Information Security Council Lightning Round

Moderated by Isaac Straley, Chief Information Security Officer, University of Toronto

Oct. 23, 2019

Cyber Security Awareness Month
ONE TEAM. ONE GOAL. October 2019

Openness = Academic Freedom + Shared Governance

Constantly Changing Users ◄——► Profoundly Decentralized

Collaborative Research Around the Globe

New Students, New Devices

Hundreds of Autonomous Units

Wide Range of IT Literacy

Few Enforcement Mechanisms

Determined to Stay "Free"

"Higher Ed is by design focused on transparency, with as few restrictions as possible to information sharing. The bedrock mindset tilts toward academic freedom."

CIO, Regional Masters University

Uniquely Risky

"Higher education is one of the most heavily regulated industries in the U.S.- and it has more risk-producing constituencies than almost any other industry."

Leta Finch, Aon Risk Management Services

Source: EAB Interviews and Analysis

POLICY

The University of Toronto adopts this ***Policy on Information Security and the Protection of Digital Assets*** as a measure to protect the privacy, confidentiality, integrity, and availability of Digital Assets, including information systems that store, process or transmit data. This *Policy* applies to all academic and administrative units, third-party agents of the University, as well as any other University affiliate that is authorized to access institutional data, services and systems.

All University of Toronto campuses, divisions, departments and other administrative or academic organizational units shall deploy and use IT systems and services in a manner consistent with the University's research and teaching mission, while vigilantly mitigating security risks to Digital Assets, including data during storage, transit, use and disposal. It is the obligation of all University community members to protect information that is created by them and stored by the University and its authorized delegates to its defined principles and standards.

OBJECTIVES

- The broad purpose of the ISC is to provide guidance to the university in matters of information security in the context of the university's, mission, objectives, and obligations.
- Act as a steering committee for the information security program, including a recommendation for the final resource allocation decisions for the annual security strategy plan.
- As per policy, ensure every academic and non-academic unit is appropriately covered by an information risk management plan.

MEMBERSHIP

Name	Role	Unit	Affiliation
Ron Deibert	Co-Chair	Political Science	Faculty
Isaac Straley	Co-Chair	ITS	Staff
Sam Chan	Member	Medicine – IT Director	Staff
Leslie Shade	Member	I-School	Faculty
Sian Meikle	Member	Library	Faculty
VACANT	Member		Faculty
Michael Stumm	Member	ECE	Faculty
Zoran Piljevic	Member	UTSC – IT Director	Staff
Rafael Eskenazi	Member	Privacy Office	Staff
Heidi Bohaker	Member	History	Faculty
VACANT	Member	Physics	Grad Student
Bo Wandschneider	Ex-officio	ITS	Staff

WORKING GROUPS

- Incident Response Planning
- Procedures, Standards and Guidelines
- Education & Awareness
- Risk, Compliance, Metrics and Reporting
- Research

Information Security Incident Response Planning

Information Security Council (ISC) Working Group

October 23, 2019

UNIVERSITY OF TORONTO

Information Security Incident

Not a matter of if, but when …

A few facts:

- By 2020 there will be roughly 200 billion connected devices
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
- More than 77% of organizations do not have a Cyber Security Incident Response plan

Source: https://www.cybintsolutions.com/cyber-security-facts-stats/

Information Security Incident Response Planning

"Every person who prepares is one less person who panics in a crisis."
— attributed to Mike Adamson, British Red Cross

Incident Detection

Incident intake

Incident Response

- Contain
- Eradicate
- Recover

Lessons Learned

- Establish Metrics
- Improve defenses
- Establish root cause

Incident Response Planning

Key focus areas:

- Document common incident types
- Define criteria for prioritizing incidents
- Develop and conduct tabletop exercises
- Develop response playbooks and checklists
- Provide input into Information Security Awareness Program

More information on the ISC and its working groups:
http://main.its.utoronto.ca/about/committees/information-security-council-isc/

LIGHTNING ROUND

Information Security Council Education and Awareness Working Group

Oct 23, 2019

Presented by Carrie Schmidt, Education and Awareness (Communications), Senior Manager, Information Technology Services and Information Security Council Education and Awareness Working Group Chair

OUR MANDATE

1. Foster communication, promote awareness and education about information security with the goal of reducing the risk of unauthorized or malicious compromise of data and services.
2. Activities are focused on four audiences: **faculty**, **students**, **technical staff** and **non-technical** staff.
3. Provide communications, education and awareness support, recommendations and expertise to information security council initiatives (and working groups).

