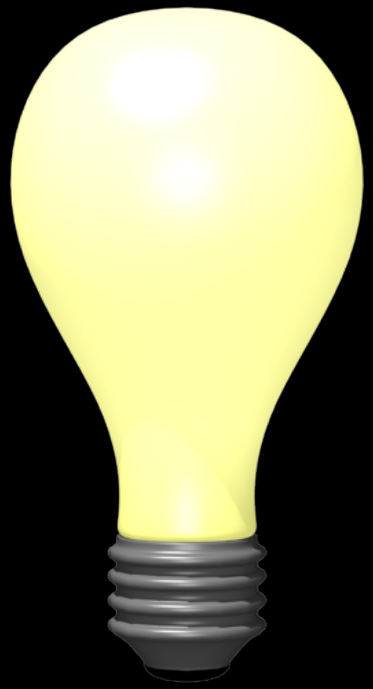


Lean Compliance's mission is to help ethical and ambitious companies in highly-regulated, high-risk industries improve the effectiveness of their compliance programs covering safety & security, quality, regulatory and environmental objectives.

www.leancompliance.ca

CYBERSECURITY RISK POST COVID-19

The Big Idea



In response to the COVID-19 pandemic organizations and individuals have rapidly adopted remote working arrangements and technologies. These actions present new and increased cybersecurity risk for organizations of all kinds and sizes.

To help contend increased risk, organizations and individuals should strengthen their defenses to protect information, assets, along with worker and public safety which requires that they:



1. Identify and assess cybersecurity uncertainty & risk
2. Develop and implement a cybersecurity strategy and plan
3. Continually measure and improve the effectiveness of their cybersecurity program

CYBERSECURITY RISK POST COVID-19

Webinar Outline

1 **RISK** → 2 → 3 **SAFETY**



1. Identify and assess cybersecurity uncertainty & risk
2. Develop and implement a cybersecurity strategy and plan
3. Measure and continual improve the effectiveness of your cybersecurity program



CYBERSECURITY RISK POST COVID-19

What comes to mind when you hear the phrase cybersecurity?



CYBERSECURITY RISK POST COVID-19

What comes to mind when you hear the phrase cybersecurity



Update to Our Customers:

Protecting Your Information

LifeLabs

To our customers,

It's been just over six months since we announced that we had been victim of a cyber-attack involving unauthorized access to our computer systems. I want to thank you for your continued support and patience. You entrust us with important information and we take that responsibility very seriously.

Back in December, I made a commitment to you. I promised you that we would learn and work hard to earn back your trust. I cannot change what happened, but I assure you that I have made every effort toward making change to provide you services you can trust. Here are just some of those changes that our team and I have made to best protect your information by strengthening our information security program:

- We have appointed a Chief Information Security Officer (CISO), who together with an expanded team, is leading our program of information security improvements;
- We have welcomed two new leaders to the LifeLabs team in the roles of Chief Privacy Officer and Chief Information Officer. Both leaders bring substantial experience in cybersecurity and privacy protections, strengthening our practices across the organization;
- We have enhanced and accelerated our Information Security Management program through an initial $50 million investment, backing our plan to achieve ISO 27001 certification - a gold standard in information security management that is achieved by only a small number of organizations;
- We have engaged an independent third-party professional services firm to objectively evaluate the response to the cyber-attack, efficacy of our security programs and capabilities, and make recommendations for further process enhancements;
- We continue to deploy cyber security firms to monitor the dark web and other online locations for information related to the cyber-attack. To date, no public disclosure of customer data from the attack has been identified.
- We established an Information Security Council with internal and external cyber security experts who will regularly report to me and the Board of Directors on information security practices and protocols;
- We have implemented strengthened cybercrime detection technology across the organization;
- Our teams organization-wide will participate in annual security and privacy awareness and training programs.

LifeLabs Response

- ▷Appointed CISO
- ▷Added CPO and CIO
- ▷Invested $50M to achieve ISO 27001 certification
- ▷Engaged third-party to evaluate their program
- ▷Established information security council
- ▷Strengthened their detection technology
- ▷Implemented yearly security awareness and training

CYBERSECURITY RISK POST COVID-19

Observations

- Threats to people and things we care about are all around us.
- Companies should be aware of their risks and manage them effectively.
- Every company has a cybersecurity program, some more effective than others.
- Cybersecurity is not only a technical problem; it is a business problem that requires a business solution.



CYBERSECURITY RISK POST COVID-19

A few definitions we need to know



- **Cyberspace:** the online world of computer networks and especially the Internet.
- **Cybersecurity:** refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as *information technology security*.
- **Cybersecurity Risk:** the effects of uncertainty on cyber security objectives.
- **Cyber Safety**: the outcome of cyber security.

CYBERSECURITY RISK POST COVID-19

Webinar Outline

1 **RISK**

SAFETY



1. Identify and assess cybersecurity uncertainty & risk
2. Develop and implement a cybersecurity strategy and plan
3. Measure and continual improve the effectiveness of your cybersecurity program



CYBERSECURITY RISK POST COVID-19

Cybersecurity Uncertainty and Risk



- In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time. (NY Times)
- In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers. (Uber)
- +62% of businesses experienced phishing and social engineering attacks in 2018. (Cybint Solutions)
- +61% of organizations have experienced an IoT security incident. (CSO Online)
- +43% of breach victims were small businesses. (Verizon)

CYBERSECURITY RISK POST COVID-19

Cybersecurity Uncertainty and Risk



- +62% of full-time employees are working from home up from 33% as result of COVID-19 (McKinsey)
- +83% of enterprise workloads will move to the cloud by the year 2020. (Forbes)
- The average time to identify a breach in 2019 was 206 days. (IBM)
- +73% of organizations are considered cyber novices. Only 11% are considered cyber experts.
- +63% of customers say they're unlikely to do business with a company that has experienced a sensitive data breach in the past.
- The average cost of a data breach is $3.92M as of 2019. (Security Intelligence)

CYBERSECURITY RISK POST COVID-19

Cybersecurity Uncertainty and Risk



"Directors need to ensure that contingency plans and arrangements are in place to deal with crystallized risks, uncertain events, and crises, emergencies and disasters as and when they occur.

Unless they are vigilant, up-to-date and able to quickly react at any time of the day or night, the members of the IT team of an established company can find its security arrangements breached, whether by lone teenage hackers in their bedrooms or organized criminal gangs.

