NCA

National/Provincial Report Data

Curtis L. Blais, Cybera's Shared CISO – Lead Technical Architect of the NCA
Masters of Leadership, CCNA, CCNP, GCIA, GCFW, WCSP, CISSP, CRISC
Harvard Cybersecurity Graduate

cybera

National Results

NCA – What is it?

- An annual, cybersecurity self-assessment
- Based on the NIST Cybersecurity Framework (CSF)
- Hosted on a commercial GRC Platform [Alyne]
- Supported by a National team spanning NREN Partners

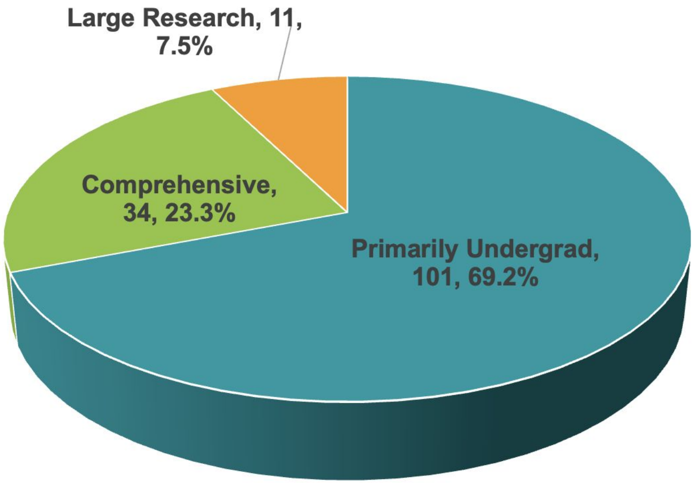
Participation

Total Eligible Organizations: **220**

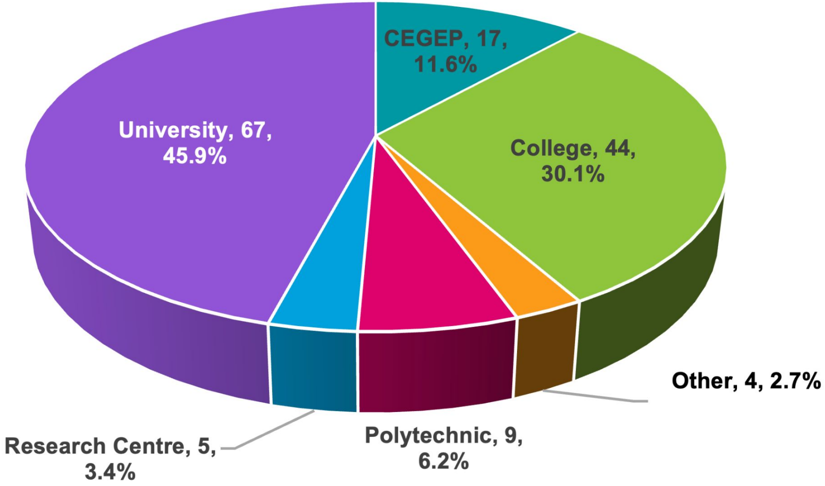
Total Participants: **146**

Total Participation Rate: **66%**

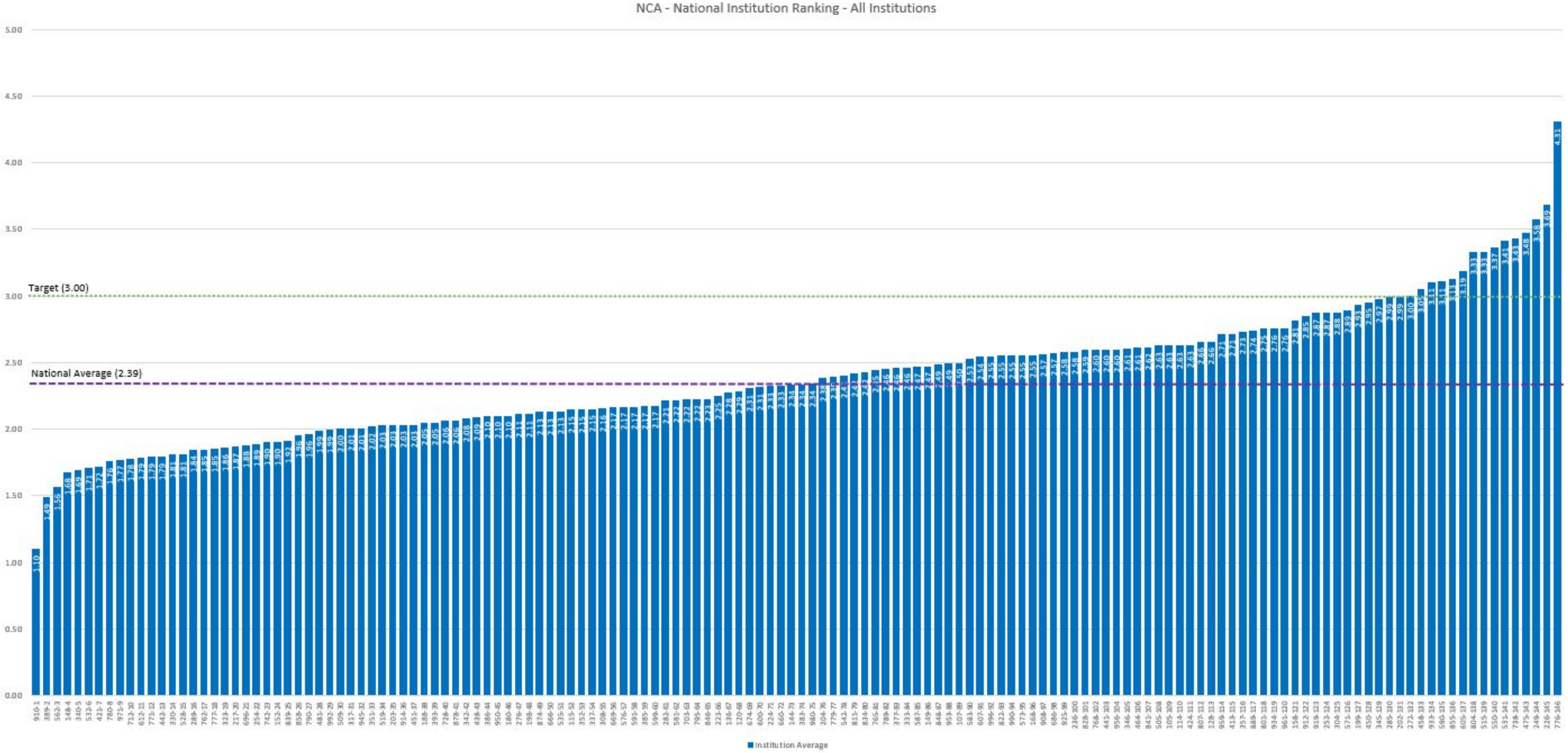
NATIONAL COUNTS - BY GCI



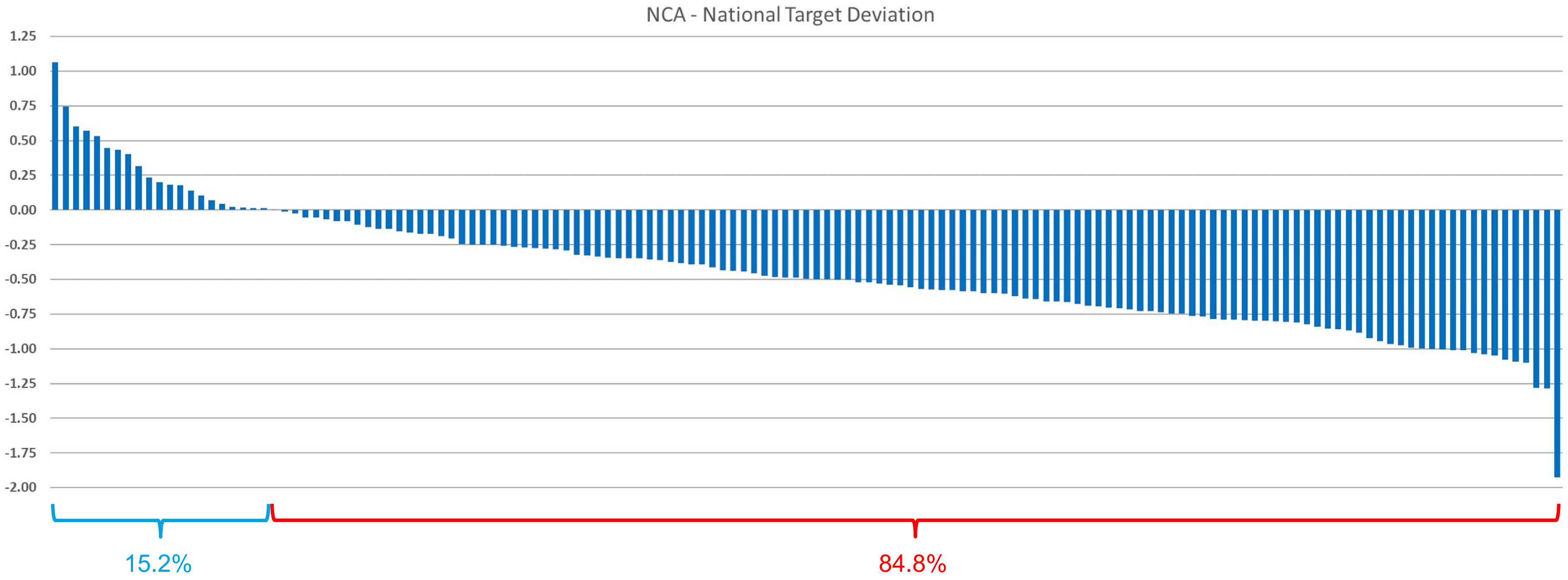
NATIONAL COUNTS - BY TYPE



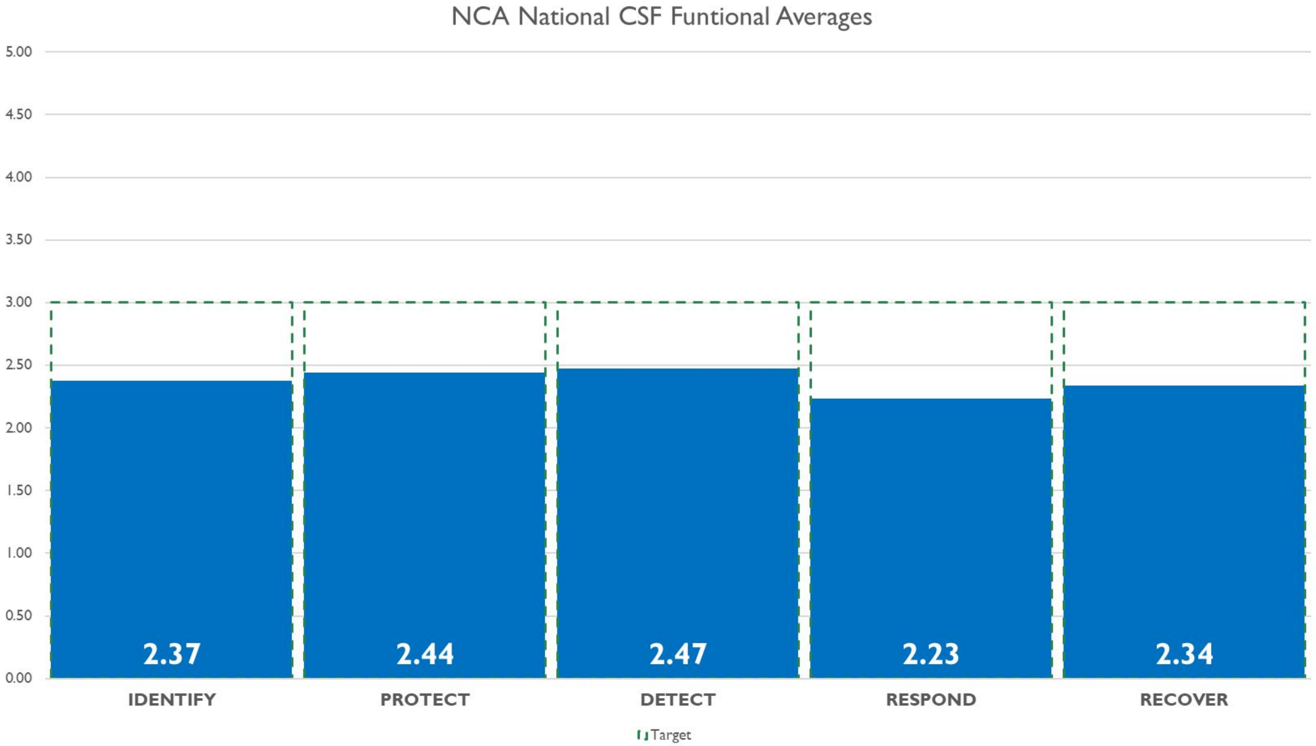
All Participants



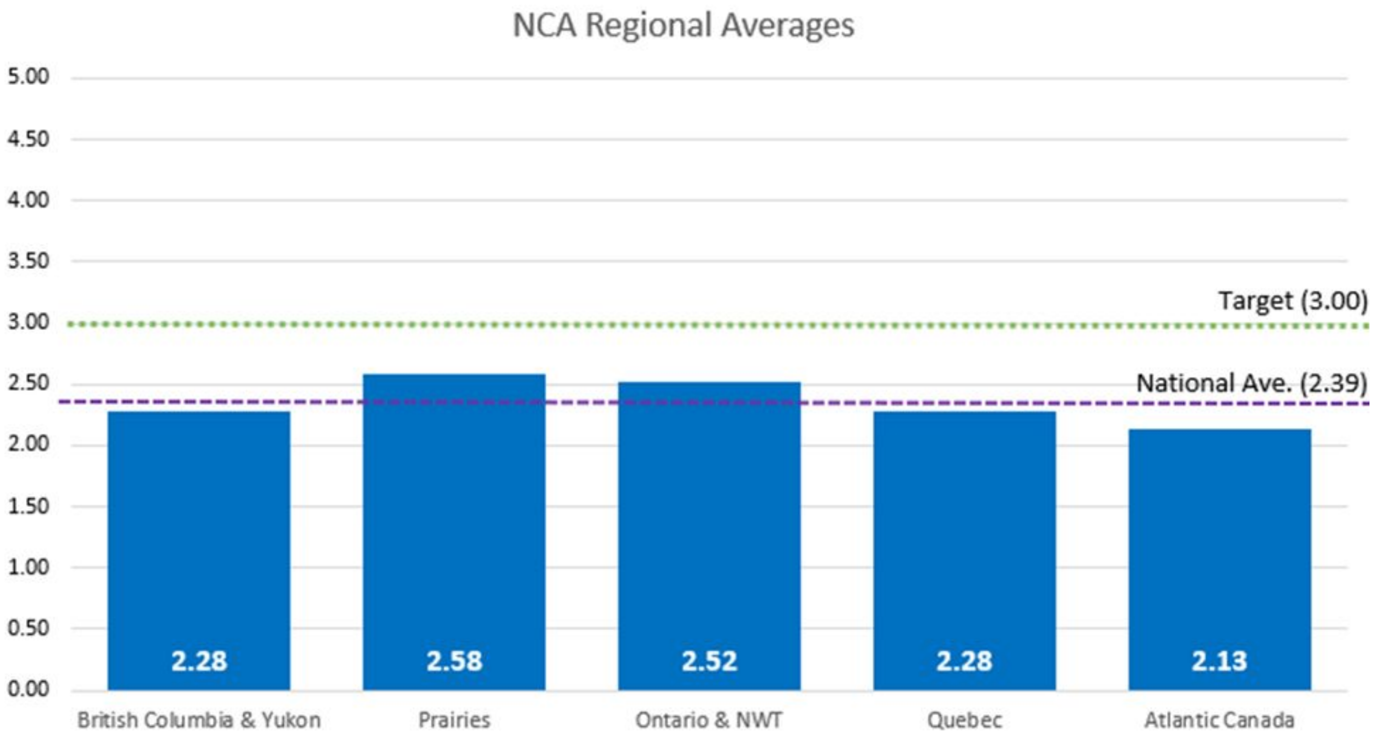
National Deviation



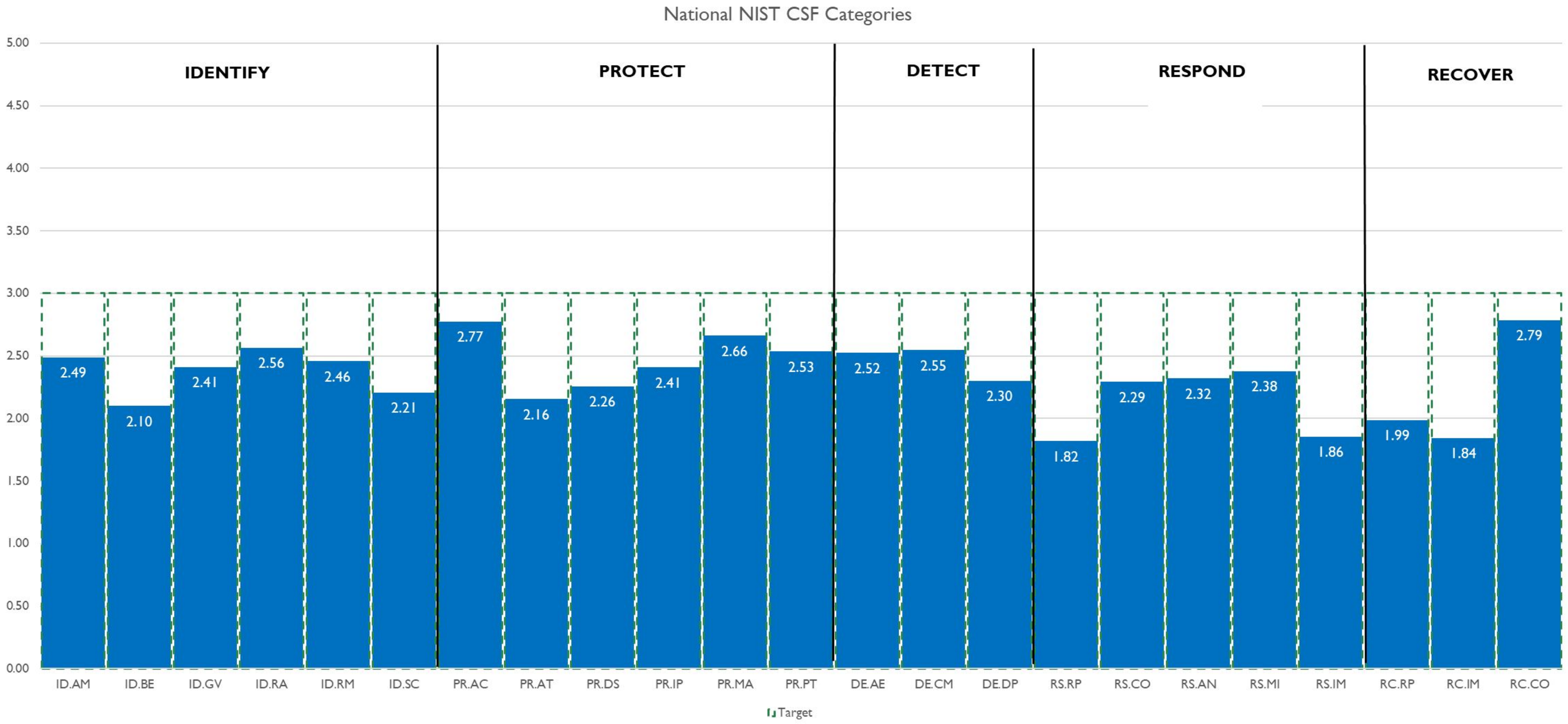
NIST Functions (National)



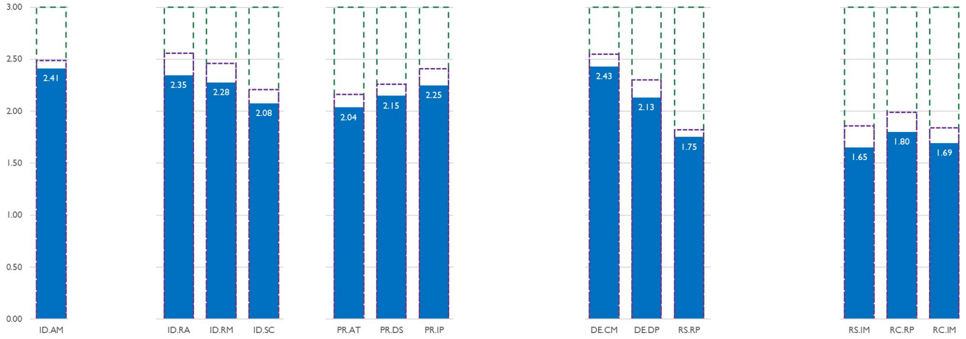