We strive for a **tri-campus and inclusive** approach.

COMMITTEE MEMBERS

- Will Campbell, HR & Equity
- John Di Marco, Department of Computer Science
- Humberto Ferreira, Division of University Advancement
- Hayley Fuller, HR & Equity
- Sue McGlashan, Information Security, Information Technology Services
- Kathleen McLeod, Education and Awareness (Communications), Information Technology Services
- Rose O'Higgins, Faculty of Arts & Science
- Daniel Ottini, Internal Audit Department
- Marden Paul, Planning, Governance and Assessment, Information Technology Services
- Andrea Russell, Office of the Vice-President and Provost
- Carrie Schmidt, Education and Awareness (Communications), Information Technology Services
- Alex Tichine, Information Security and Enterprise Systems, Faculty of Engineering
- Mike Wiseman, Information Security, Information Technology Services
- Cheryl Ziegler, Office of Student Life

TEAM SHOUT OUT

ANN-MARIE, SENIOR COMMUNICATIONS OFFICER

CARRIE, SENIOR MANAGER

KIM, COMMUNICATIONS COORDINATOR

EARL, WEB DEVELOPER

KATHLEEN, EDUCATION AND AWARENESS OFFICER

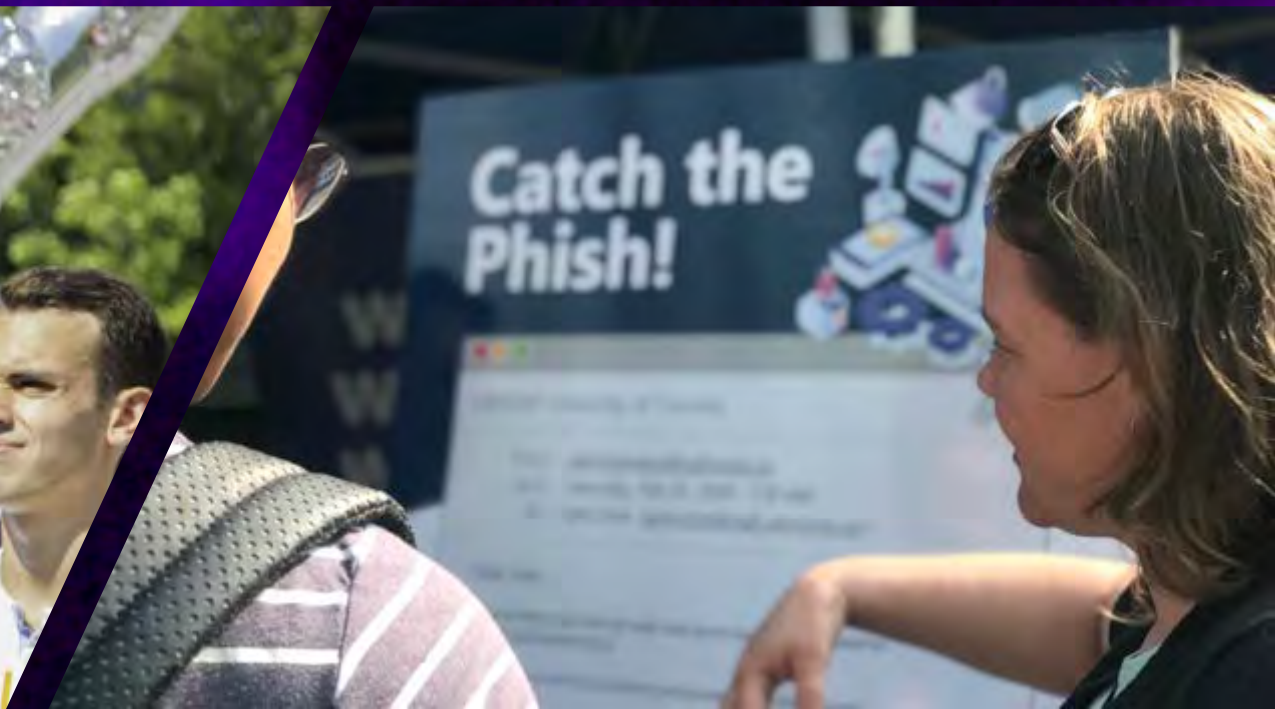
The Education and Awareness team is a growing group of creative communication professionals that are helping to advance the objectives, pillars, initiatives and culture outlined in the IT@UofT Strategic plan.