Speed of reaction is critical as sensitive and valuable information can be downloaded in seconds, and as news gets out customers and other groups that could be at risk may become alarmed as awareness of a breach of security is spread by both social and traditional media. ”

– Prof. Colin Coulson-Thomas

Cybersecurity is a business problem that requires a business solution

CYBERSECURITY RISK POST COVID-19

7 Laws of Cyber Security Risk

Law 1: everything happens in the presence of uncertainty.
Law 2: uncertainty creates the opportunity for risk.
Law 3: the risks that matter are connected with what is valued.
Law 4: if there is a vulnerability, it will be exploited.
Law 5: humans can trust when they shouldn't.
Law 6: with change comes opportunity for risk.
Law 7: when in doubt, see law 1.

CYBERSECURITY RISK POST COVID-19

Webinar Outline

1 **RISK** → 2 **SAFETY**

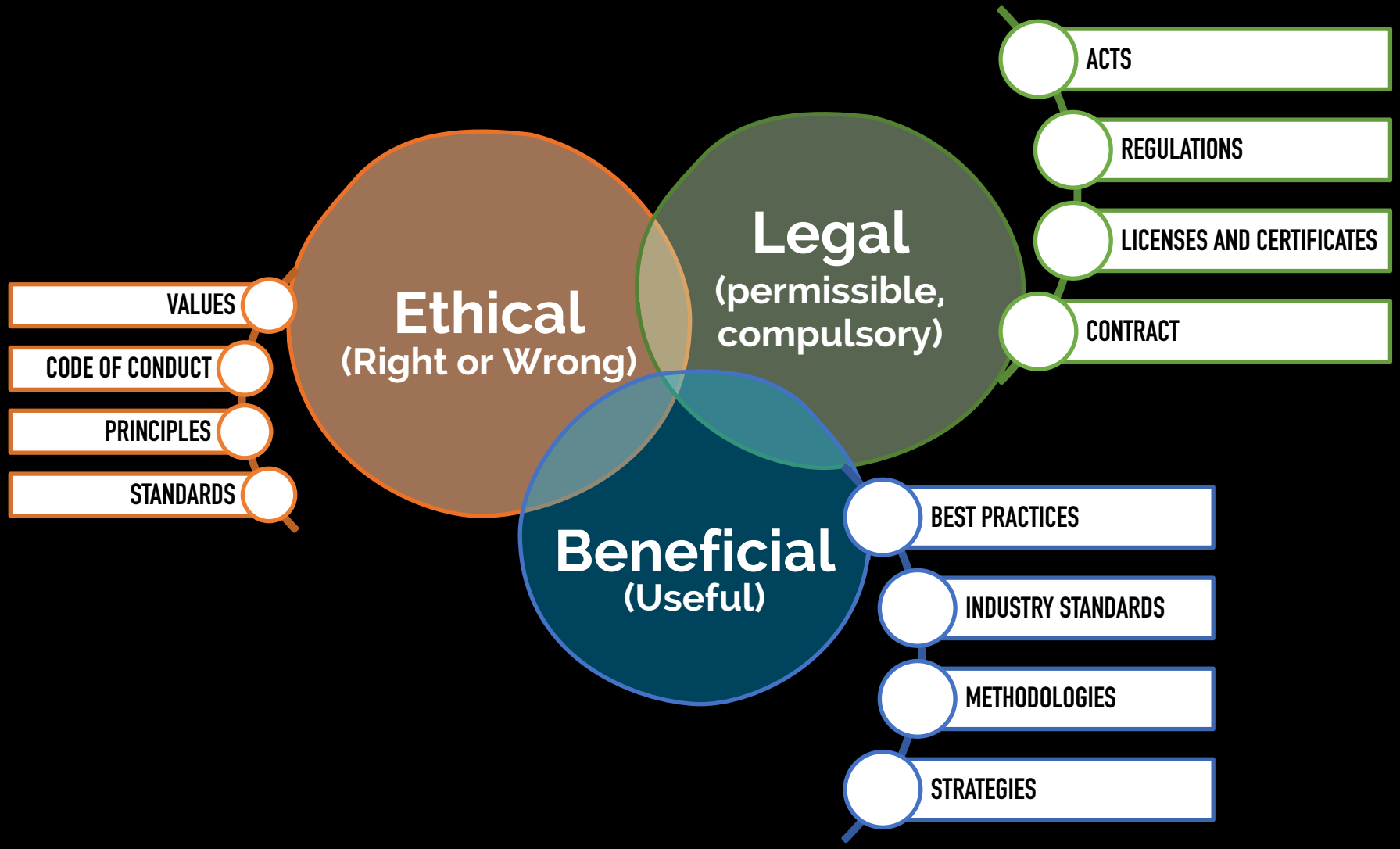


1. Identify and assess cybersecurity uncertainty & risk
2. Develop and implement a cybersecurity strategy and plan
3. Measure and continual improve the effectiveness of your cybersecurity program



CYBERSECURITY RISK POST COVID-19

Strategy, Motivation, and Intent



CYBERSECURITY RISK POST COVID-19

Risk Attitude



Ostrich
I don't want to know

RISK TOLERANT



Avoider
I don't want any risk

RISK INTOLERANT



Manager
Let's size the risk and decide

RISK NEUTRAL



Gambler
Let's play the odds

RISK SEEKING



Strategist
Let's improve the probability of success

RISK OPTIMIZING

Our attitude towards risk affects our approach

CYBERSECURITY RISK POST COVID-19

Risk Objectives



Avoid Mission Failure

- Protect (guard) against loss.
- Minimize the impact of threats.
- Pay attention to what might cause failure and what could go wrong.



Pursue Mission Success

- Ensure (make certain of) outcomes.
- Maximize the probability of success.
- Pay attention to what is critical to success and what needs to go right.

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

LEAN COMPLIANCE

NETACCESS

Managed Safety Program

- What do we need to keep safe?
- What are the effects of uncertainty on safety objectives?
- What threatens safety?
  - **Conditions** – enable the opportunity for harm
  - **Actions** – exploit the opportunity for harm
- What and how strong do defences need to be to achieve safety objectives?
- How do we maintain the performance of our defences (i.e. controls)
- How do we continuously improve effectiveness?

Managed Safety System

Continuous Improvement

- Safety Goals & Objectives
- Safety Risk Assessment
- Threat & Vulnerability Identification
- Security and Risk Controls
- System and Management Controls
- Governance and Oversight

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?