NIST Functions (Regional)



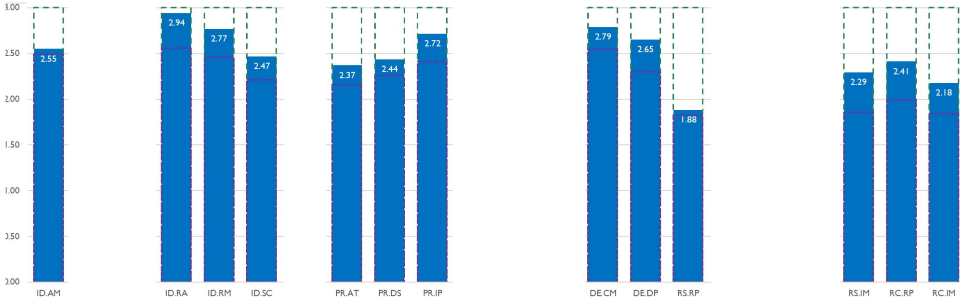
NIST Categories



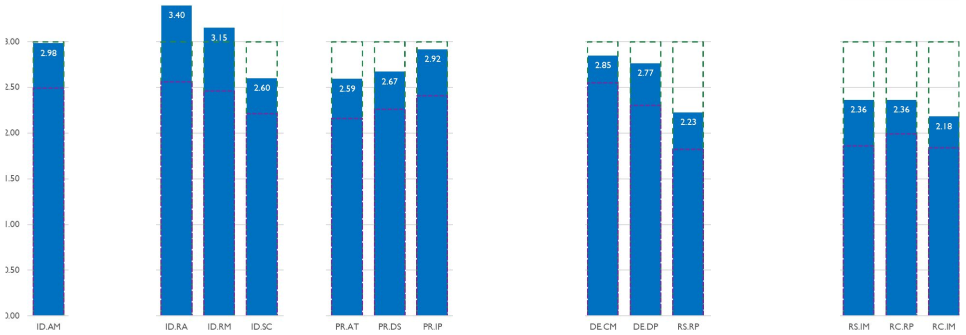
PRIMARILY UNDERGRAD



COMPREHENSIVE



LARGE RESEARCH



ID - Asset Management

ID - Supply Chain Risk Mgmt.

PR - Awareness and Training

PR - Data Security

PR - Info Protection Proc/Procedures

DE - Security Continuous Monitoring

DE - Detection process

RS - Response Planning

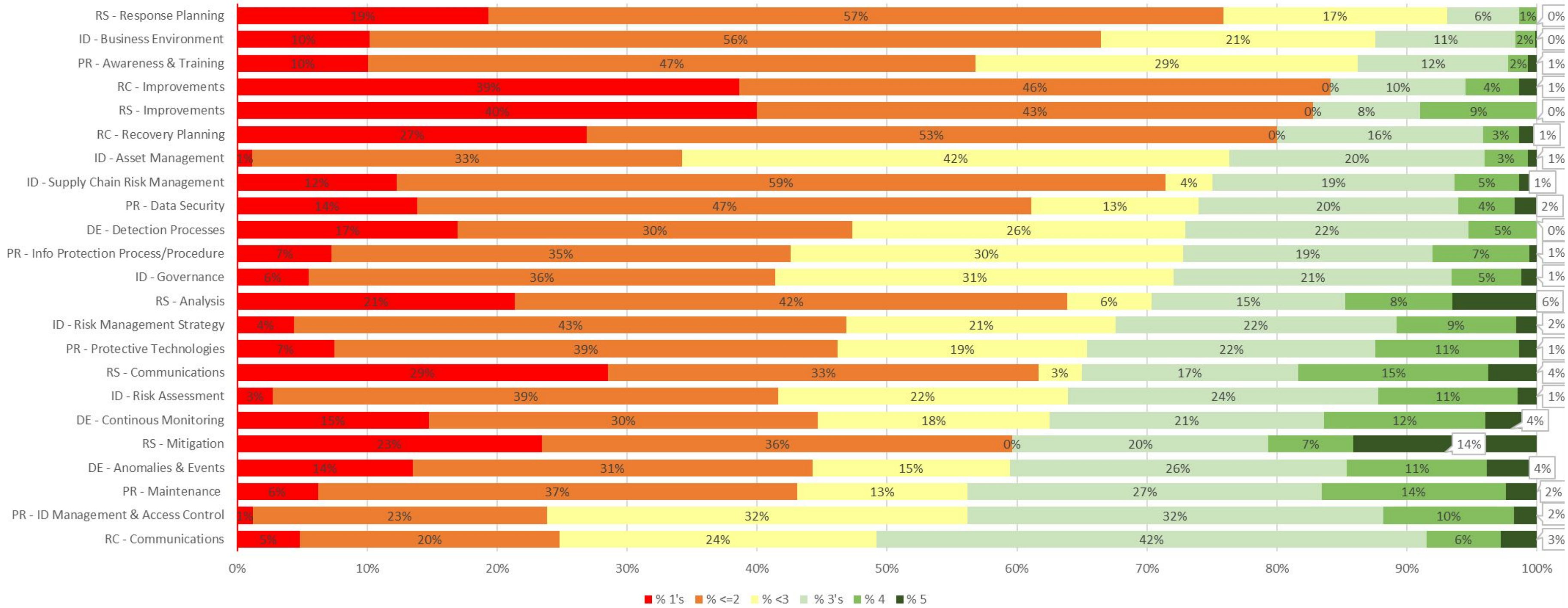
RS - Improvements

RC - Recovery Planning

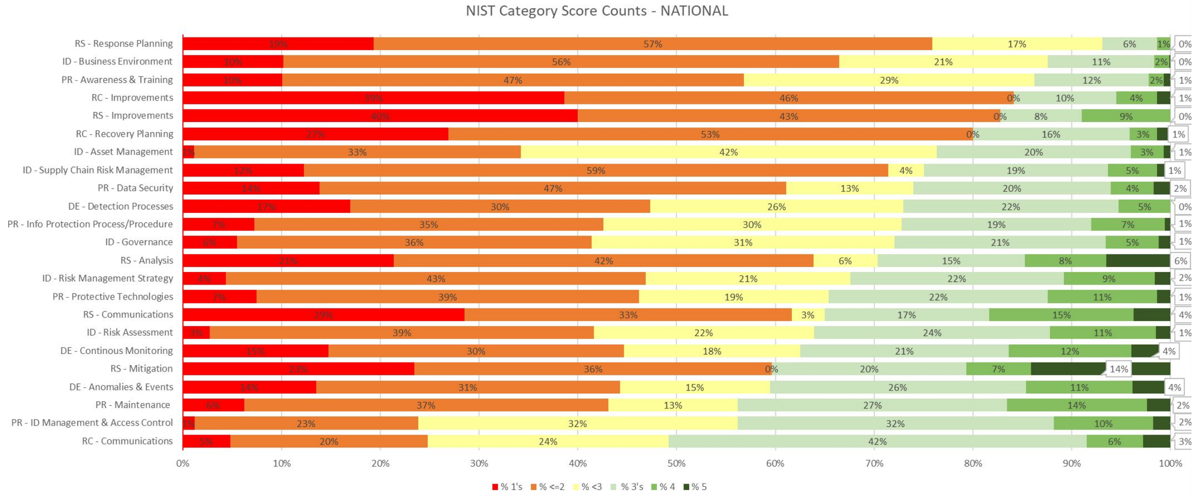
RC - Improvements

NIST Categories (cont'd)

NIST Category Score Counts - NATIONAL



NIST Categories (cont'd)



RS - Response Planning

ID - Business Environment

PR - Awareness and Training

RS - Improvements

RC - Improvements

RC - Recovery Planning

ID - Asset Management

ID - Supply Chain Risk Mgmt.

PR - Data Security

DE - Detection process

PR - Info Protection Proc/Procedures

ID - Governance

GCI & Low Maturity Counts

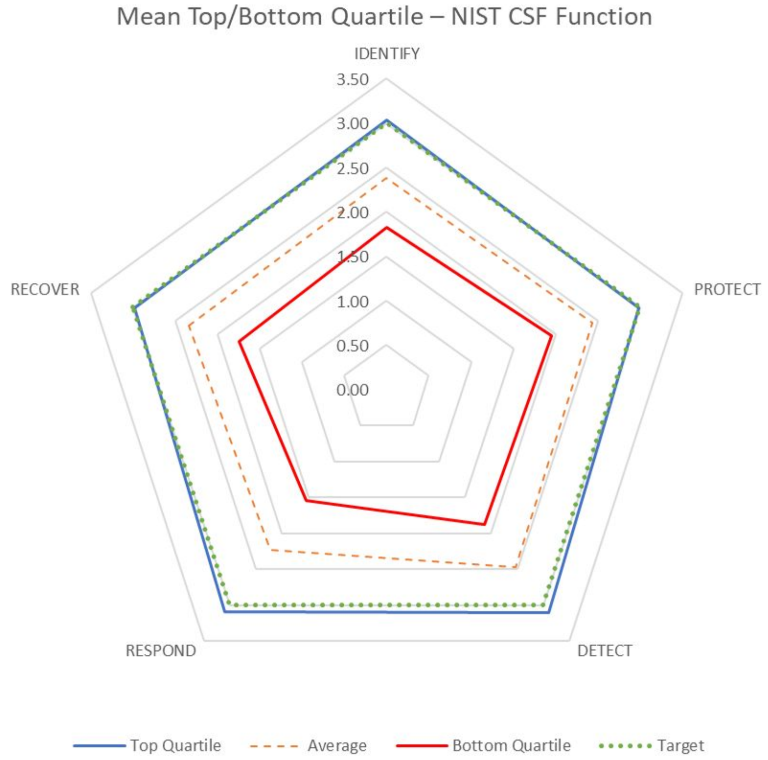
GCI (COMMON FOR ALL)