The team supports the Information Technology division, including the Office of the Chief Information Officer. They provide innovative planning, strategy, event planning, writing, design and editing services and solutions.

ACTIVITIES

PHISHING ALERT!

LEARN MORE AT
SECURITYMATTERS.UTORONTO.CA



Cyber Security Awareness Month

ONE TEAM. ONE GOAL. October 2019

Tri-campus community events and activities throughout October.
Visit Security Matters for updates and get involved today!

@ITSUOFT | @UOFTCYBERAWARE
#oneteamonegoal #securitymatters
Learn more at securitymatters.utoronto.ca

UNIVERSITY OF TORONTO

DATA PRIVACY DAY, JAN. 28, 2019

OPEN WORLD. PRIVATE DATA.

SECURITYMATTERS.UTORONTO.CA

LET'S TALK ABOUT DATA PRIVACY.

VISIT OUR POP-UP BOOTH AT THE **BAHEN CENTRE** FROM 10:30 A.M. TO 4:30 P.M. WHERE YOU CAN:
MEET U OF T'S NEW CHIEF INFORMATION SECURITY OFFICER **ISAAC STRALEY** FROM 11 A.M. TO 12:30 P.M.
AND **RAFAEL ESKENAZI** DIRECTOR, INFORMATION AND PROTECTION OF PRIVACY FROM 2:30 P.M. TO 3:30 P.M.
READ OUR ARTICLES.
JOIN THE CONVERSATION ON SOCIAL MEDIA.
AND MORE...

@UOFTCYBERAWARE
#CYBERSECURITY
#PRIVACYAWARE
#DATAPRIVACYDAY

SECURITY MATTERS

Safeguarding your data while travelling

We all share in the responsibility of protecting the University of Toronto's (U of T's) data, and we are all responsible for our devices and the safety of the data they contain. When travelling outside of Canada, cyber security threats are very real: malicious attacks can intercept calls and internet traffic, or demand direct access to our devices. This tip sheet offers good practices for any U of T staff, student or faculty member who travels on behalf of the University.

BEFORE YOU TRAVEL

1. **Make sure the software on all your travel devices is up to date.** Updates to your computer software and mobile device applications will work to fix known security gaps.
2. **Empty the devices you will take with you.** You should not travel with confidential data on your mobile phone and computer. Create temporary online data stores with only the data you need for the trip.
3. **Use a "burner" device.** Burners are inexpensive devices that can be used on a temporary basis when travelling. If you choose to bring your own personal devices, back up your information with a cloud service or a secure device you leave at home.
4. **Before you depart, turn off "remember me" and wipe stored passwords from all travel device applications and browsers.** Change your existing device and online account passwords to temporary travel passwords. To keep secure records of your new passwords, use a password manager such as Password Safe or KeePass.
5. **If you need to bring a portable hard drive or USB drive with you, ensure the devices are trusted and encrypted.** Never use an unfamiliar or untrusted device for this purpose.
6. **Make sure all devices and accounts are protected by strong passwords.** Where possible, set up multi-factor authentication (also known as MFA, 2FA, two-factor authentication and two-step authentication). This will ensure that the only person with access to your accounts is you.
7. **Ensure you have the departmental authorization to take data off-site.** Always check with your departmental contact first.

