


# Building an Information Security Program: The 12 Step Method

April 2017



**Gary Perkins, MBA, CISSP**  
*Chief Information Security Officer (CISO)*  
*Executive Director, Information Security Branch*  
*Government of British Columbia*

# 10 step program

- Step 1: Ensure you have executive support for security (ask!)
- Step 2: Ensure you are well aligned with government and ministry strategy, goals, priorities (compare with security vision, mission, goals and they should be well aligned)
- Step 3: Understand organizations' risk appetite (likely med or med-low)
- Step 4: Focus on a risk-based approach
- Step 5: Focus on security by design – building security in from the ground up; ensure security review as part of capital allocation process
- Step 6: Determine your approach (risk, compliance, or capability)
- Step 7: Update and review high level risk registry quarterly
- Step 8: Identify what is secure enough for your organization – what is sufficient to mitigate risk to an acceptable level? What is defensible? (eg. hygiene + compliance)
- Step 9: Identify a security standard appropriate for your organization and measure compliance, identify gaps, prioritize, and remediate
- Step 10: Assemble components into a ministry specific information security program

# Step 1: Ensure you have executive support

- security culture and support for security comes from the top
- ensure a common understanding of the threat
- how do you find out whether you have support?  
Ask!



# Step 2: Align with organization's vision, mission, goals, strategy

Example starting with “Making a World of Difference” International Plan



Create a culture of exchange through STUDENT MOBILITY

Enhancing the INTERNATIONAL STUDENT EXPERIENCE






Providing INTERCULTURAL CURRICULA for a global-ready institution

Making a vital impact through INTERNATIONAL ENGAGEMENT

Establishing an EXTRAORDINARY ENVIRONMENT FOR INTERNATIONALIZATION

# Step 2: Align with organization's vision, mission, goals, strategy

Example starting with “Making a World of Difference” International Plan

Program	Categories				
	Enhancing the INTERNATIONAL STUDENT EXPERIENCE 	Establishing an EXTRAORDINARY ENVIRONMENT FOR INTERNATIONALIZATION 	Providing INTERCULTURAL CURRICULA for a global-ready institution 	Making a vital impact through INTERNATIONAL ENGAGEMENT 	Creating a culture of exchange through STUDENT MOBILITY 
Security Education and Awareness	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enhanced identity & authentication	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure collaboration space	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enabling mobile device use with endpoint/device security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## Step 3: Understand organization risk appetite



- low
- medium
- high
- very high



# Step 4: Take a risk-based approach and examine the forces changing the risk profile



# Step 5: Focus on Security by Design

Build security in from the ground up & insert review in capital allocation process

## IM/IT Capital Investment - Security Considerations

No.	Area	Questions
1	<b>Security By Design</b>	How will you demonstrate that information security has been considered in each phase of your system/service development and implementation plans (i.e. define security requirements, define security architecture, engage security SMEs-MISO, DBA, Developers and System Administrators)?
2	<b>Critical System-Availability</b>	Is your system/service critical? If Yes, what are your plans to comply with the "Critical Systems Standard" including establishing, maintaining and exercising DRP?
3	<b>Confidential information</b>	Does your service/system handle (process, store or transmit) confidential information (including personal information)? If Yes, what are your plans to protect this confidential information?
4	<b>Internal/Network access</b>	Does your system/service operate within the BC Government network? If Yes, What are your plans to manage security risks related to this internal network access (e.g. vulnerability scans)? (Consider Information Security Policy).
5	<b>External/Internet access</b>	Is any information within your system/service accessible from the internet or sites external to BC Government network? If Yes, What are your plans to manage security risks related to this internet/external access (e.g. vulnerability scans)? (Consider Information Sharing agreement).



# Step 5: Focus on Security by Design

## IM/IT Capital Investment - Security Considerations

6	<b>Operational Security</b>	What are your plans to ensure ongoing operational security (i.e. change management, patch management, access review, incident management, investigation, and vulnerability management)?
7	<b>Access Control</b>	What are your plans to manage access to system/service and its information?
8	<b>Outsourced</b>	Is any component of the service outsourced or performed by a third party or performed by a contractor?  If Yes, what contractual agreements are needed (e.g. NDA, Contract, SLA, OLA, Security/Privacy schedules) for each vendor/third party/contractor?
9	<b>Cloud</b>	Does your service/system use cloud for any function?  If Yes, what are your plans to protect information in the cloud?  (Consider if your cloud-based service/system meets your business security requirements).
10	<b>Regulatory Compliance</b>	Besides PCI-DSS & FOIPPA, Are there any acts, standards or regulations that your service/system must comply with from information and information management perspectives?
11	<b>Credit Cards</b>	Does your service/system handle (process, store or transmit) Credit Cards?  If Yes, what are your plans to comply with PCI-DSS?
12	<b>Security Review</b>	What are your plans to ensure that your system/service is built/implemented securely (e.g. Security testing, Completing a STRA, Certification/Review by third party)?  Will the system/service meet the requirements of BC Government security policies & standards?