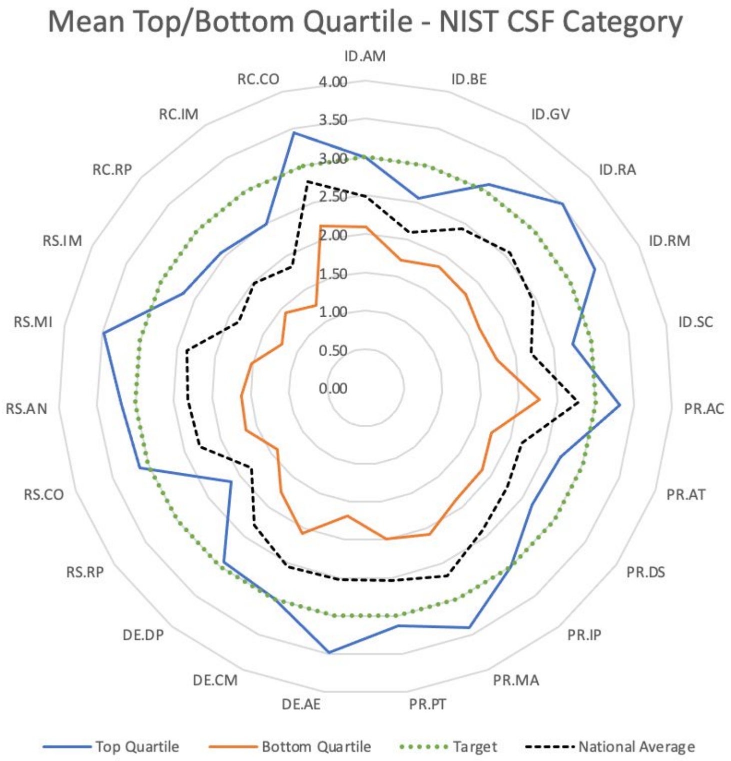
ID - Asset Management
PR - Awareness and Training
PR - Data Security
PR - Info Protection Proc/Procedures
DE - Detection process
RS - Response Planning
RS - Improvements
RC - Recovery Planning
RC - Improvements

HEATMAP (SORTED)

ID - Asset Management
PR - Awareness and Training
PR - Data Security
PR - Info Protection Proc/Procedures
DE - Detection process
RS - Response Planning
RS - Improvements
RC - Recovery Planning
RC - Improvements

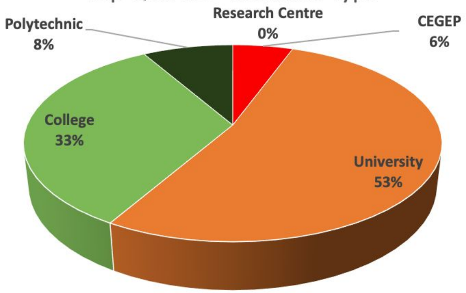
Top & Bottom Quartiles



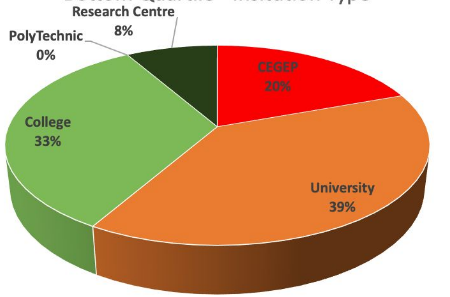


Top & Bottom Quartiles (cont'd)

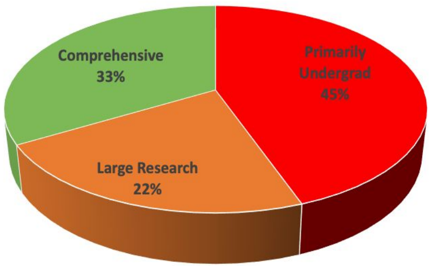
Top Quartile - Insitution Type



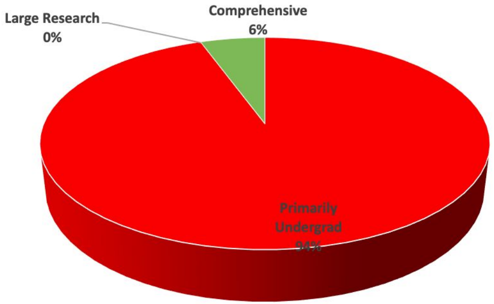
Bottom Quartile - Insitution Type



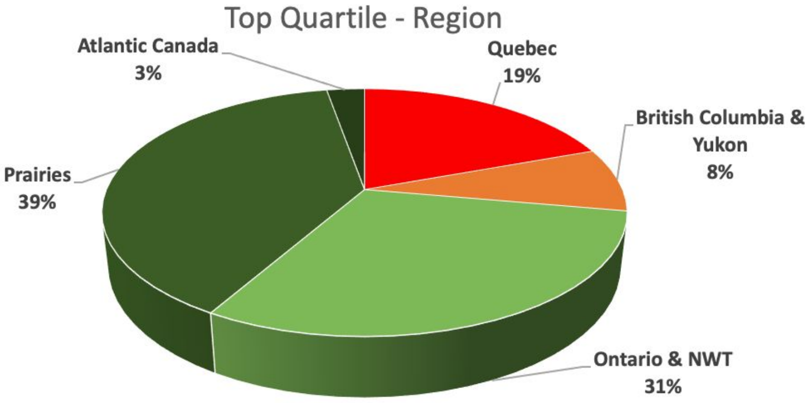
Top Quartile - GCI Category

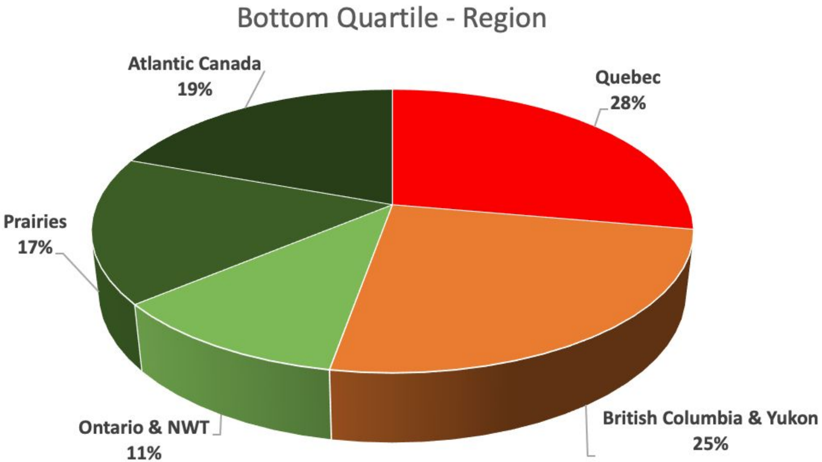


Bottom Quartile - GCI Category

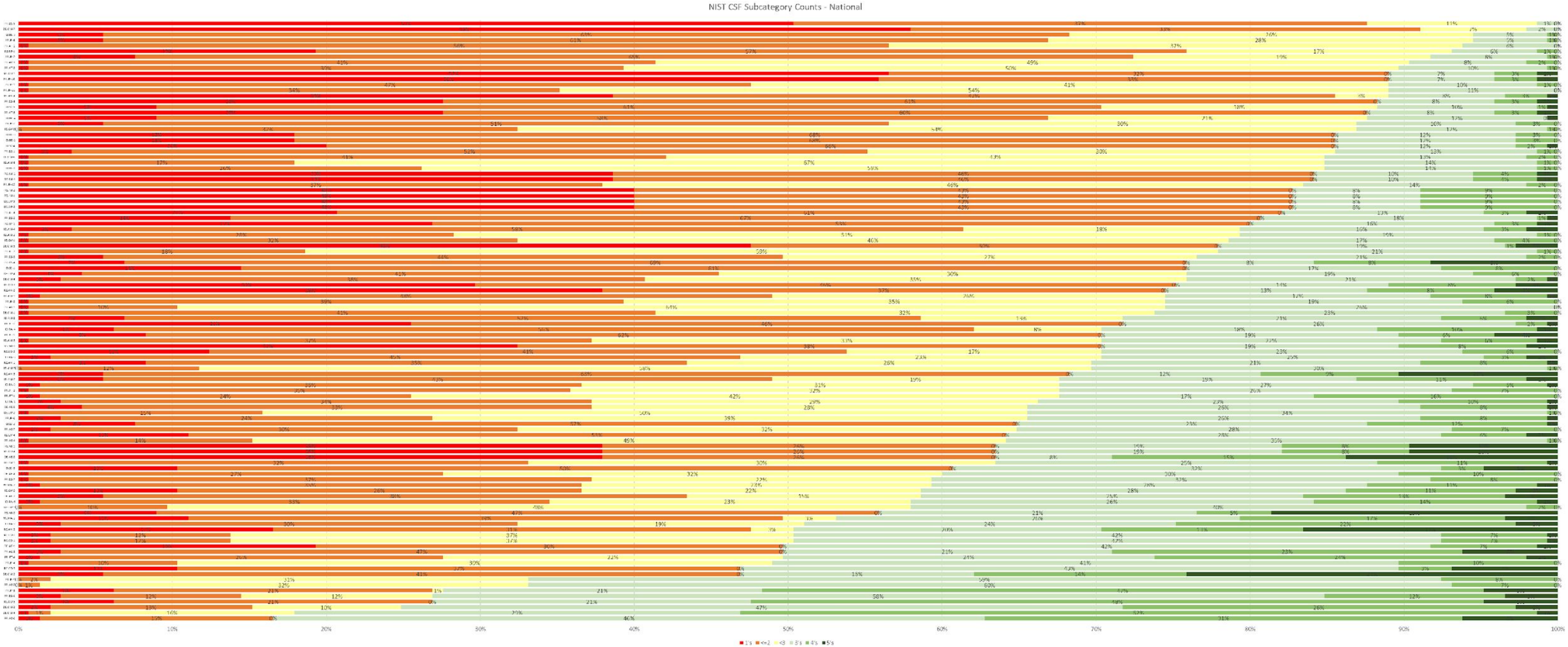


Top & Bottom Quartiles (cont'd)





NIST Subcategories



NIST Subcategories (cont'd)

TOP 5 SUBCATEGORIES

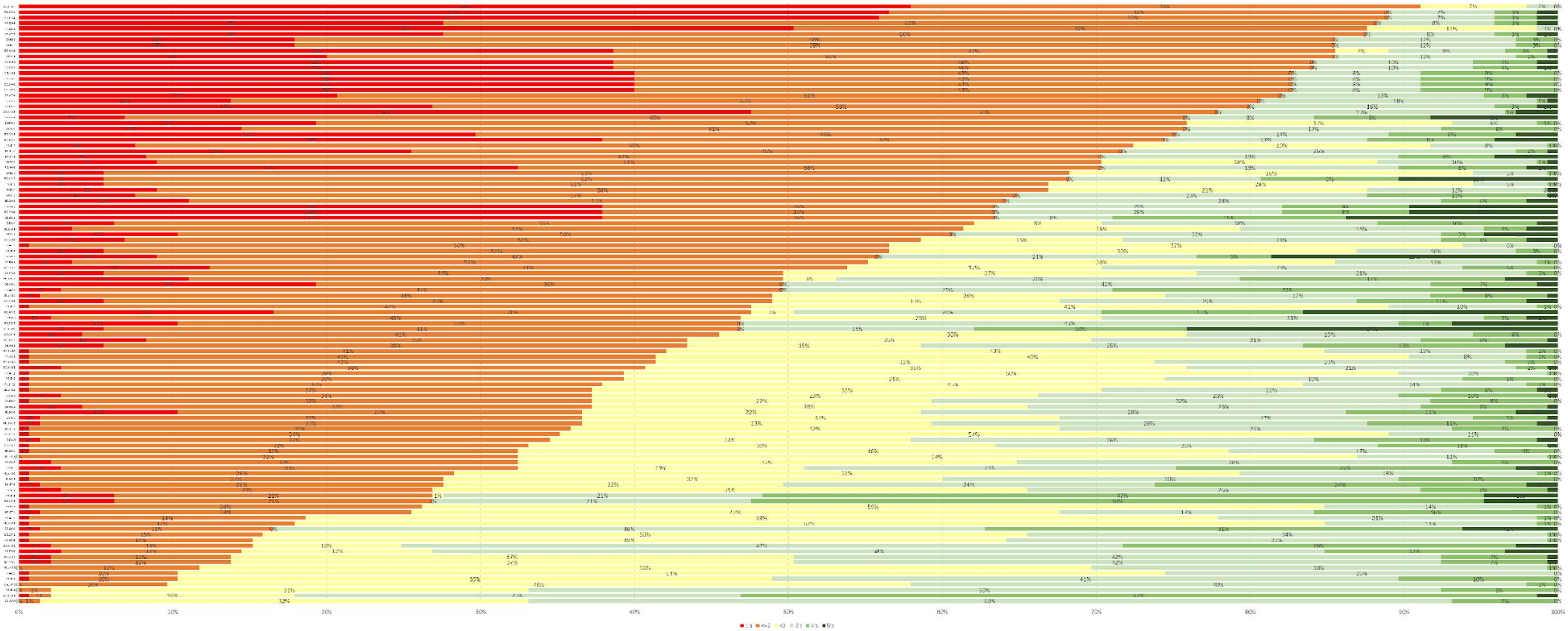
1. **PR.AC-2** - Physical access to assets is managed and protected
2. **DE.CM-4** - Malicious code is detected
3. **PR.IP-5** - Policy and regulations regarding the physical operating environment for organizational assets are met
4. **DE.DP-1** - Roles and responsibilities for detection are well defined to ensure accountability
5. **PR.IP-4** - Backups of information are conducted, maintained, and tested

BOTTOM 5 SUBCATEGORIES

1. **DE.CM-7** - Monitoring for unauthorized personnel, connections, devices, and software is performed
2. **RS.CO-1** - Personnel know their roles and order of operations when a response is needed
3. **PR.IP-10** - Response and recovery plans are tested
4. **PR.DS-8** - Integrity checking mechanisms are used to verify hardware integrity
5. **PR.DS-5** - Protections against data leaks are implemented

NIST Subcategories (cont'd)

NIST CSF Subcategory Counts - National



NIST Subcategories (cont'd)

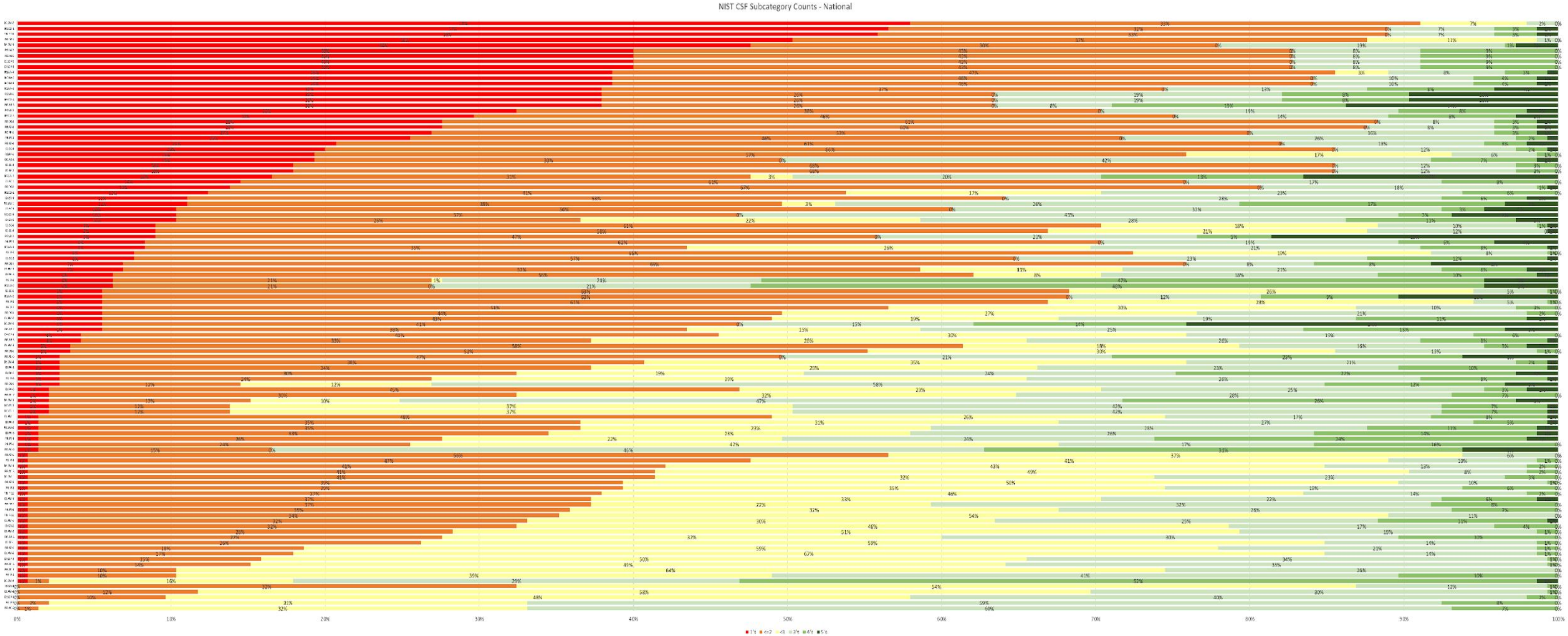
TOP 5 SUBCATEGORIES

1. **PR.AC-6** - Identities are proofed and bound to credentials and asserted in interactions
2. **DE.CM-4** - Malicious code is detected
3. **DE.CM-3** - Personnel activity is monitored to detect potential cybersecurity events
4. **RS.CO-5** - Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
5. **PR.DS-6** - Integrity checking mechanisms are used to verify software, firmware, and information integrity