WHAT WE WANT
TO KEEP SAFE

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

Everything happens in the presence of uncertainty



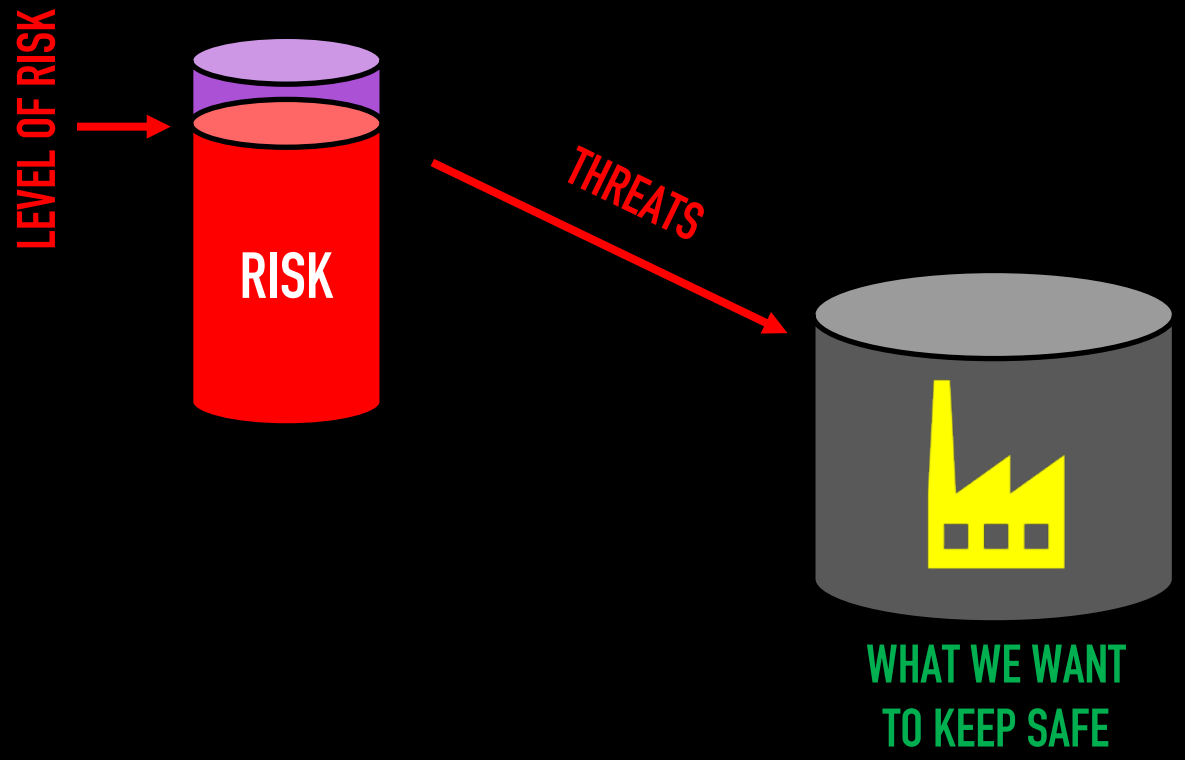


WHAT WE WANT
TO KEEP SAFE

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

Everything happens in the presence of uncertainty



Uncertainty creates the opportunity for risk

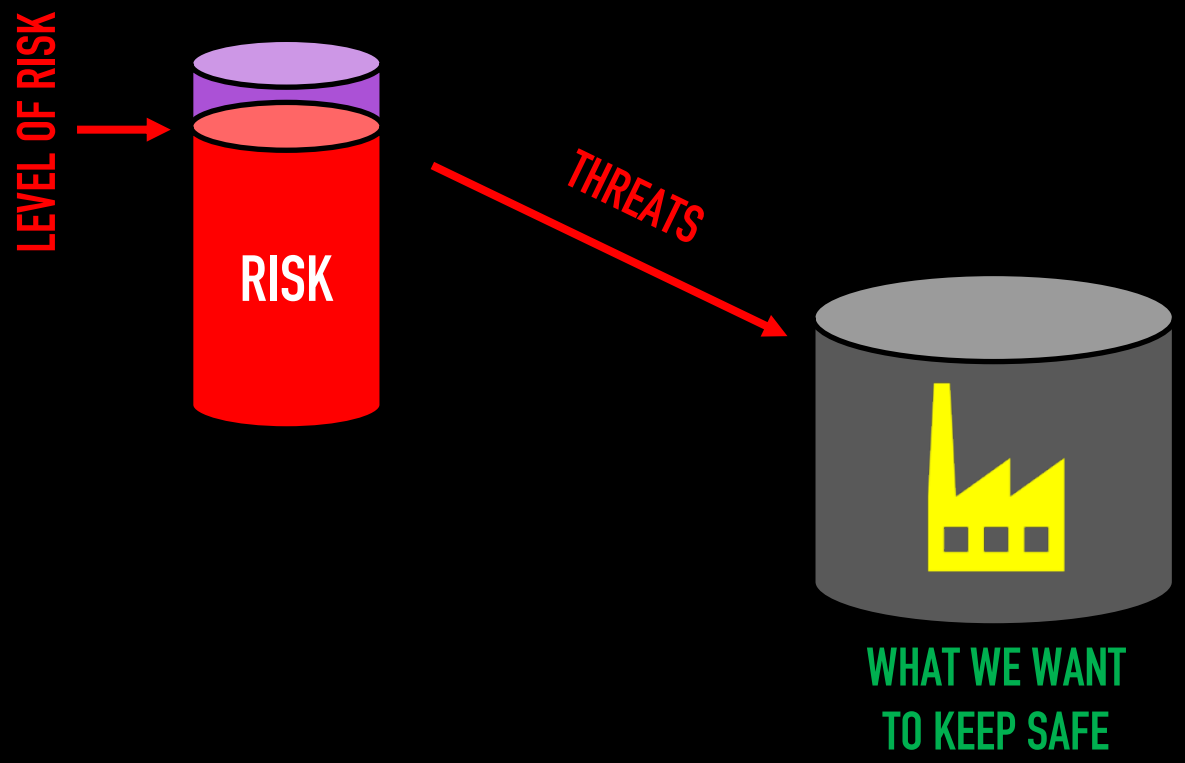
CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

Safety

- The condition of being ***protected*** from or unlikely to cause danger, risk, or injury.
- To ***protect*** against failure, breakage, or accident.
- The state of being "safe"; the condition of being ***protected*** from harm or non-desirable outcomes.