SECURITY MATTERS
SECURITYMATTERS.UTORONTO.CA

UNIVERSITY OF TORONTO

Have you received a phishing email?

If you're unsure, watch out for these signs:

1. Sender is an unknown email contact OR sender is a known email contact, yet the message and/or links contained are out of the ordinary.
2. The overall content seems odd, unexpected and/or conveys a false sense of urgency.
3. Contains instructions to click a link, download an attachment, enter your credentials and/or send money or gift cards.
4. Includes phony links (tip: hover over link(s) with your cursor to see where they actually lead).
5. Has spelling or grammatical errors, yet beware that many sophisticated attackers will use professional language too.

@ITSUOFT | @UOFTCYBERAWARE

SECURITYMATTERS.UTORONTO.CA

Cyber Security Awareness Month
ONE TEAM. ONE GOAL. October 2019

UNIVERSITY OF TORONTO

TAKE THE DATA PRIVACY DAY CHALLENGE

THREE STEPS IN FIVE MINUTES TO PROTECT YOUR PRIVACY

@ITSUOFT @UOFTCYBERAWARE
SECURITYMATTERS.UTORONTO.CA

JOIN US!

- We are looking for more members of the University tri-campus community to join our working group.
- Please contact Carrie Schmidt if you are an interested student, University of Toronto Mississauga, University of Toronto Scarborough or University of Toronto St. George community member.
    - **Email:** carrie.schmidt@utoronto.ca
    - **Phone number:** 416-946-8155

Procedures, Standards & Guidelines

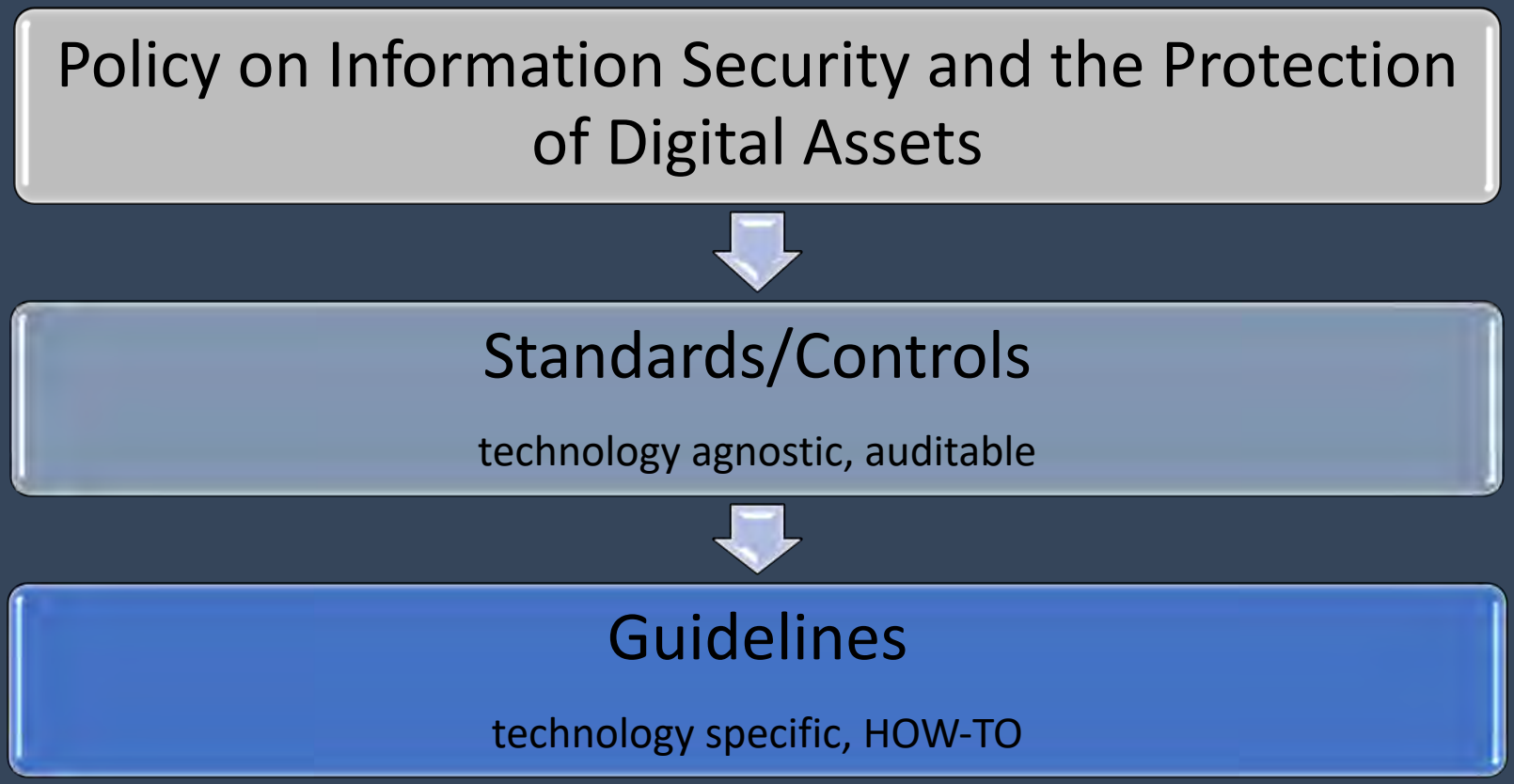
D. Gruner, J. Di Marco, D. Ottini, G. Raposo,
J. Bate, J. Pristupa,
Priya Murugaiah, M. Wiseman