BOTTOM 5 SUBCATEGORIES

1. **PR.DS-5** - Protections against data leaks are implemented
2. **DE.CM-7** - Monitoring for unauthorized personnel, connections, devices, and software is performed
3. **ID.BE-5** - Resilience requirements to support delivery of critical services are established for all operating states
4. **PR.IP-9** - Response plans (Incident & Business Continuity) and recovery plans (Incident & DR) are in place and managed
5. **PR.AT-1** - All users are informed and trained

NIST Subcategories (cont'd)



NIST Subcategories (cont'd)

TOP 5 SUBCATEGORIES

1. **PR.AC-2** - Physical access to assets is managed and protected PR.IP-5

2. **PR.IP-5** - Policy and regulations regarding the physical operating environment for organizational assets are met

3. **DE.DP-1** - Roles and responsibilities for detection are well defined to ensure accountability

4. **ID.AM-3** - Organizational communication and data flows are mapped

5. **ID.GV-3** - Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

BOTTOM 5 SUBCATEGORIES

1. **DE.CM-7** - Monitoring for unauthorized personnel, connections, devices, and software is performed

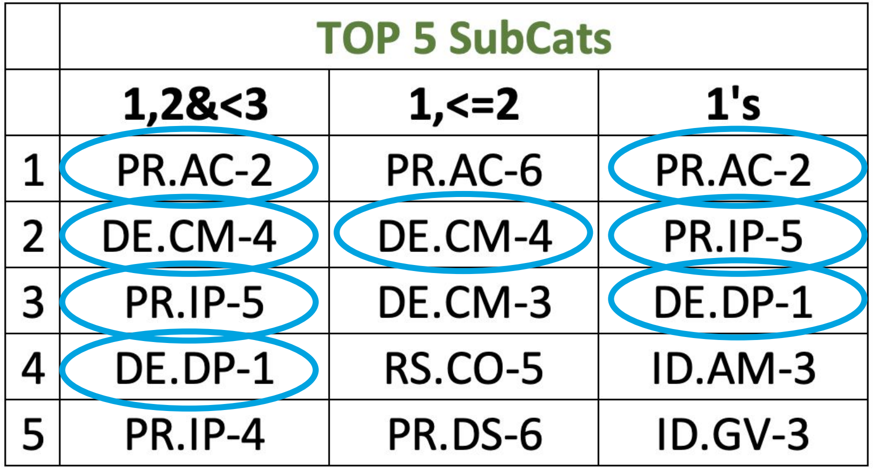
2. **RS.CO-1** - Personnel know their roles and order of operations when a response is needed

3. **PR.IP-10** - Response and recovery plans are tested

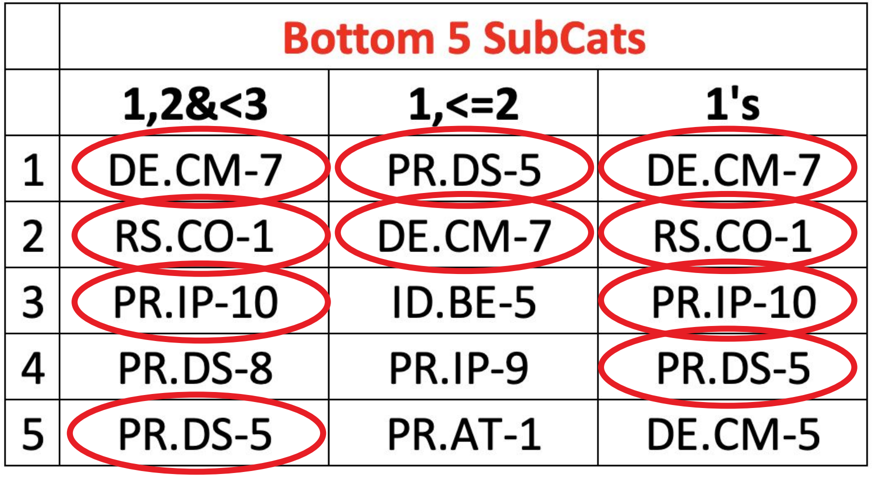
4. **PR.DS-5** - Protections against data leaks are implemented

5. **DE.CM-5** - Unauthorized mobile code is detected

NIST Subcategories (cont'd)

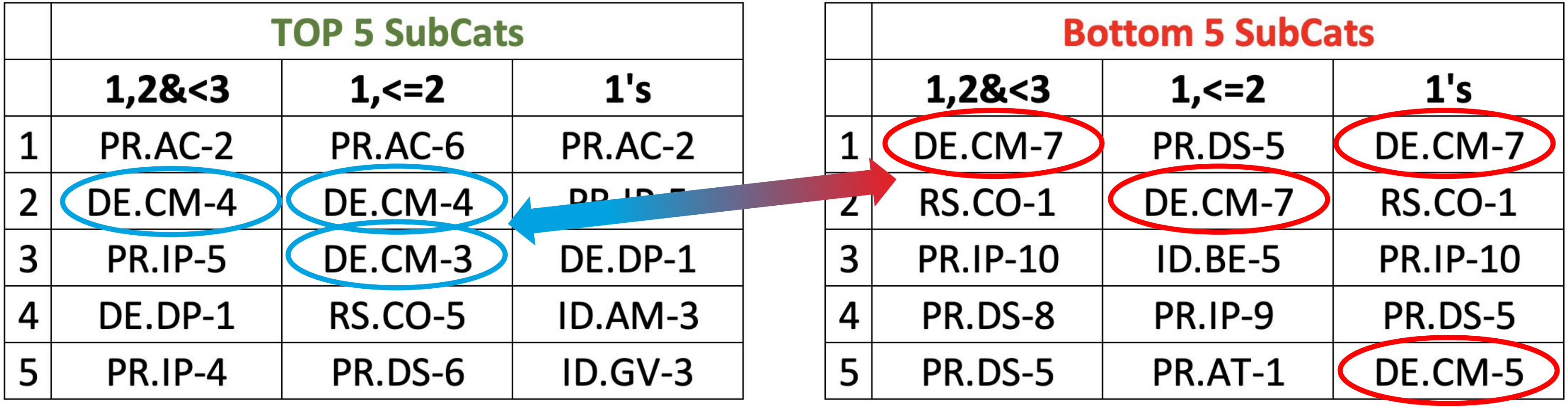


	TOP 5 SubCats		
	1,2&<3	1,<=2	1's
1	PR.AC-2	PR.AC-6	PR.AC-2
2	DE.CM-4	DE.CM-4	PR.IP-5
3	PR.IP-5	DE.CM-3	DE.DP-1
4	DE.DP-1	RS.CO-5	ID.AM-3
5	PR.IP-4	PR.DS-6	ID.GV-3



	Bottom 5 SubCats		
	1,2&<3	1,<=2	1's
1	DE.CM-7	PR.DS-5	DE.CM-7
2	RS.CO-1	DE.CM-7	RS.CO-1
3	PR.IP-10	ID.BE-5	PR.IP-10
4	PR.DS-8	PR.IP-9	PR.DS-5
5	PR.DS-5	PR.AT-1	DE.CM-5

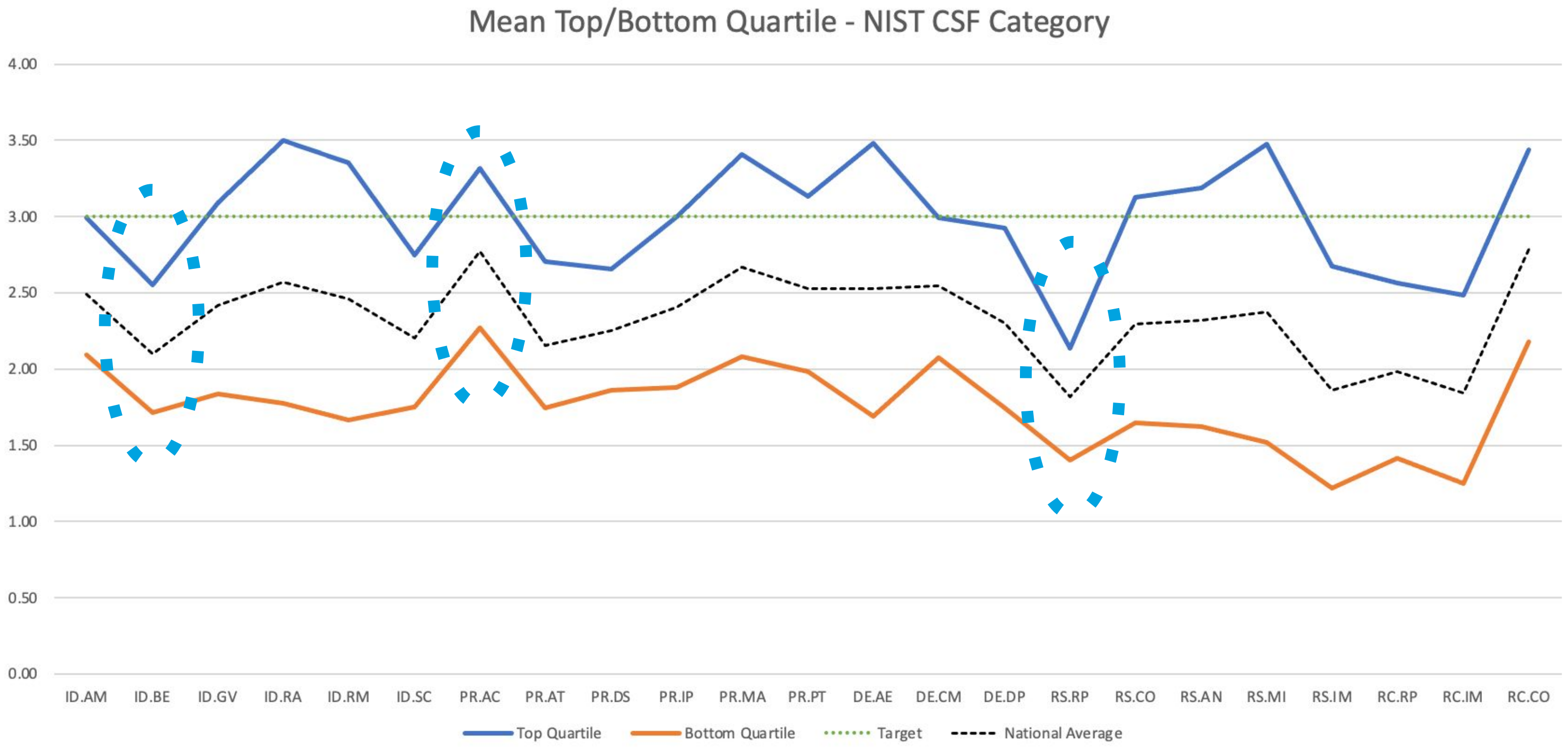
NIST Subcategories (cont'd)



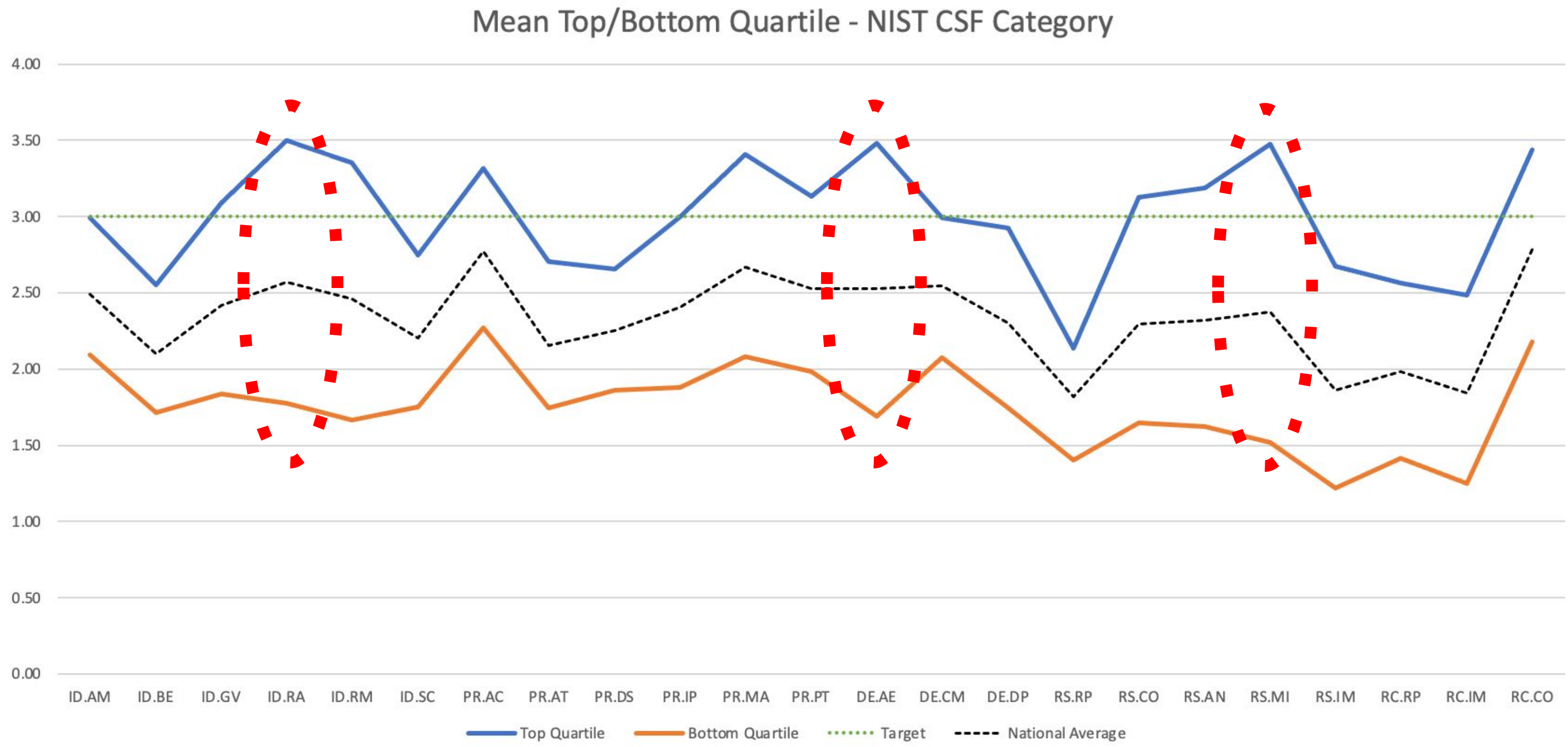
	TOP 5 SubCats		
	1,2&<3	1,<=2	1's
1	PR.AC-2	PR.AC-6	PR.AC-2
2	DE.CM-4	DE.CM-4	PR.IP-5
3	PR.IP-5	DE.CM-3	DE.DP-1
4	DE.DP-1	RS.CO-5	ID.AM-3
5	PR.IP-4	PR.DS-6	ID.GV-3