Everything happens in the presence of uncertainty



Uncertainty creates the opportunity for risk

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

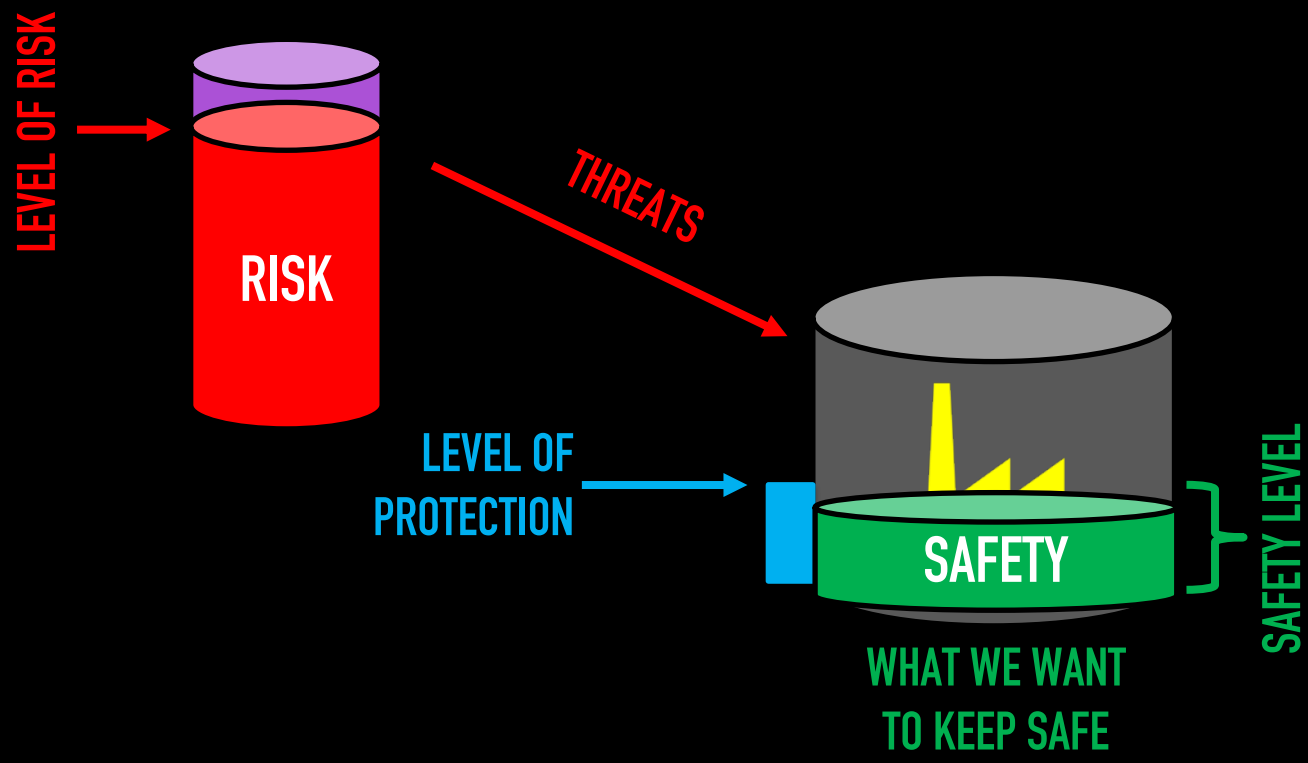
Safety

- The condition of being ***protected*** from or unlikely to cause danger, risk, or injury.
- To ***protect*** against failure, breakage, or accident.
- The state of being "safe"; the condition of being ***protected*** from harm or non-desirable outcomes.

Security

- Freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others.
- Security mostly refers to ***protection*** from hostile forces,
- Refers to acts and systems whose purpose is to ***provide security***.

Everything happens in the presence of uncertainty



Uncertainty creates the opportunity for risk

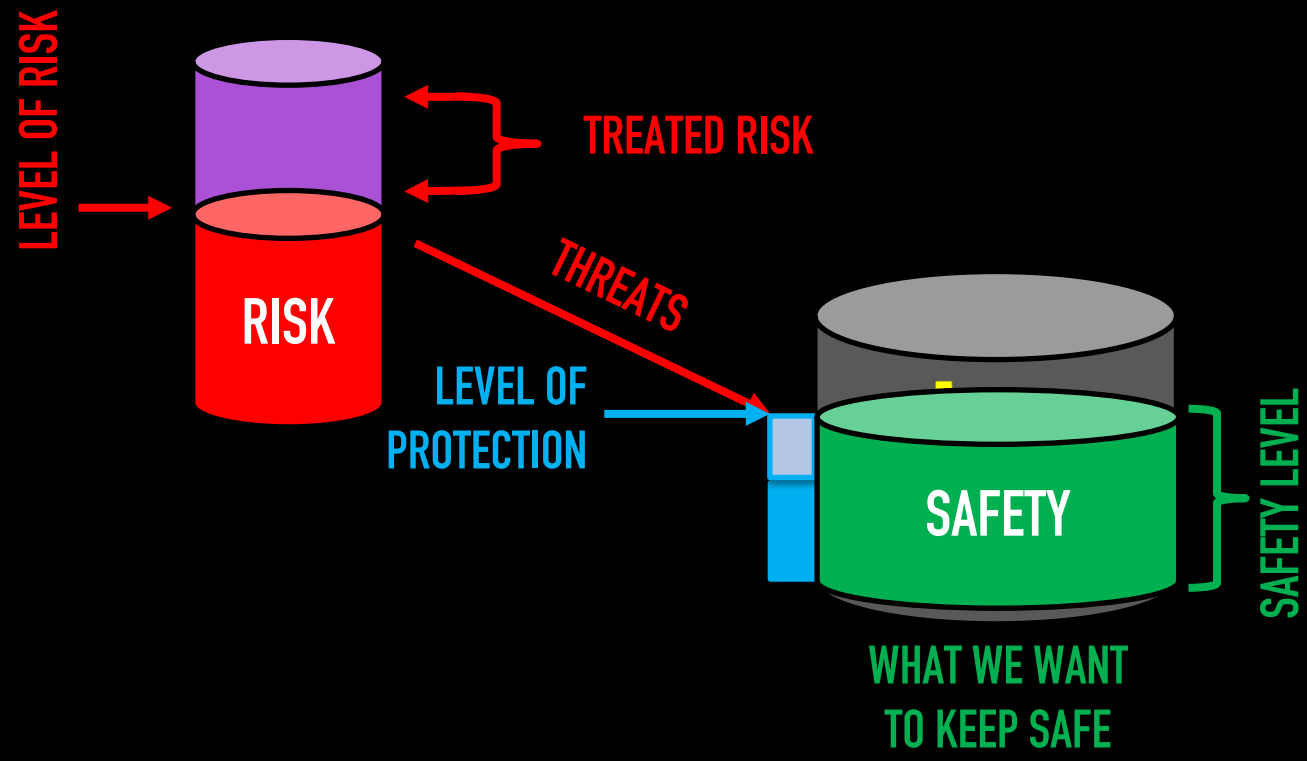
CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?