Oct 23, 2019

PROCEDURES, STANDARDS &
GUIDELINES WORKING GROUP
INFORMATION SECURITY COUNCIL

UNIVERSITY OF TORONTO

Procedures, Standards & Guidelines



Data Classification

Approved by ISC

1	Public
2	Internal
3	Confidential
4	Protected

Plus one!

https://isea.utoronto.ca/policies-procedures/standards/data-classification/

PROCEDURES, STANDARDS &
GUIDELINES WORKING GROUP
INFORMATION SECURITY COUNCIL

UNIVERSITY OF TORONTO

What's Next

ACCESS CONTROL
AUDIT AND ACCOUNTABILITY
CONFIGURATION MANAGEMENT
MEDIA PROTECTION
IDENTIFICATION AND AUTHENTICATION
AWARENESS AND TRAINING

Standards and Controls

NIST Special Publication 800-171

CIS Center for Internet Security

PROCEDURES, STANDARDS & GUIDELINES WORKING GROUP
INFORMATION SECURITY COUNCIL

UNIVERSITY OF TORONTO

Information Risk, Compliance, Metrics and Reporting Working Group - IRCMRWG

Sue McGlashan, John Kerr, Linda Ye, Paul Morrison, Steve Butterworth, Robin Wilcoxen, Kathleen McLeod

UNIVERSITY OF TORONTO

IRCMRWG Journey – Who?

- Chosen by IT@UofT Leaders
- Members are from IS, Risk, Audit, KPE, A&S, ITS.
- If you are interested in taking part, please reach out. If you know of interested academic faculty, please reach out.

IRCMRWG Journey - Mandate

Overall, develop an Information Risk Reporting **Framework** to:

- Develop security status metrics and a reporting **framework** that will allow units to **self-measure** their performance against metrics.
- **Track** the **progress** of remediation on risk items
- Provide feedback on the risk register.
- Develop a framework for auditors on the type and level of assurance most needed during corresponding audit cycles.
- Provide guidance to the campus Information Risk Assessment Process.