	Bottom 5 SubCats		
	1,2&<3	1,<=2	1's
1	DE.CM-7	PR.DS-5	DE.CM-7
2	RS.CO-1	DE.CM-7	RS.CO-1
3	PR.IP-10	ID.BE-5	PR.IP-10
4	PR.DS-8	PR.IP-9	PR.DS-5
5	PR.DS-5	PR.AT-1	DE.CM-5

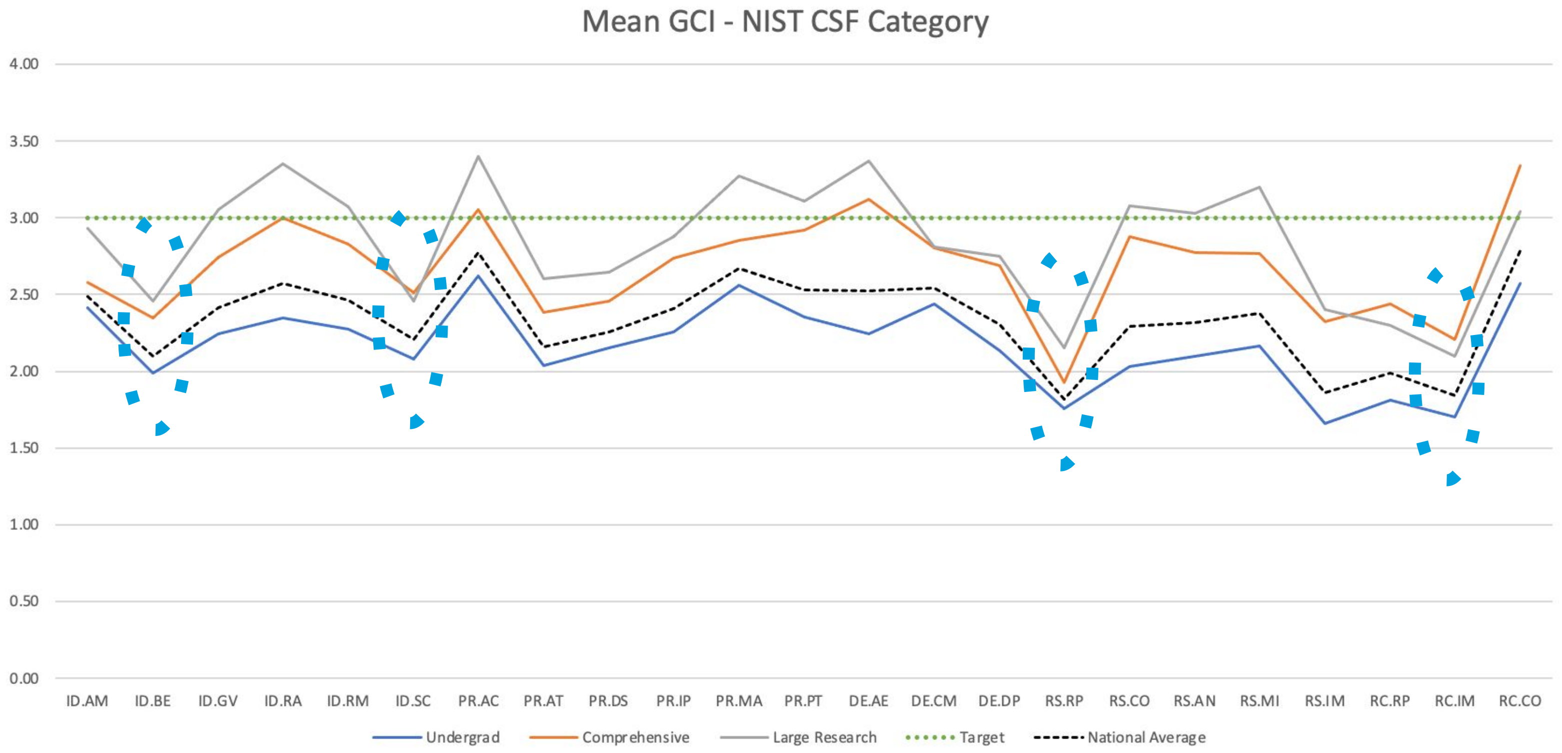
Top & Bottom Quartiles (cont'd)



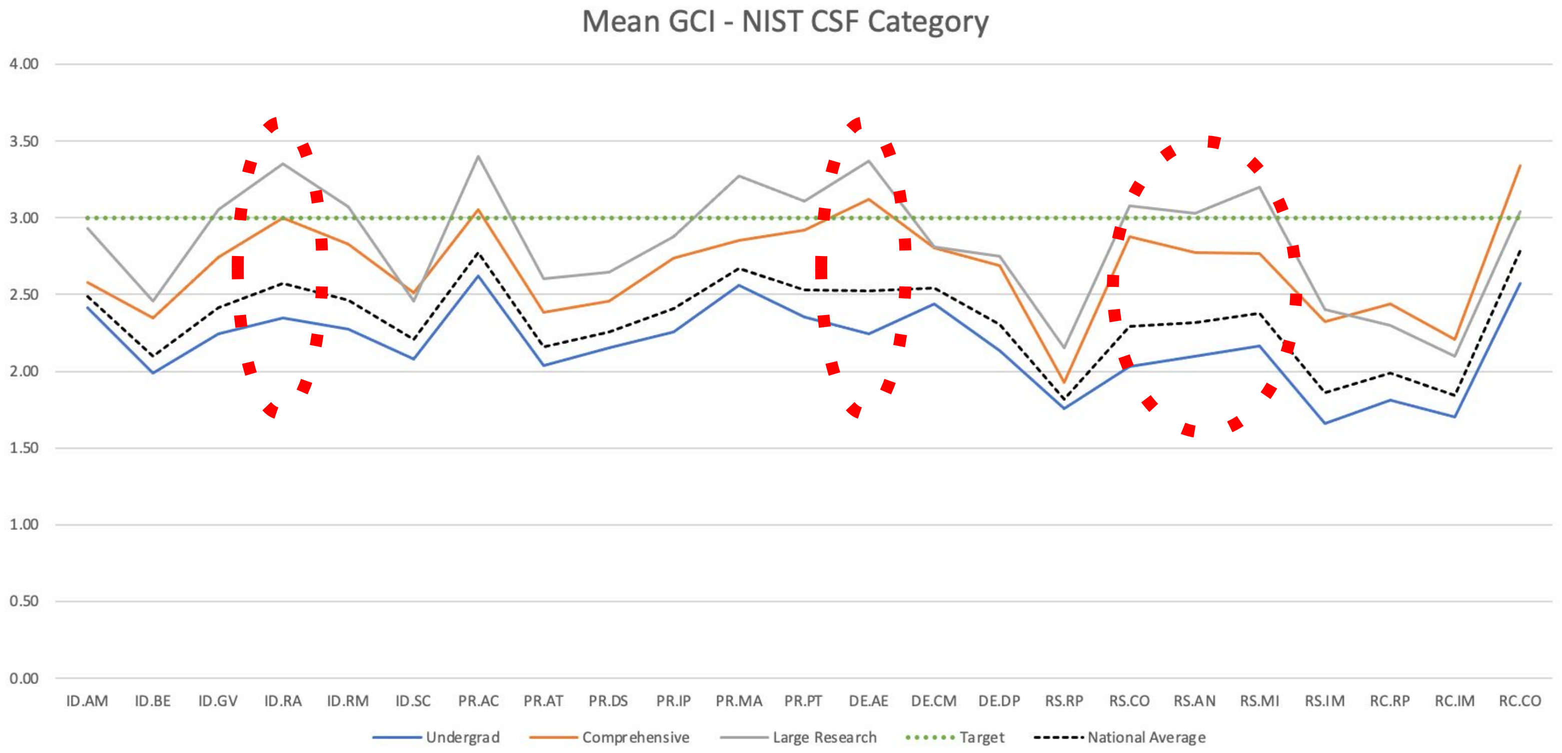
Top & Bottom Quartiles (cont'd)