## Step 6: Consider maturity level in approach

Maturity	Approach	Steps
Low	Risk register	<ol style="list-style-type: none"><li>1. identify key risks</li><li>2. rate inherent risk and trend</li><li>3. identify controls in place</li><li>4. rate residual risk</li><li>5. compare with risk appetite</li></ol>
Medium	Standards-based compliance	<ol style="list-style-type: none"><li>1. identify an appropriate standard for your organization</li><li>2. assess present state</li><li>3. determine desired target state based on appropriate controls</li><li>4. gap analysis</li><li>5. plan, prioritize</li><li>6. execute</li></ol>
High	Capability-based	<ol style="list-style-type: none"><li>1. review trends in environment</li><li>2. focus on changes in risk posture</li><li>3. consider relevant updates in standards</li><li>4. augment with increased capabilities</li></ol>

# Step 7: Update and review risk registry regularly

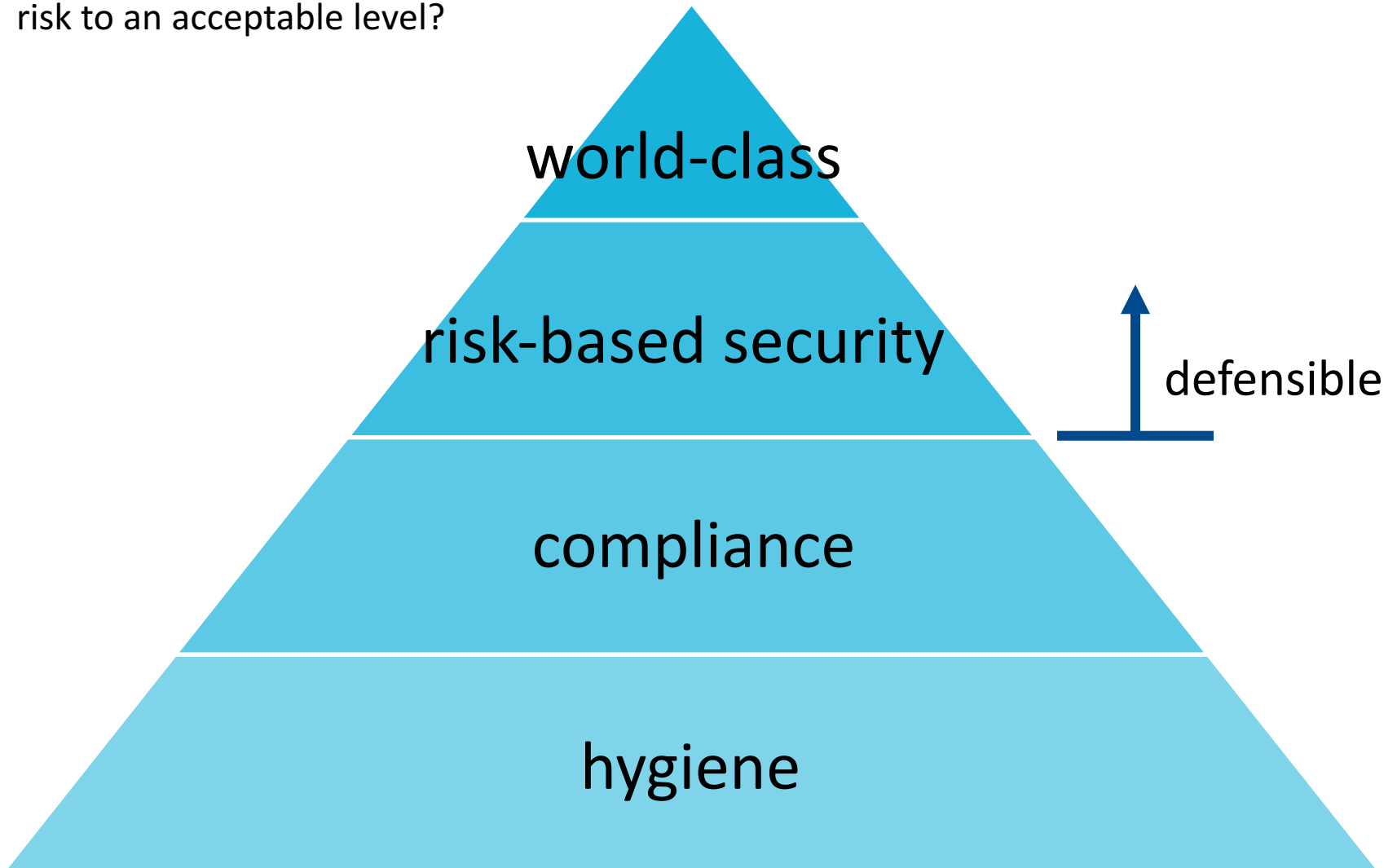
Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Network Security	Insufficiently proactive approach on identification of threats and vulnerabilities in network infrastructure and timely mitigation may result in network outages and exposure	H	↑	•		
Data Security	Insufficient application of adequate security controls, heightened by limitation of vulnerability management tools resulting in inability to identify and mediate data breaches, theft, destruction or manipulation of data	H	↑	•		