IRCMRWG Journey - Start

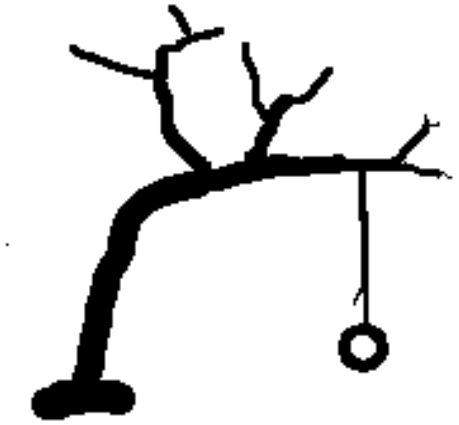
What is risk? (Information risk / risk?)

- The combination of the probability of an event and its consequence
  - The likelihood a threat will exploit a vulnerability x the impact
- Effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive and/or negative.

IRCMRWG Journey - Start

What is risk? (Information risk / risk?)

- The combination of the probability of an event and its consequence
  - The likelihood a threat will exploit a vulnerability x the impact
- Effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive and/or negative.

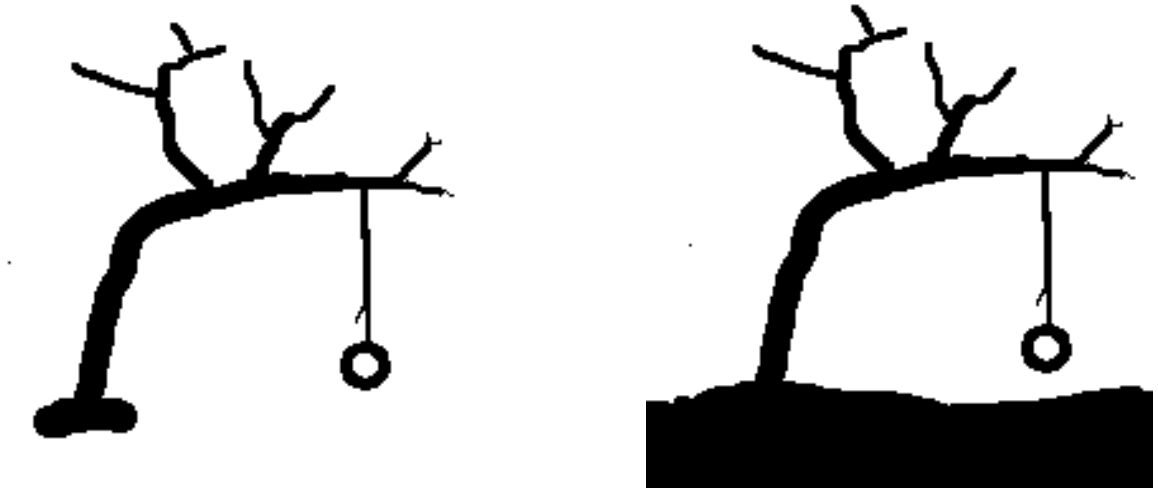


UNIVERSITY OF TORONTO

IRCMRWG Journey - Start

What is risk? (Information risk / risk?)