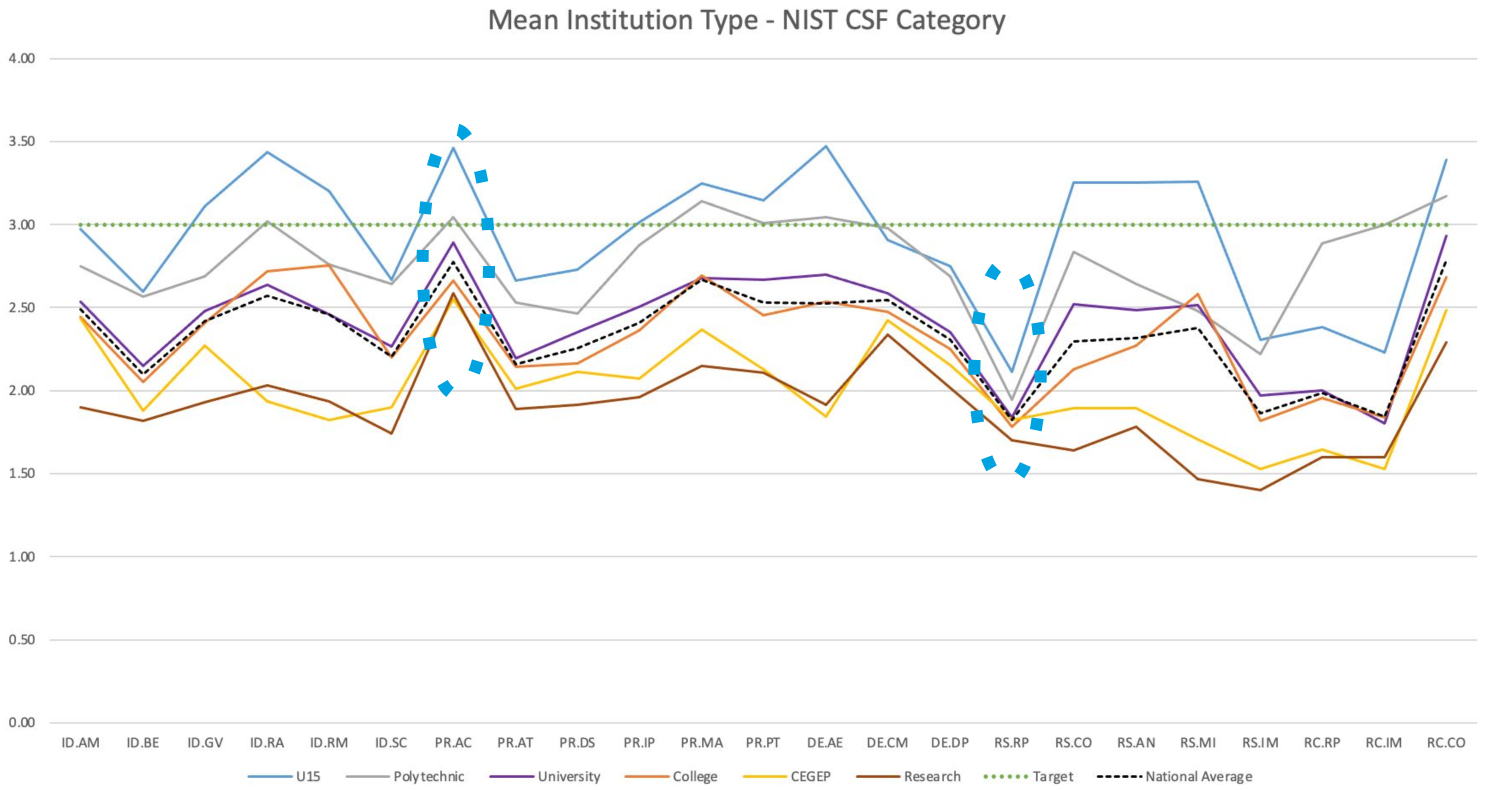
Global Complexity Index



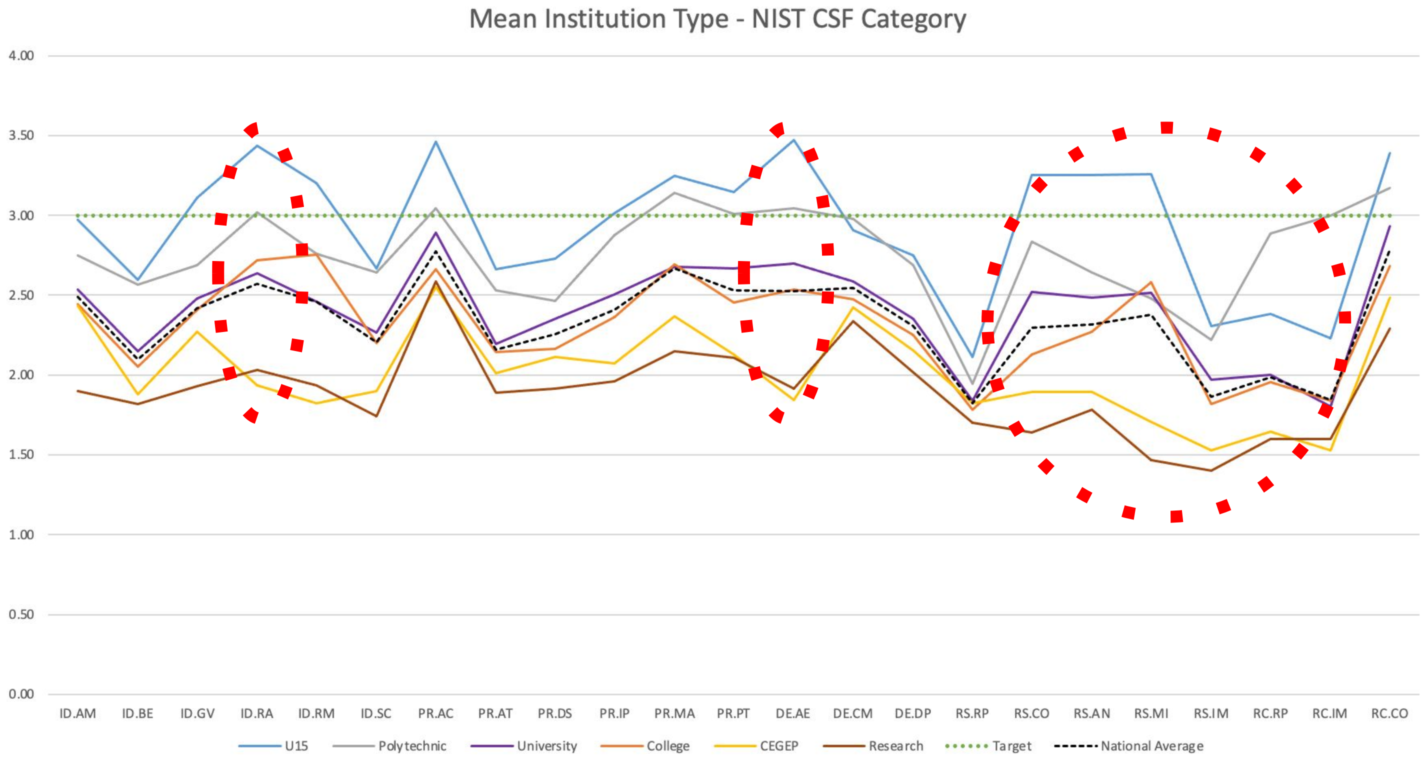
Global Complexity Index



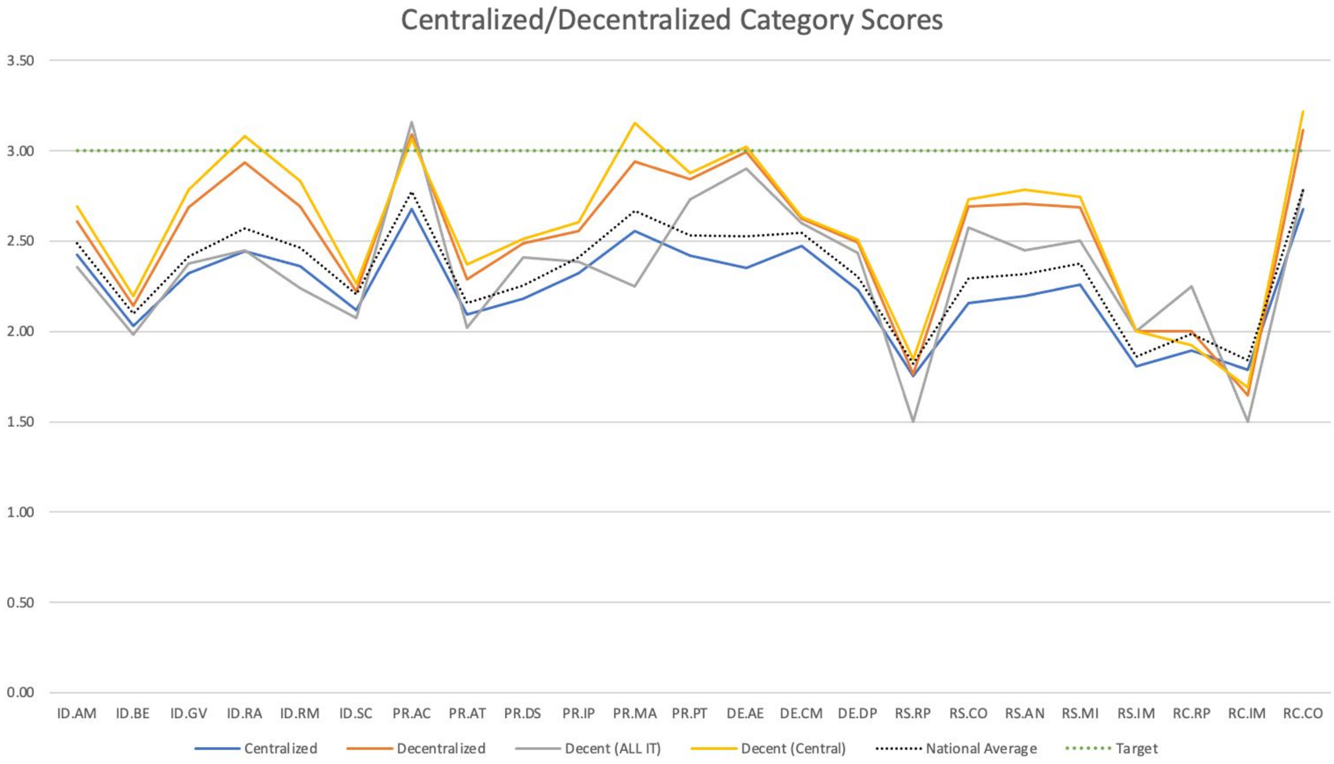
Institution Type



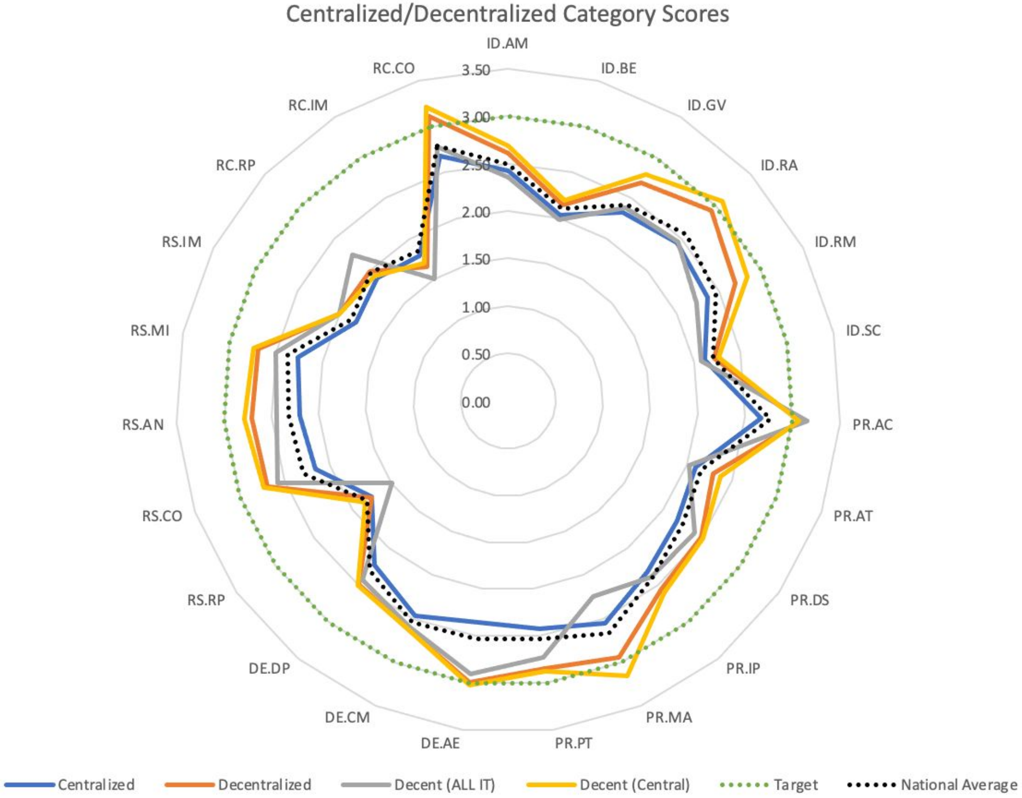
Institution Type



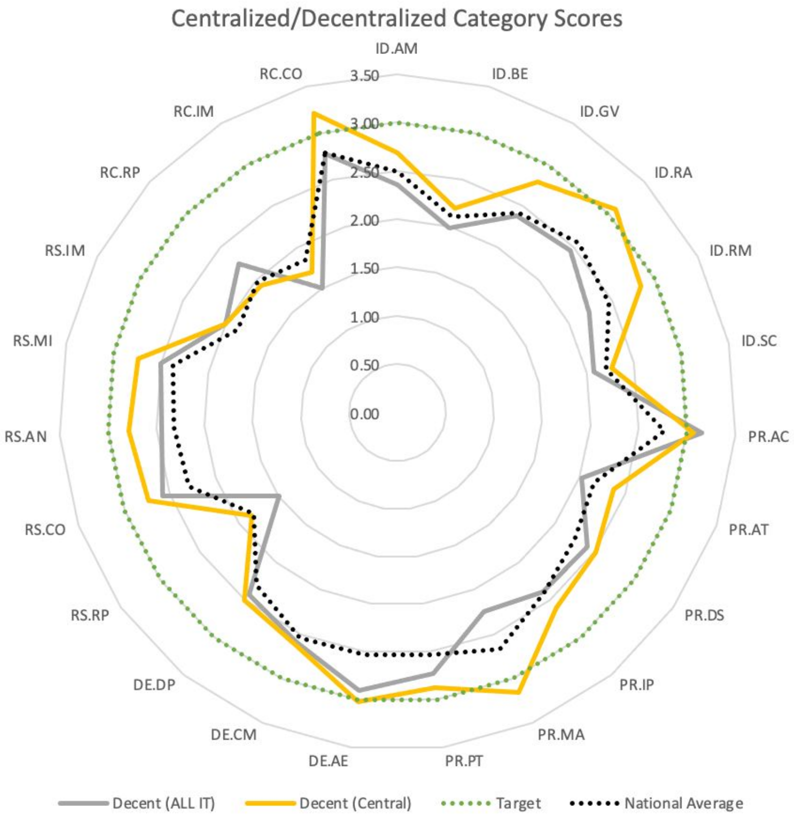
IT Disposition (cont'd)



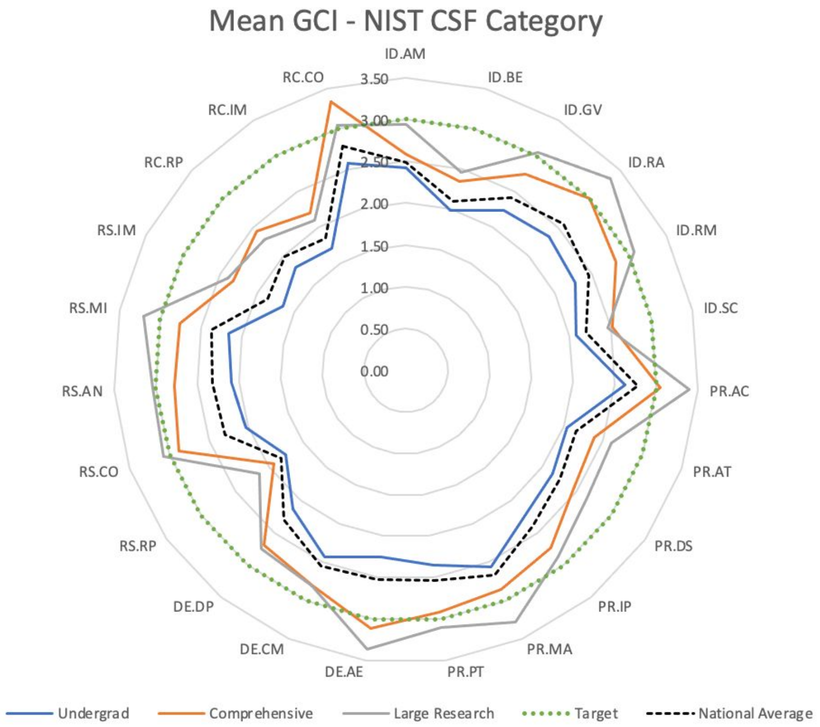
IT Disposition

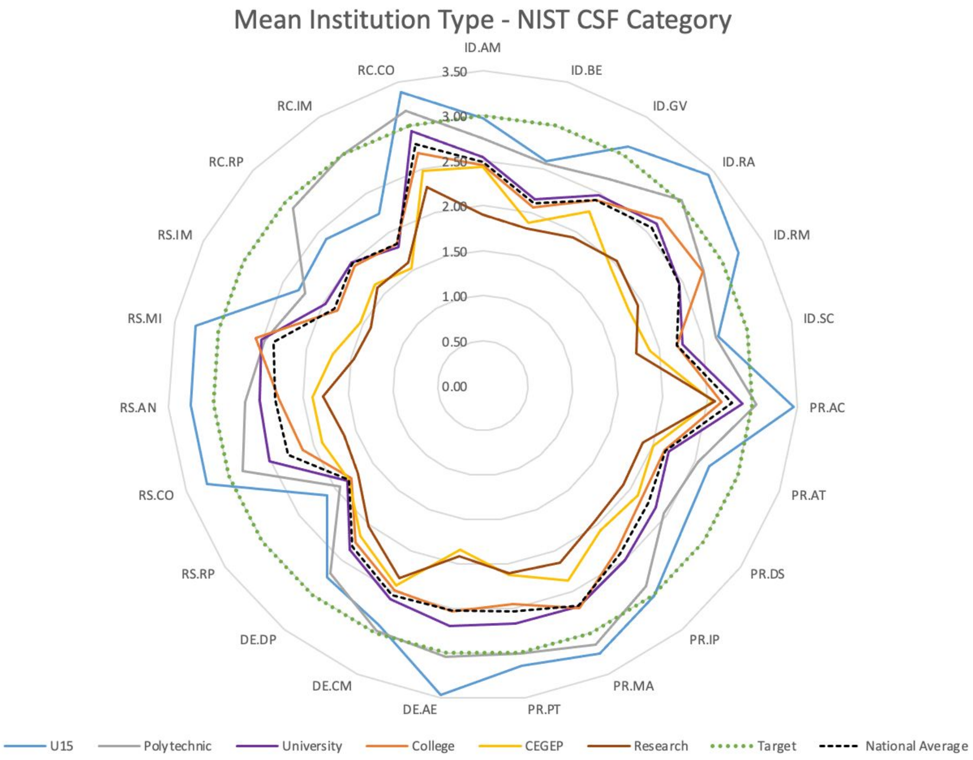


IT Disposition (cont'd)

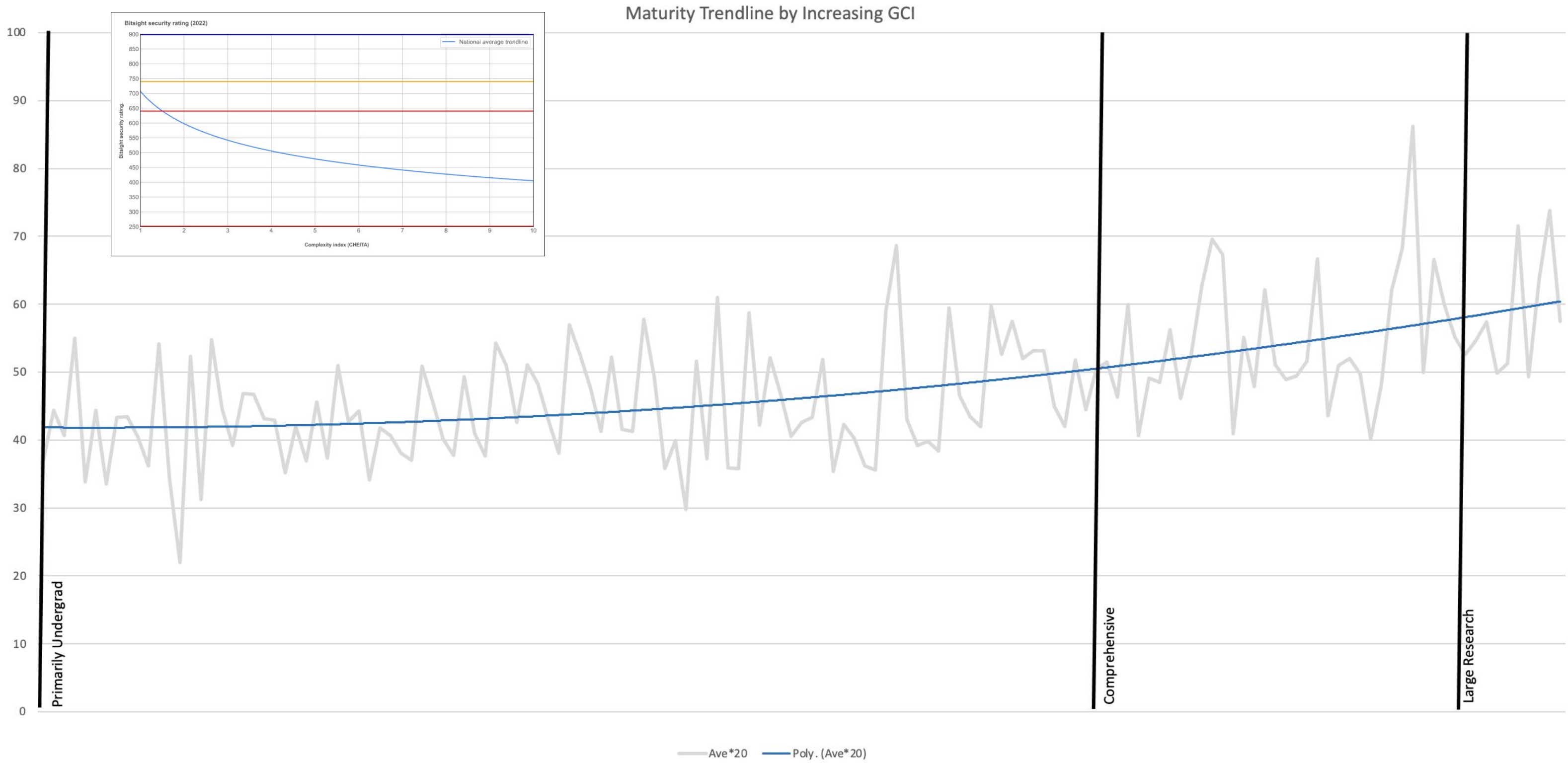


GCI & Institution Type





Global Complexity Index (cont'd)



