SEPTEMBER 2019 AUDIT COMMITTEE INFORMATION SECURITY UPDATE

ISAAC STRALEY

CHIEF INFORMATION SECURITY OFFICER

UNIVERSITY OF TORONTO

KEY POINTS

- Issues & risks continue to be tracked. Mitigation efforts are in progress but substantive risk remains.
- External assessment of overall security program is in progress - on-site interviews the week of November 4th and report in December.
- Information Security Council (ISC) is engaged to endorse external assessment targets, increasing governance maturity.
- Priority ITS security projects for FY19-20 are on track.
- Initial draft budget request for FY20-21 includes increases for security operations, risk assessment, and program support.
- Canadian Shared Security Operations Center (CanSSOC) proof-of-concept progressing.

ISSUES & RISKS – CISO HIGHLIGHTS

Item	Mitigation
Unknown data repositories	**Publish data classification**, **train on risk self-assessment**, create inventory project with units
Credit card security	**Request funding**, review overall program, secure & reduce payment channels
Network segmentation	**Deploy border firewall**, research access control tools, support network upgrades for modern routing,
Nation State threats	**Create travel guidelines**, **escalate as a risk,** improve attribution, focus on research
Compromised accounts & email security	**Focus on anti-phishing, move to native O365 protection tools, launch multi-factor authentication service(s), create identity strategic plan**
Unpatched devices & vulnerability management	**Deploy enterprise scanning tool**, increase scanner visibility, create device quarantine procedure, improve metrics
Incident response	**Focus ISC workgroup on playbook development**, tabletops for practical training with units, fill staff vacancies, **CanSSOC,** improve metrics
Security staffing	**Make hiring an ITS priority, support unit staffing needs, increase opportunities for students**

* **Bold** denotes in progress

PRIORITIES 2019-2020

Identify	Protect	Detect	Respond	Recover
Risk Assessment Program	Office 365 Security	Vulnerability Management Program	Incident Response Playbooks	Table-top Exercises
Security Standards Baseline	Gateway Firewall	Security Event Monitoring System	Establish retainers with incident response service provider(s)	Review Back-up Strategy
Data Classification	Multi-factor Authentication			
Awareness and Training	VPN			

EXTERNAL SECURITY ASSESSMENT

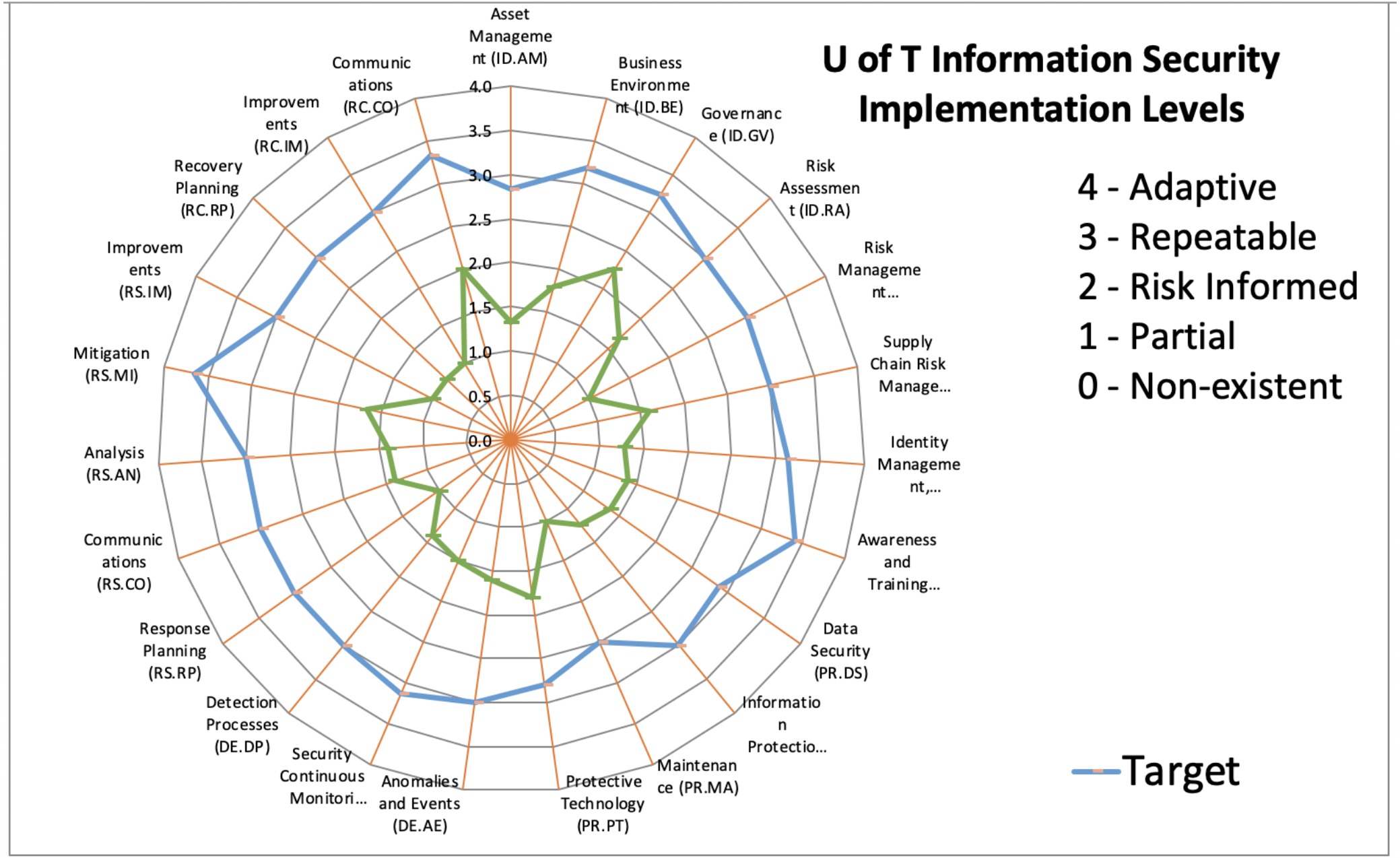
Summary

- Based on NIST Cyber Security Framework (CSF)
- “Hybrid” - EY & 3 U15/R1 CISOs
- Targets set with Information Security Council (ISC)
- Broad assessment – depth will be achieved with facilitated & self-assessment risk program
- CISO will respond with action plan and budget proposals

Update

- On-site interviews week of Nov 4

Timeline
July - August Selection & negotiation
September - October Scheduling, document review
November Interviews, report draft
December Report



UNIVERSITY OF TORONTO

EXAMPLE

INITIAL DRAFT BUDGET REQUEST

Proposals Carried Over From Last DAC

- Information Security Compliance and Risk Assessment

New Proposals

- Info Security Program Maturity and Enhancements
- Info Risk Program Maturity and Enhancements
- Identity & Access, Info Security Space, and CISO Support

In-negotiation Joint Proposals

- Research info security & risk analyst
- PCI compliance program