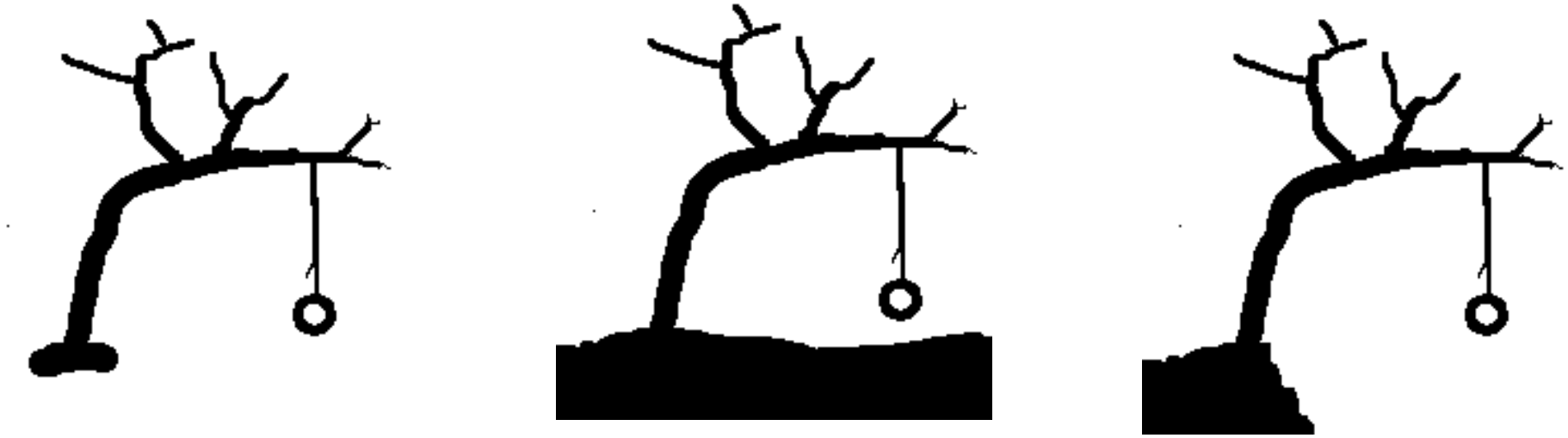
- The combination of the probability of an event and its consequence
  - The likelihood a threat will exploit a vulnerability x the impact
- Effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive and/or negative.



IRCMRWG Journey - Start

What is risk? (Information risk / risk?)

- The combination of the probability of an event and its consequence
  - The likelihood a threat will exploit a vulnerability x the impact
- Effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive and/or negative.