Provincial Results

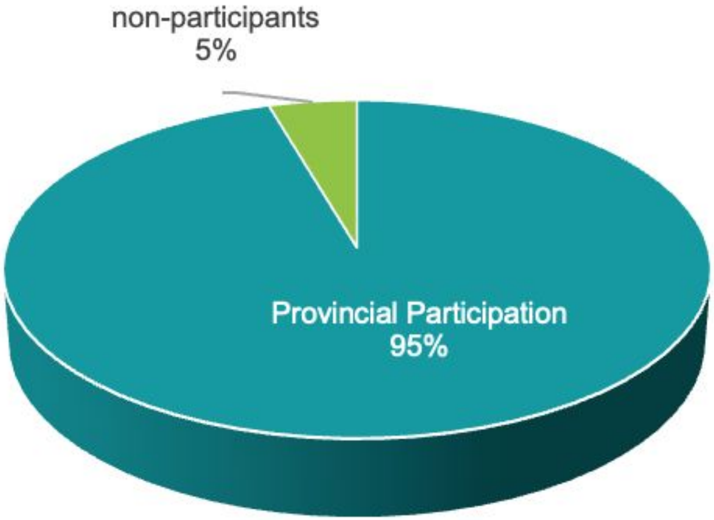
Participation

Total Eligible Organizations: **22**

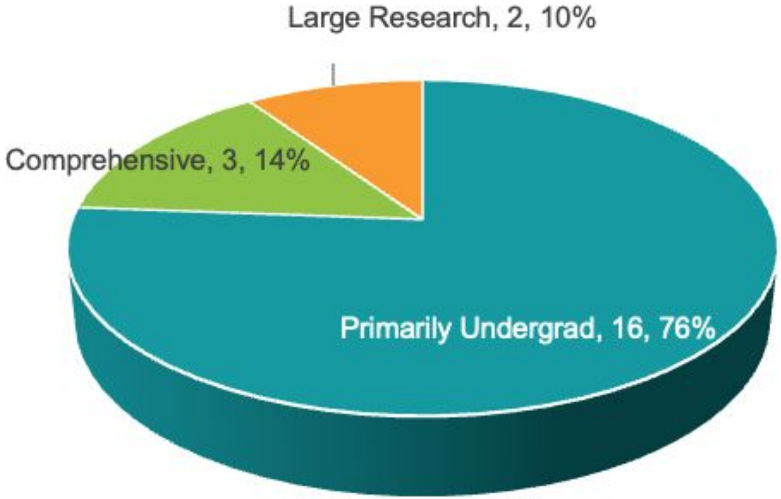
Total Participants: **21**

Total Participation Rate: **95.45%**

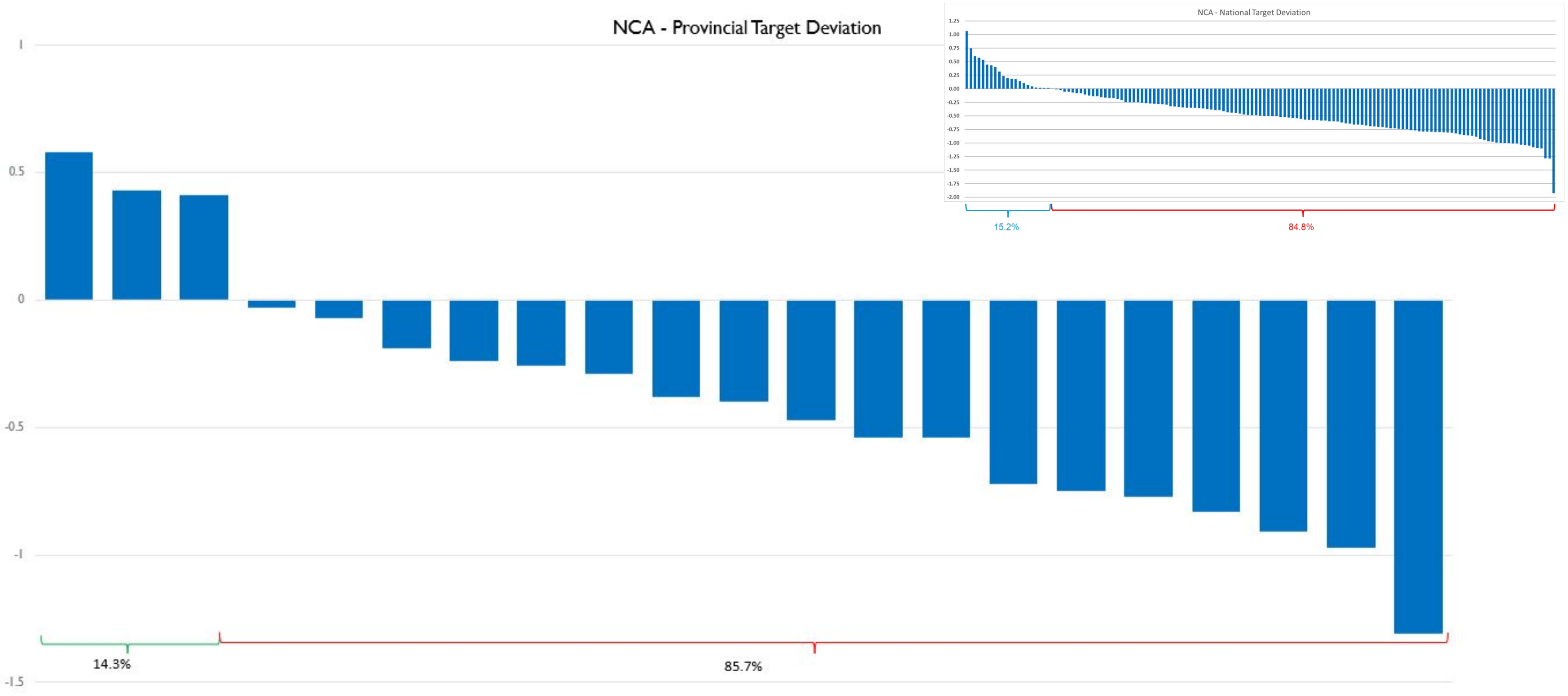
PROVINCIAL NCA SERVICE



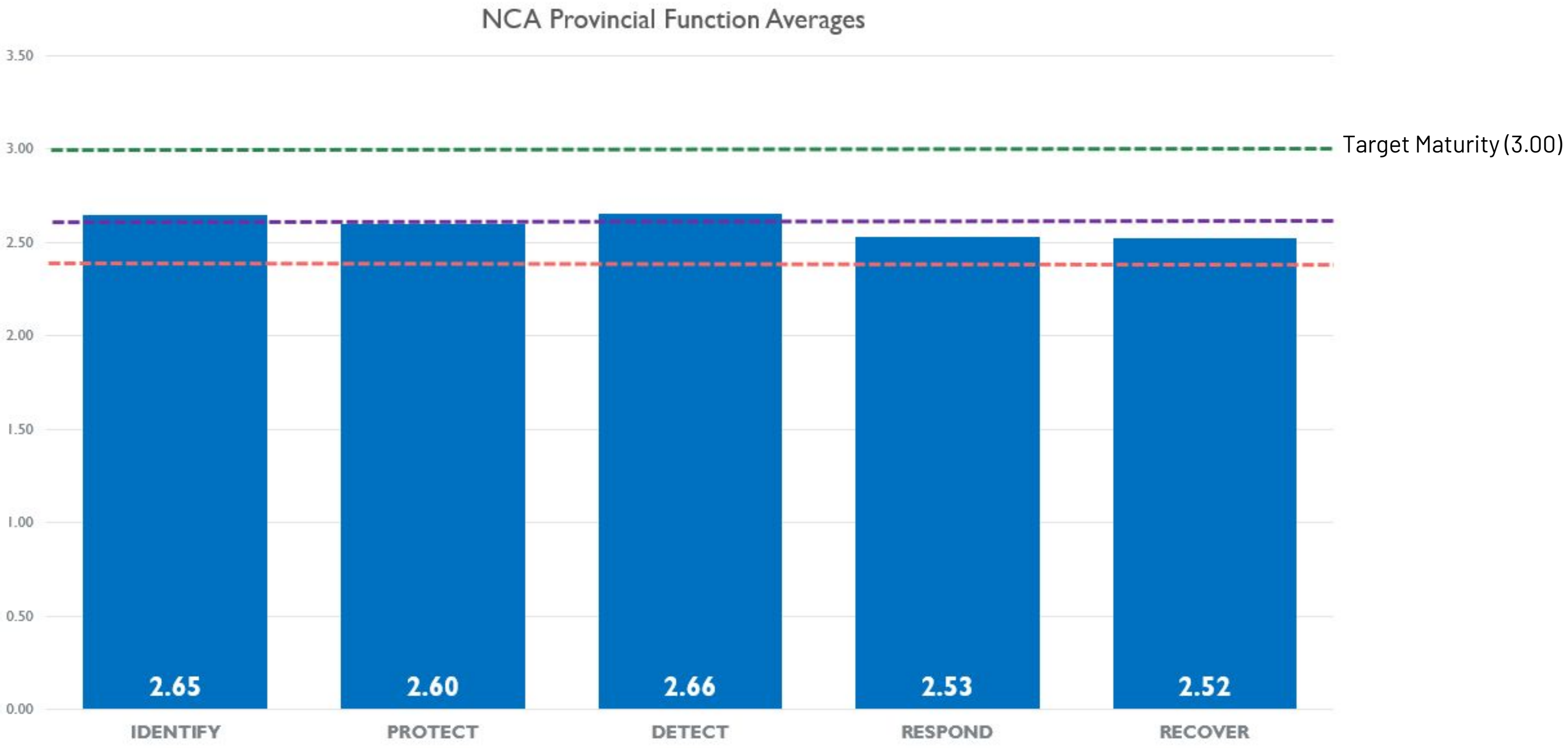
PROVINCIAL COUNTS – BY GCI



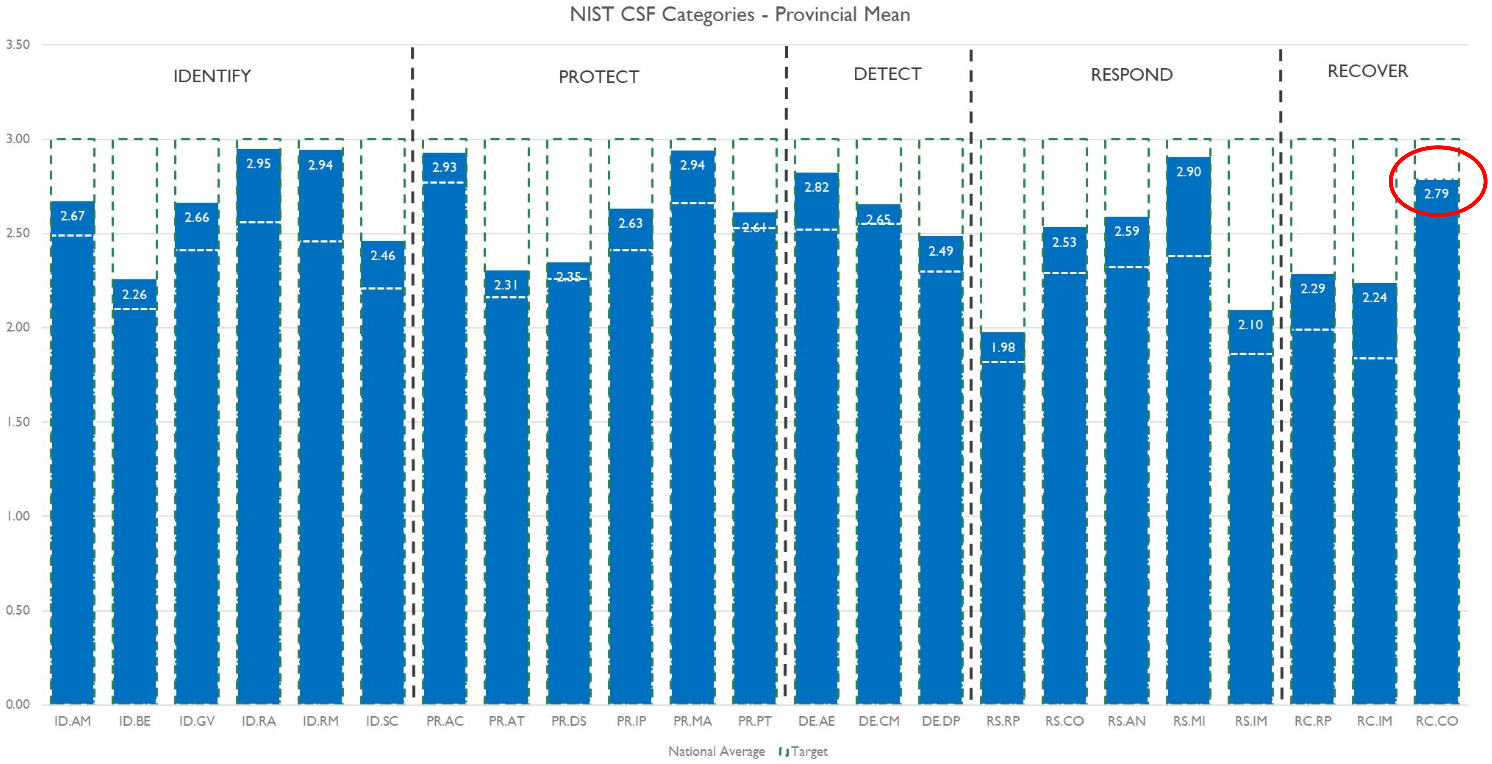
Provincial Target Deviation



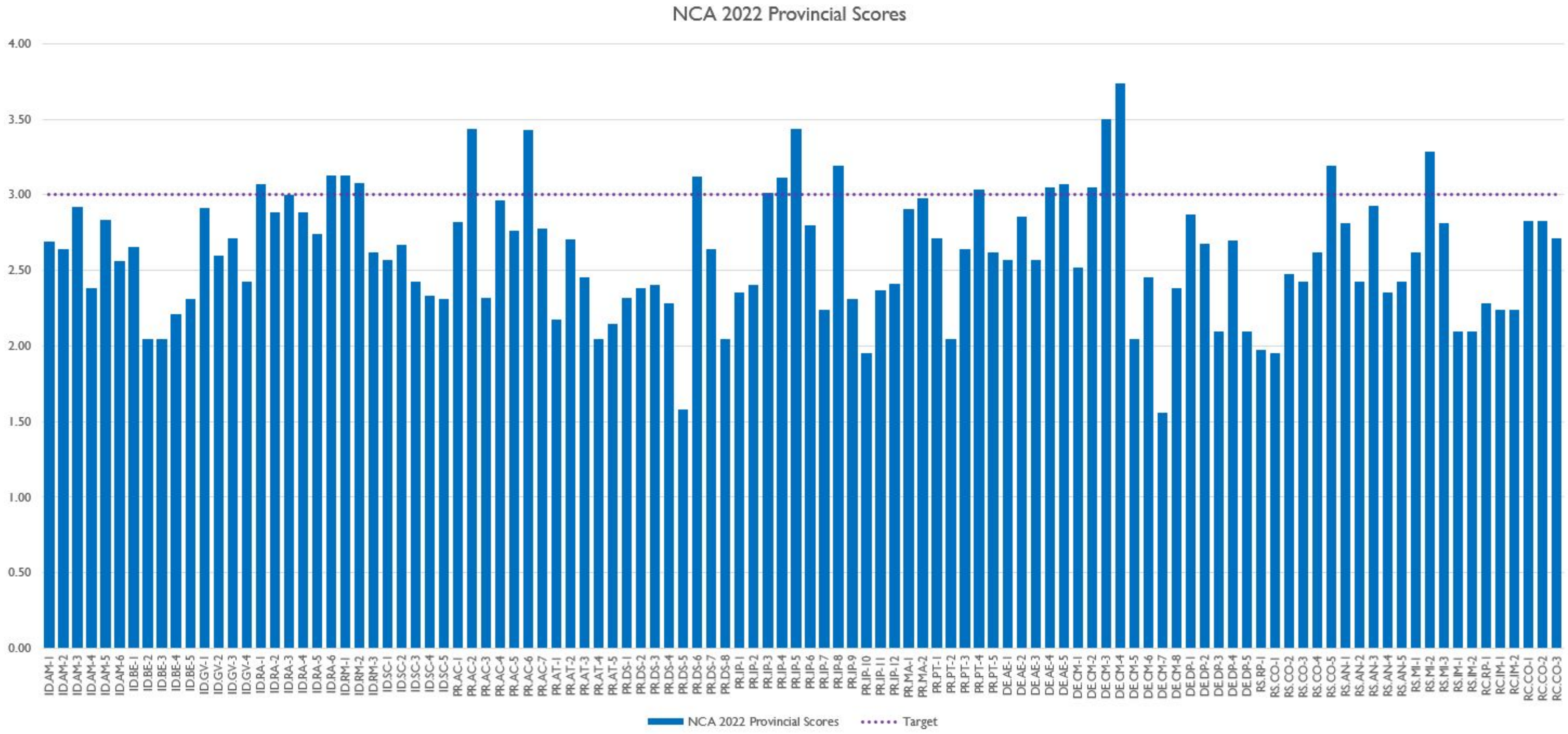
Functional Averages



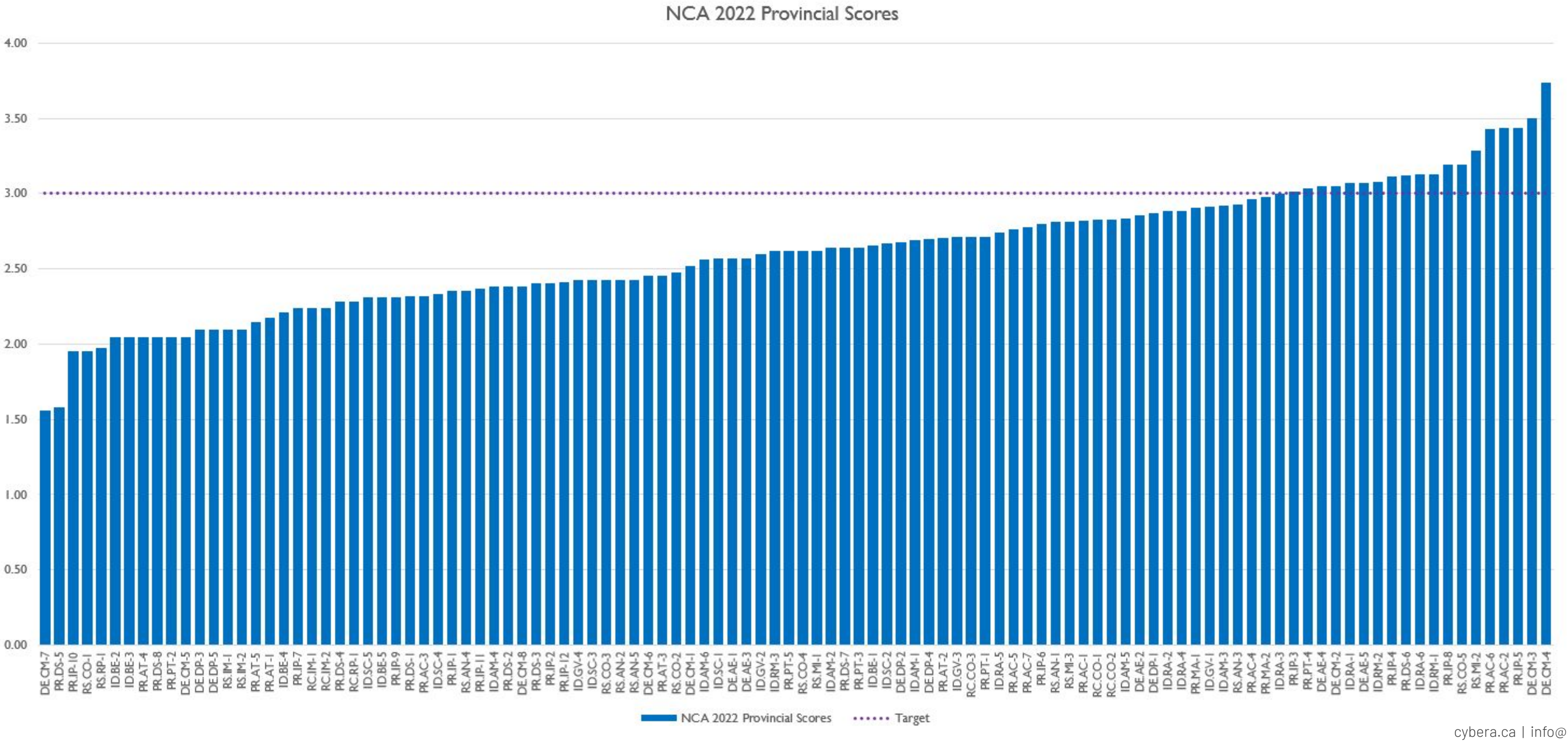
Category Averages



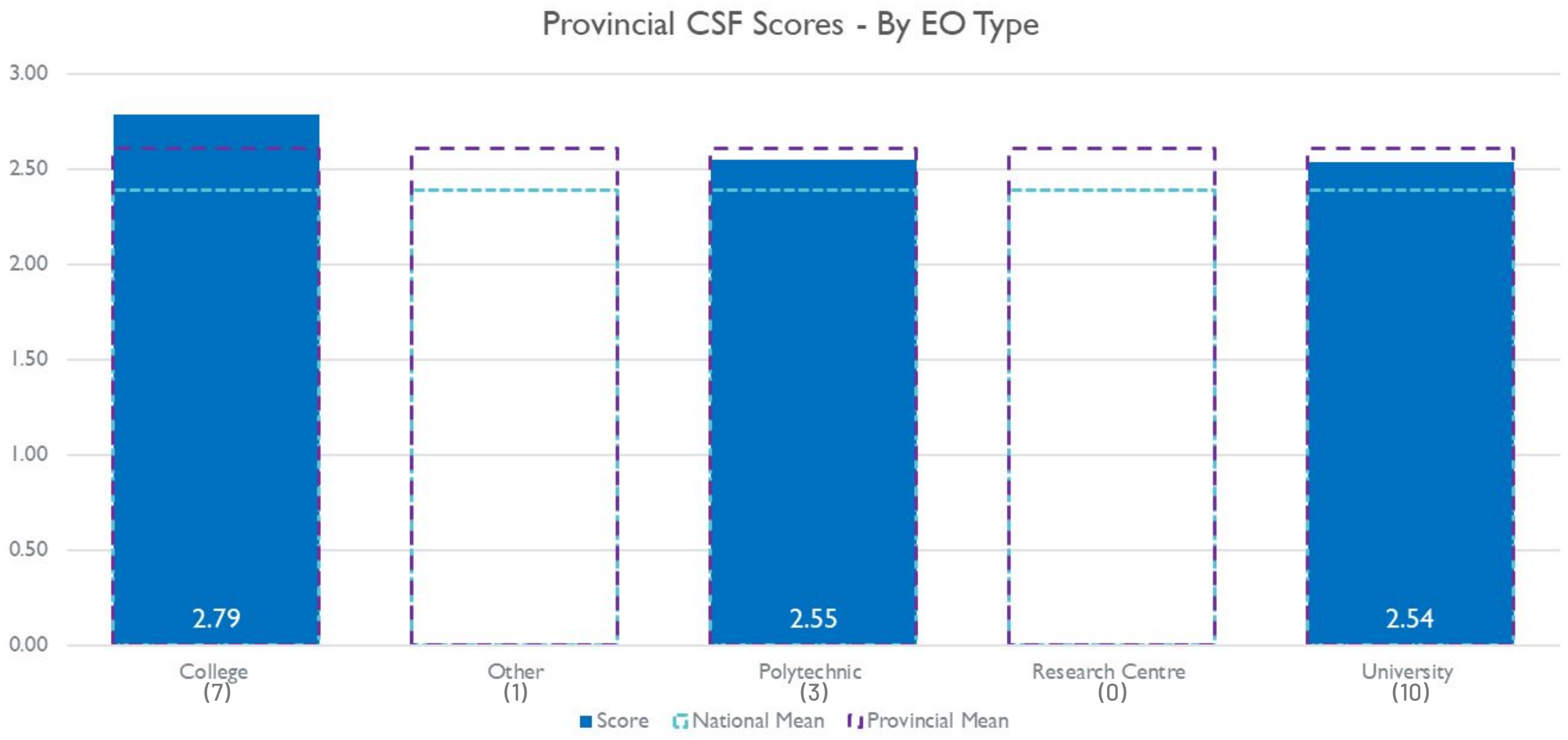
Provincial NCA Scores



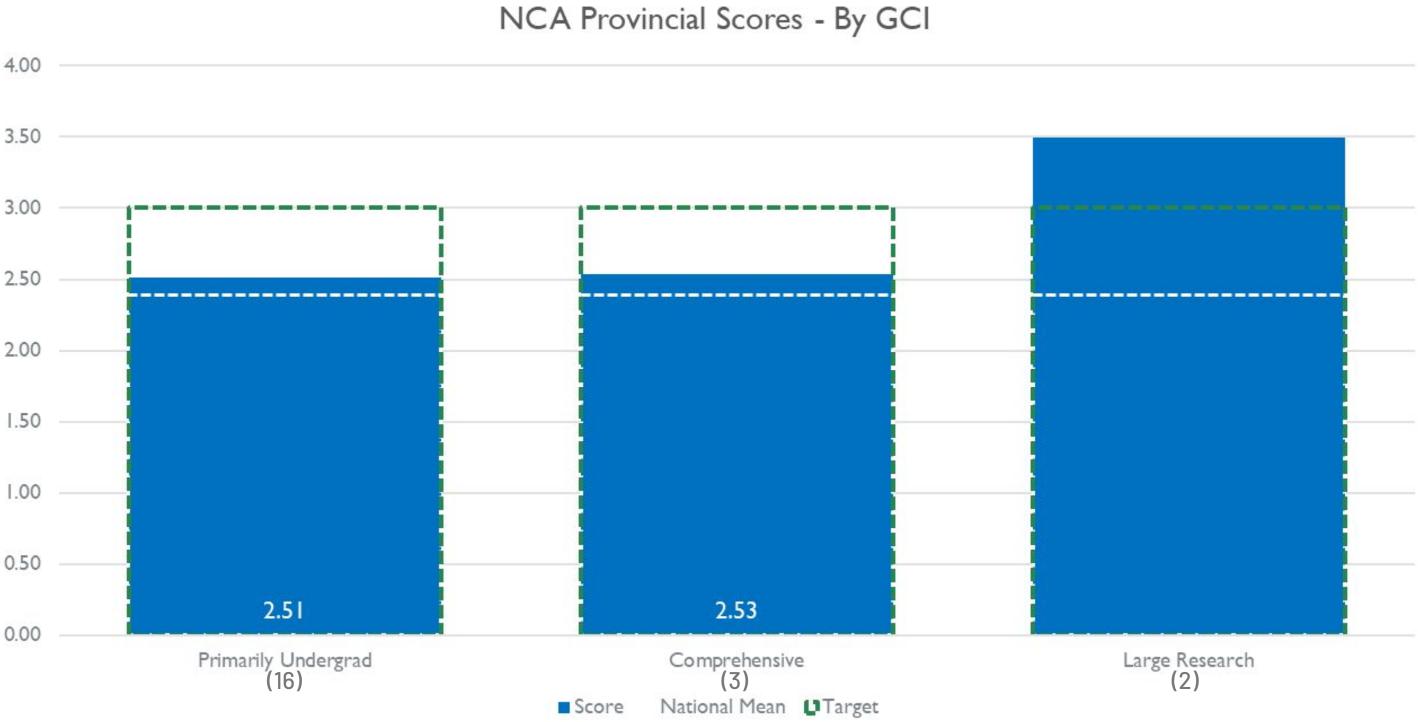
Provincial NCA Scores (sorted)