Managed Safety System

- A businesslike approach to cyber safety. It is a systematic, **explicit and comprehensive process for managing safety risks**. As with all management systems, a safety management system provides for goal setting, planning, and measuring performance.
- Is woven into the fabric of an organization. **It becomes part of the culture;**

Everything happens in the presence of uncertainty



Uncertainty creates the opportunity for risk

CYBERSECURITY RISK POST COVID-19

How do we manage cyber safety?



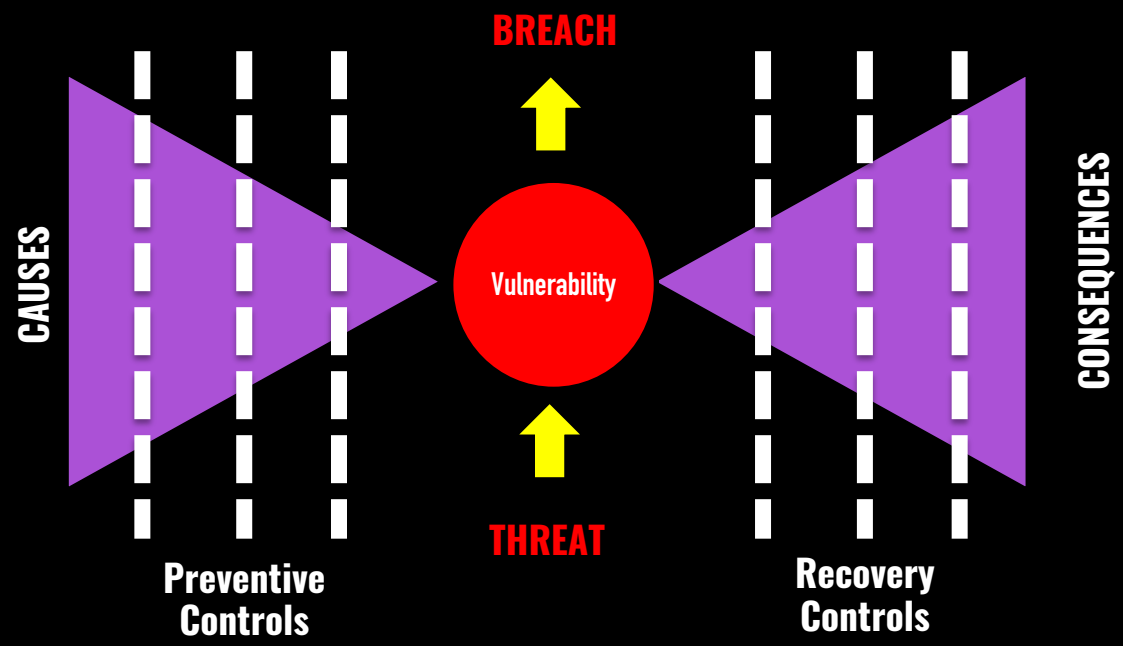
CYBERSECURITY RISK POST COVID-19

Management and Technical Capabilities

LEAN COMPLIANCE

NETACCESS

TECHNICAL PROCESSES



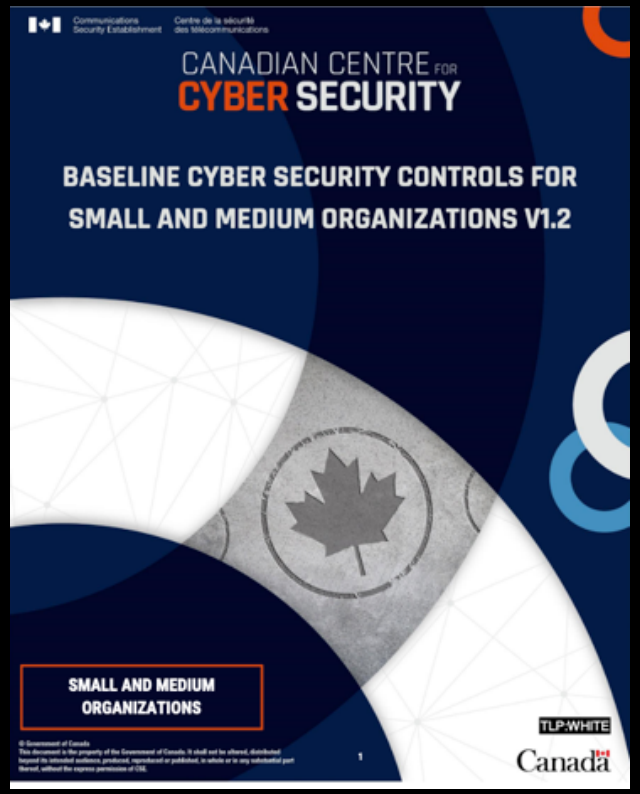
MANAGEMENT PROCESSES



www.securecontrolsframework.com

CYBERSECURITY RISK POST COVID-19

Management Standards and Guidelines



CyberSecure Canada Program



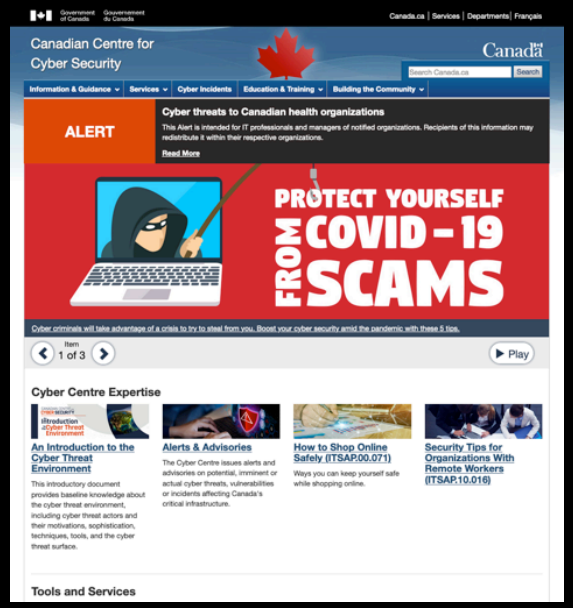
NIST Cybersecurity Framework, DOE C2M2, CISA-CRR