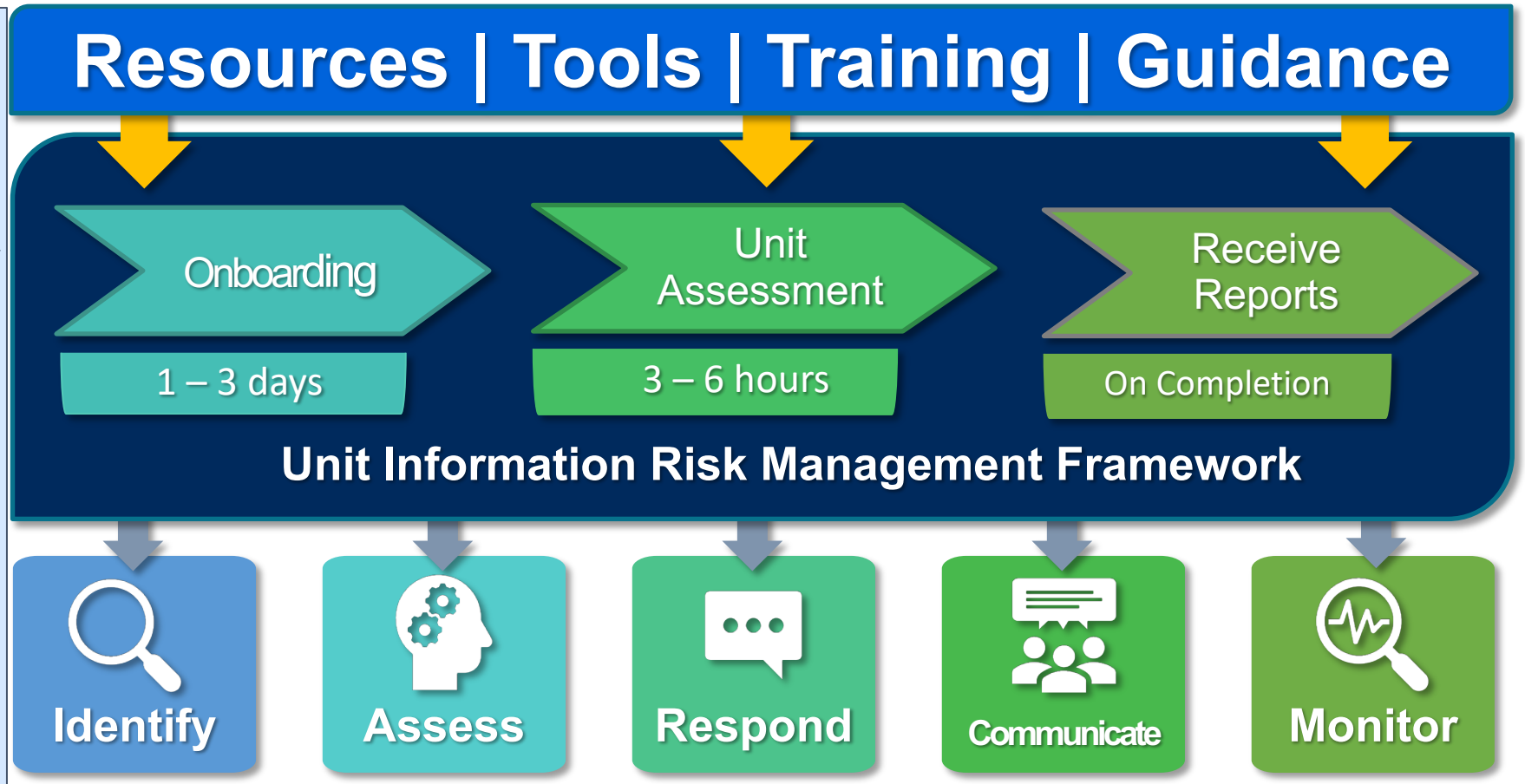
Through end 2019
Pilot – 30 Units

2020 Jan - Apr
Communications
Units Complete Assessment

2020 May - Aug
Program Evaluation

2020 Sep - Dec
Program Improvements

2021
Cycle repeats



Common framework for units to produce a *Unit Information Risk Management Program*

uoft.me/IRSA

IRCRWG - Information risk self-Assessment (IRSA)

Assessment Categories

- Management Risk
- Business Risk
- Purchasing Risk
- Human Resources Risk
- Facilities Risk
- Legal Risk
- Institutional Data Risk
- Information Technology Risk

Categories map to Cybersecurity Framework

University of Toronto Information Risk Scorecard

Unit Information	
Unit Number	2
Unit Name:	U of T Division Administrative

Overall Score				
Unit	Academic	Administrative	IT Services	U of T
1.9	2.0	1.9	1.8	1.9

Score Summary by Priority						
Comments		Unit	Academic	Administrative	IT Services	U of T
U of T Priorities	P1	1.8	2.3	1.8	1.8	2.0
		2.1	1.7	2.1	1.7	1.9
		1.0	2.5	1.0	2.0	1.7

Summary by Information Risk Functional Area						
Comments	Function	Unit	Academic	Administrative	IT Services	U of T
Information risk in the functional area eg. Legal requirements for data HR onboarding and offboarding processes	MANAGEMENT RISK	0.0	0.3	0.0	0.0	0.1
	BUSINESS RISK	0.5	1.5	0.5	1.7	1.2
	PURCHASING RISK	3.0	1.5	3.0	3.0	2.5
	HUMAN RESOURCES RISK	3.5	2.0	3.5	3.0	3.0
	FACILITIES RISK	3.3	3.5	3.3	3.0	3.3
	LEGAL RISK	3.0	2.5	3.0	1.0	2.3
	INSTITUTIONAL DATA RISK	2.0	2.4	2.0	2.0	2.2
	INFORMATION TECHNOLOGY RISK	1.9	1.8	1.9	1.6	1.7

UNIVERSITY OF TORONTO

Questions

Cyber Security
Awareness Month
ONE TEAM. ONE GOAL. October 2019