# Step 7: Update and review risk registry regularly

Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Physical Security	Insufficient security awareness and physical security controls may fail to mitigate physical risk exposures and could impact staff and citizen safety.	M	↔	•		
Property Risk	Inconsistent and inadequate preventative measures around key building systems (such as HVAC, electrical, fire suppression / detection) maintenance, housekeeping (i.e., storage of combustibles) and safety procedures may result in avoidable loss or damage of assets such as network, infrastructure, computing that could impact internal processes or client service and delivery.	M	↔	•		
Identity Theft & Fraud	Increased incidents of identity theft and fraud globally, including constantly evolving card related fraud, have heightened the need for appropriate controls to safeguard assets, and protect team member and citizen privacy and brand.	M	↑	•		

## Step 8: Define target state

Identify what is secure enough for your organization – what is sufficient to mitigate risk to an acceptable level?



## Step 9: Consider a standards-based approach

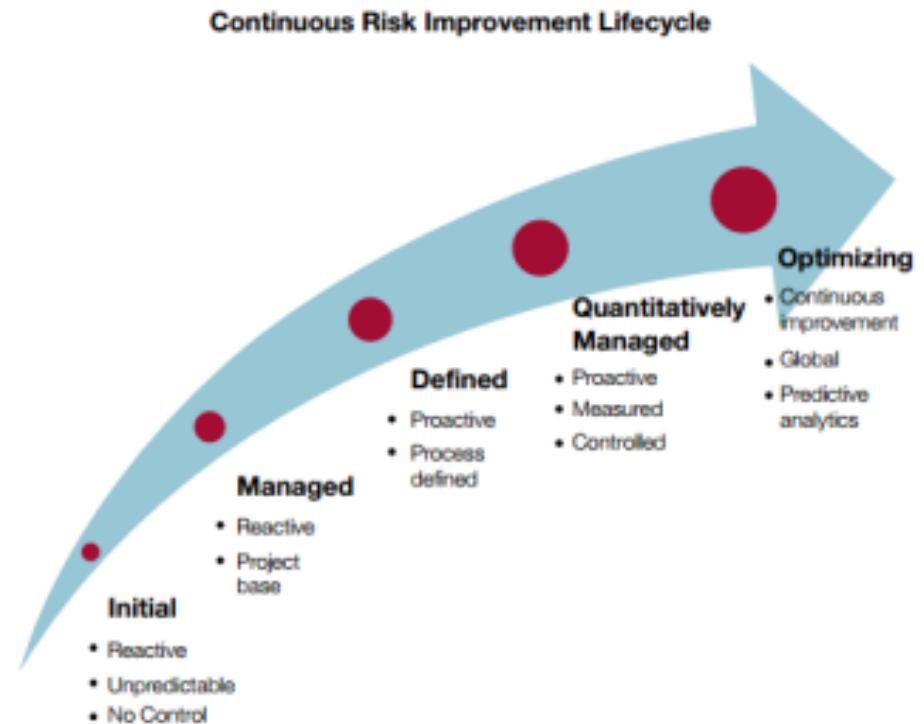
Identify a security standard appropriate for your organization and measure compliance, identify gaps, prioritize, and remediate

- ISO 27000 series (eg. ISO 27001, 27002)
- NIST 800-53
- Industry specific (eg. NERC)
- Others: CIS, SANS