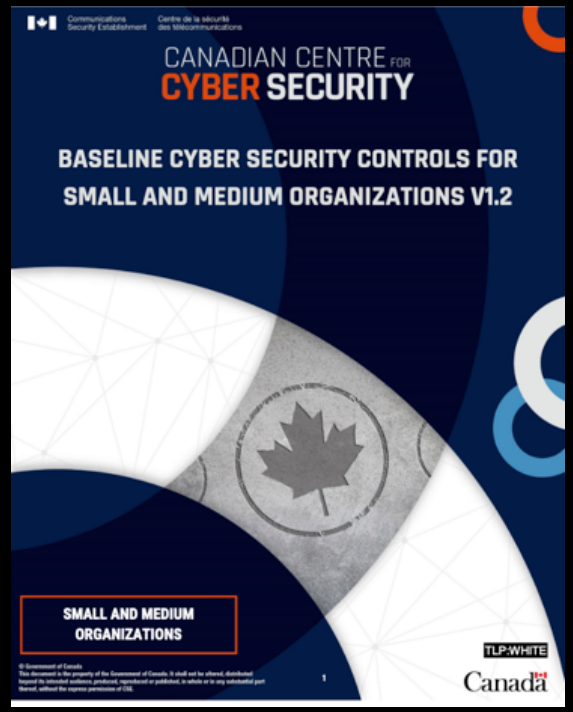
ISO/IEC 27001

CYBERSECURITY RISK POST COVID-19

CyberSecure Canada Program



Canadian Centre for Cyber Security



Baseline Cyber Security Controls for Small and Medium Organizations

- Valuable source of information, regarding cybersecurity.
- Guidelines and checklists to help you get started if you don't have anything in place.
- You will need to develop a management framework to advance your cybersecurity capabilities.
- Good place to start.

https://cyber.gc.ca/en/

CYBERSECURITY RISK POST COVID-19

CRR, CF, C2M2

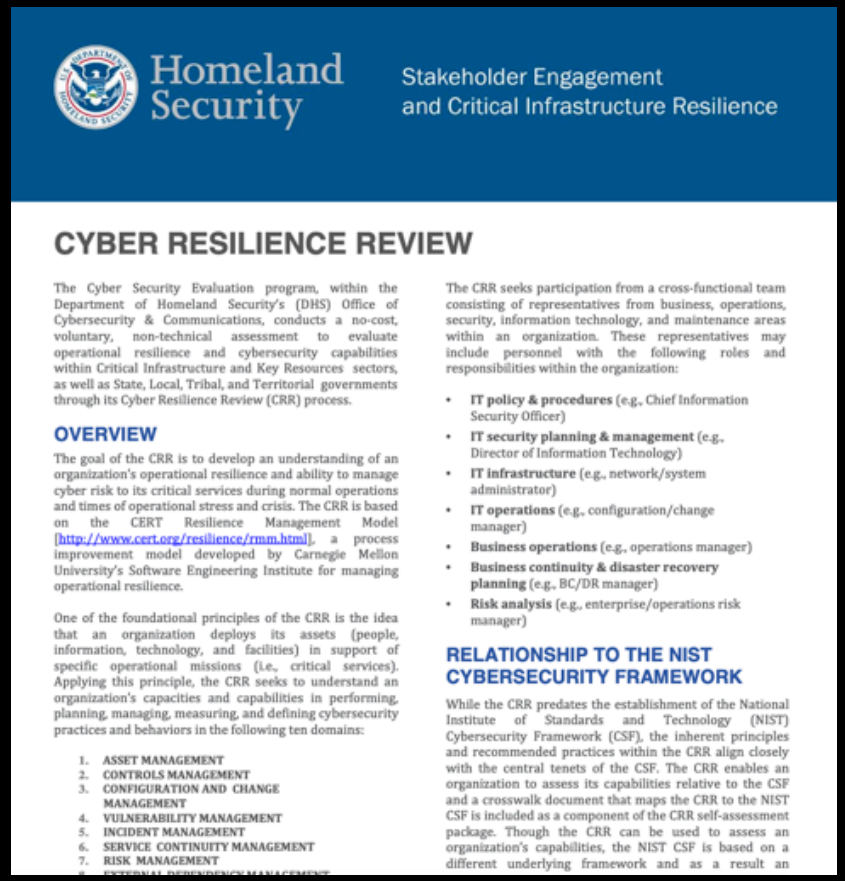


Triple Threat Against Cyber Risk

- ▷ Cyber Resilience Review (CRR)
- ▷ Cybersecurity Framework (CF)
- ▷ Cybersecurity Capability Maturity Model (C2M2)
  - ▷ Electricity Subsector (ES-C2M2)
  - ▷ Oil and Natural Gas Subsector (ONG-C2M2)

CYBERSECURITY RISK POST COVID-19

Cyber Resilience Review (CRR)



Homeland Security

Stakeholder Engagement and Critical Infrastructure Resilience

CYBER RESILIENCE REVIEW

The Cyber Security Evaluation program, within the Department of Homeland Security's (DHS) Office of Cybersecurity & Communications, conducts a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities within Critical Infrastructure and Key Resources sectors, as well as State, Local, Tribal, and Territorial governments through its Cyber Resilience Review (CRR) process.

OVERVIEW

The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. The CRR is based on the CERT Resilience Management Model [http://www.cert.org/resilience/rmm.html], a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience.

One of the foundational principles of the CRR is the idea that an organization deploys its assets (people, information, technology, and facilities) in support of specific operational missions (i.e., critical services). Applying this principle, the CRR seeks to understand an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors in the following ten domains:

1. ASSET MANAGEMENT
2. CONTROLS MANAGEMENT
3. CONFIGURATION AND CHANGE MANAGEMENT
4. VULNERABILITY MANAGEMENT
5. INCIDENT MANAGEMENT
6. SERVICE CONTINUITY MANAGEMENT
7. RISK MANAGEMENT

The CRR seeks participation from a cross-functional team consisting of representatives from business, operations, security, information technology, and maintenance areas within an organization. These representatives may include personnel with the following roles and responsibilities within the organization:

- **IT policy & procedures** (e.g., Chief Information Security Officer)
- **IT security planning & management** (e.g., Director of Information Technology)
- **IT infrastructure** (e.g., network/system administrator)
- **IT operations** (e.g., configuration/change manager)
- **Business operations** (e.g., operations manager)
- **Business continuity & disaster recovery planning** (e.g., BC/DR manager)
- **Risk analysis** (e.g., enterprise/operations risk manager)

RELATIONSHIP TO THE NIST CYBERSECURITY FRAMEWORK

While the CRR predates the establishment of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the inherent principles and recommended practices within the CRR align closely with the central tenets of the CSF. The CRR enables an organization to assess its capabilities relative to the CSF and a crosswalk document that maps the CRR to the NIST CSF is included as a component of the CRR self-assessment package. Though the CRR can be used to assess an organization's capabilities, the NIST CSF is based on a different underlying framework and as a result an

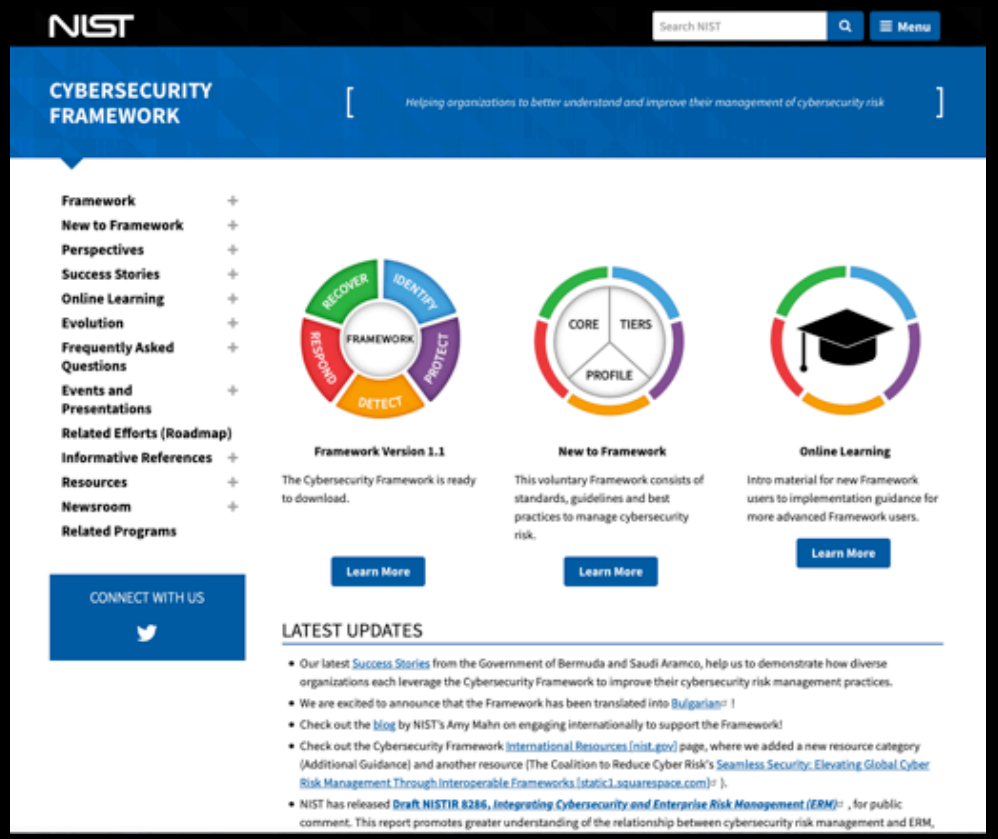
Cybersecurity	Cyber Resilience
Definition: procedures followed, or measures taken to ensure the safety of a state or organization	Definition: the capacity to recover quickly from difficulties; toughness
Technologies and processes designed to protect an organization from cybercrime	Technologies and processes designed to keep delivering intended services in spite of cyber incidents
Works to reduce the risk of cyber attacks and to protect the organization from cyber theft/espionage	Works to ensure continuity on a wider scope, comprising cybersecurity and business requirements
Can work effectively without compromising the usability of other systems	Requires organization-wide culture shift the normalizes and embeds security best practices
Includes a business plan to resume operations in the event of a successful attack	Requires the organization to become agile and adaptable in the face of cyber-attacks and incidents

- ▷ Voluntary
- ▷ Non-technical
- ▷ Evaluation of operational resilience and cybersecurity capabilities of an organization.
- ▷ Compatible with C2M2 and NIST cybersecurity framework
- ▷ Self-assessment tools, and practice guidelines are available.

https://www.us-cert.gov/resources/assessments

CYBERSECURITY RISK POST COVID-19

NIST Cybersecurity Framework



Function
Identify
Protect
Detect
Respond
Recover

- ▷ Common and accessible language
- ▷ Adaptable to many technologies, lifecycle phases, sectors and uses
- ▷ Risk-based
- ▷ Based on international standards
- ▷ Guided by many perspectives – private sector, academia, public sector
- ▷ Focus is on security controls and measures
- ▷ Self-assessment and practice guidelines available

https://www.nist.gov/cyberframework

CYBERSECURITY RISK POST COVID-19

Cybersecurity Capability Maturity Model (C2M2) Program



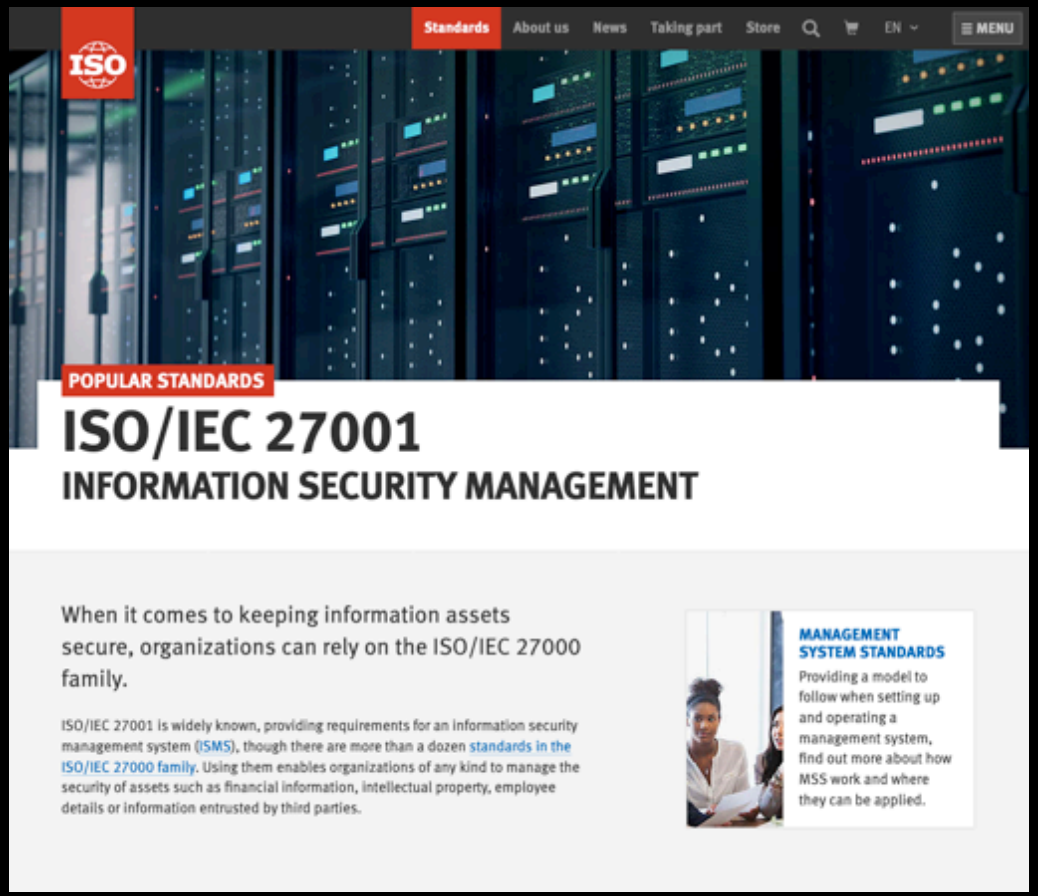
Maturity	Characteristics
MIL 0	Practices not performed
MIL 1	Initial practices are performed but may be ad-hoc
MIL 2	Practices are documented and more complete.
MIL 3	Activities are guided by policy and governance and practices are advanced