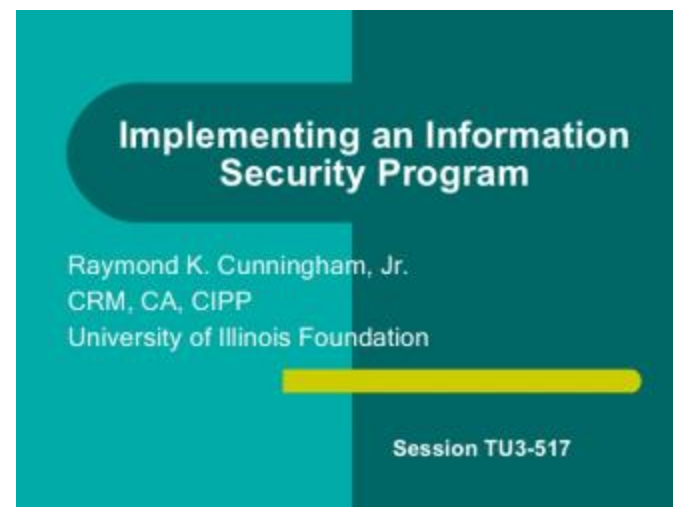
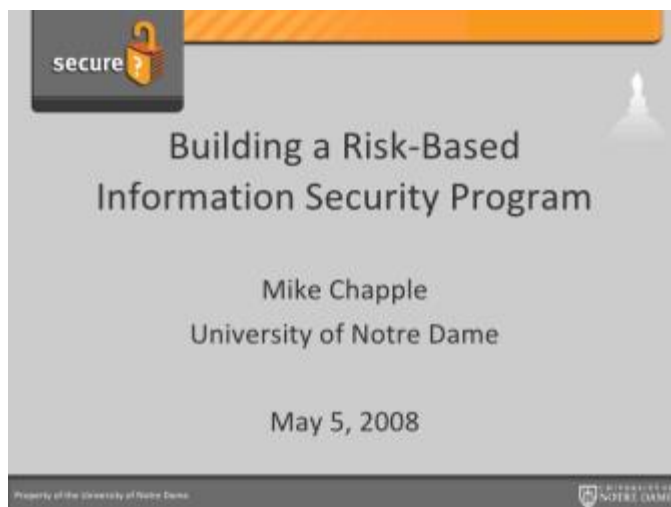
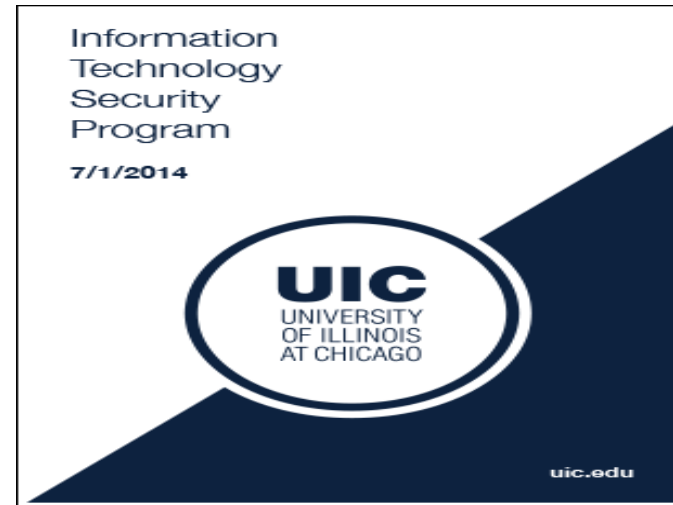
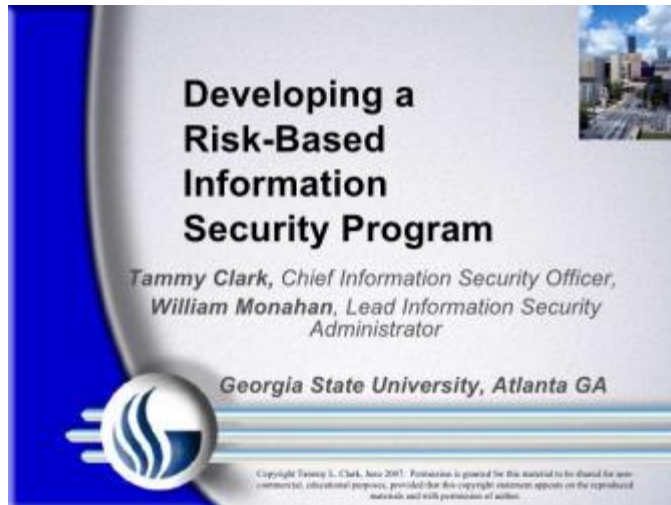


# Step 9: Capability Maturity Model

- 0 – Not Implemented
- 1 – Initial
- 2 – Repeatable
- 3 – Defined
- 4 – Managed
- 5 – Optimized



# Step 10: Assemble components into a program



## Step 11: Communicate the plan appropriately

- know your audience
- use their language
- communicate appropriately
- make it relevant
- demonstrate alignment with strategy
- ensure they understand why they should care

# Step 12: Execute the plan

- don't boil the ocean
- understand your present level of maturity
- set achievable goals
- break them down into doable chunks
- measure the progress
- communicate the progress
- celebrate the successes

# Summary

Security programs will be successful when they are:

- supported by executive
- aligned with government and ministry goals
- risk-based, aligned with business and risk appetite
- standards-based, evolve over time
- capture present and target state accurately
- plans are realistic and actionable
- resourced effectively
- focused on building security in from the ground up
- measured/monitored
- continuous improvement
- communicated appropriately
- executed on

# Questions?



**OCIO**  
Office of the Chief Information Officer