- Strengthening organizations' cybersecurity capabilities;
- Enabling organizations to effectively and consistently evaluate and benchmark their cybersecurity capabilities;
- Sharing knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities;
- Enabling organizations to prioritize actions and investments to improve cybersecurity; and
- Supporting adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- Self-assessment tools and practice guidelines available

https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

CYBERSECURITY RISK POST COVID-19

ISO/IEC 27001



- ▷Information Security Management Standard
- ▷Compatible with other ISO standards and guidelines
- ▷Adds a management layer to existing controls
- ▷Emphasizes continuous improvement
- ▷Third party self-assessment tools available

CYBERSECURITY RISK POST COVID-19

Webinar Outline

1 **RISK** → 2 → 3 **SAFETY**



1. Identify and assess cybersecurity uncertainty & risk
2. Develop and implement a cybersecurity strategy and plan
3. Measure and continual improve the effectiveness of your cybersecurity program



CYBERSECURITY RISK POST COVID-19

Steps to Strengthen your Defences

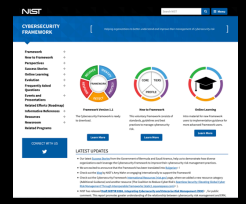
1. Evaluate Defences & Develop Improvement Roadmap
2. Select Standard & Conduct Detailed Assessments
3. Develop & Implement Detailed Improvement Plans



Cybersecurity Resilience Review



CyberSecure Program



NIST Cybersecure Framework



ES C2M2 Program



ISO 27001 Management System

Continuous Improvement

CYBERSECURITY RISK POST COVID-19

What will you do next?

RISK ? **SAFETY**



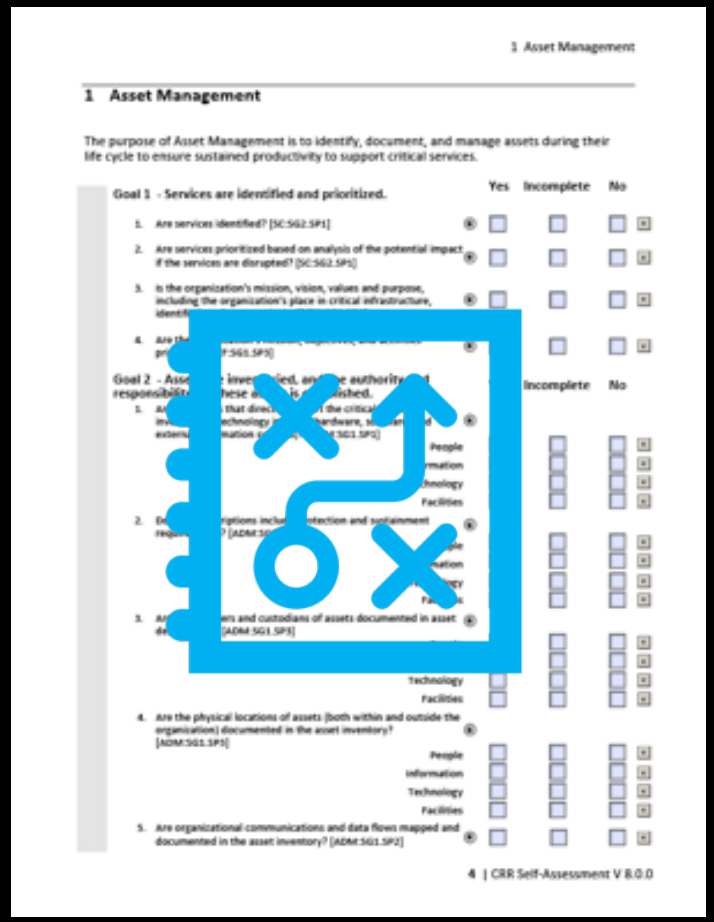
1. Have you identified the risks that really matter?
2. Do you have a cybersecurity strategy and plan?
3. Are your defences strong enough?



Cybersecurity is a business problem that requires a business solution

CYBERSECURITY RISK POST COVID-19

Evaluate Defences – CRR Assessment & Improvement Roadmap



1 Asset Management

1 Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.

Goal 1 – Services are identified and prioritized.	Yes	Incomplete	No
1. Are services identified? [SC:SG2.SP1]			
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]			
3. Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified?			
4. Are the [illegible] [SG1.SP3]			

Goal 2 – Asset [illegible] ied, and [illegible] authority and responsibility [illegible] these [illegible] is established.	Yes	Incomplete	No
1. [illegible] that direct [illegible] the critical [illegible] technology [illegible] hardware, [illegible] and external [illegible] [SG1.SP1]			
People			
[illegible]mation			
[illegible]hnology			
Facilities			
2. [illegible]riptions including protection and sustainment requirements? [ADM:SG1.SP2]			
[illegible]ple			
[illegible]mation			
[illegible]gy			
[illegible]ities			
3. [illegible]ers and custodians of assets documented in asset [illegible] [ADM:SG1.SP3]			
Technology			
Facilities			
4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]			
People			
Information			
Technology			
Facilities			
5. Are organizational communications and data flows mapped and documented in the asset inventory? [ADM:SG1.SP2]			

▷Facilitated Cyber Resilience Review

- Asset Management
- Controls Management
- Configuration and Change Management
- Vulnerability Management
- Incident Management
- Service Continuity Management
- Risk Management
- External Dependencies Management
- Training and Awareness
- Situational Awareness

▷Assessment Summary & Recommendations

▷Cyber Safety Improvement Roadmap

CYBERSECURITY RISK POST COVID-19

Cybersecurity Resilience Review Assessment

If you are interested in improving your cybersecurity program, please contact:



Raimund Laqua, PMP, P.Eng

Ray.laqua@leancompliance.ca
(289)799- 9655
www.leancompliance.ca



Emerai Morgan

Emerai.morgan@netaccess.ca
(905)524-2001 x 243
www.netaccess.ca

CYBERSECURITY RISK POST COVID-19

LEAN COMPLIANCE

NETACCESS

Bow-tie Analysis