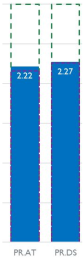
Provincial by Type



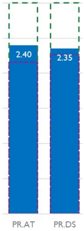
Provincial by GCI



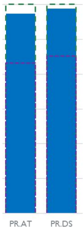
PRIMARILY UNDERGRAD



COMPREHENSIVE



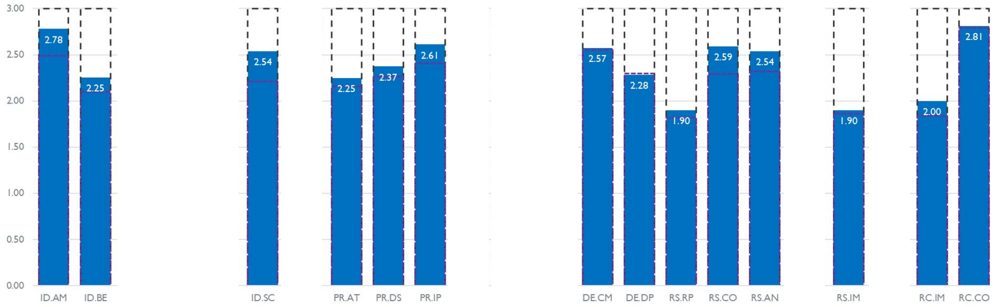
LARGE RESEARCH



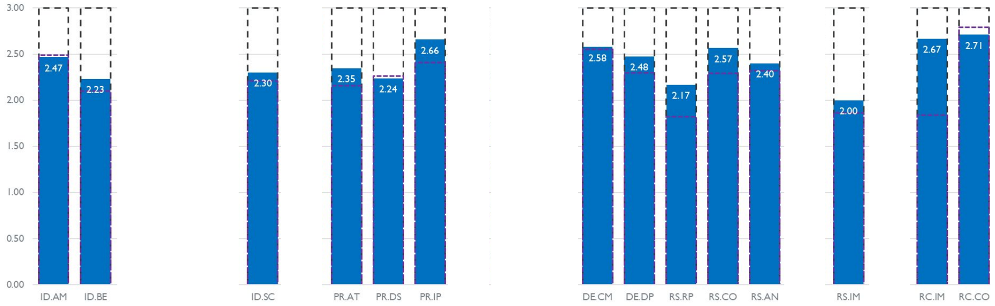
PR - Awareness and Training

PR – Data Security

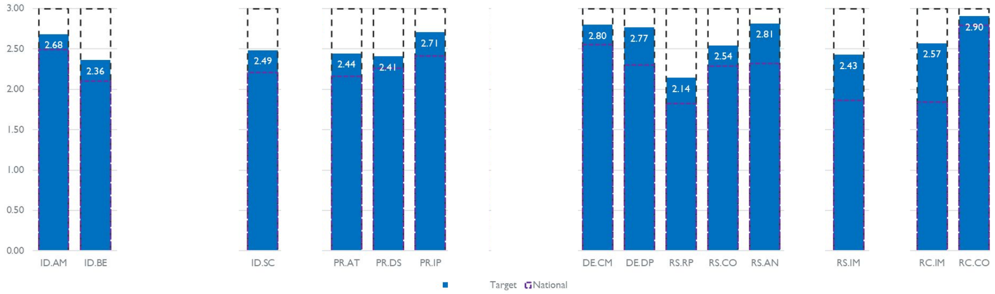
UNIVERSITY (10)



POLYTECHNIC (3)



COLLEGE (7)



ID - Asset Management

ID – Business Environment

ID - Supply Chain Risk Mgmt.

PR - Awareness and Training

PR – Data Security

PR - Info Protection Proc/Procedures

DE - Security Continuous Monitoring

DE - Detection process

RS - Response Planning

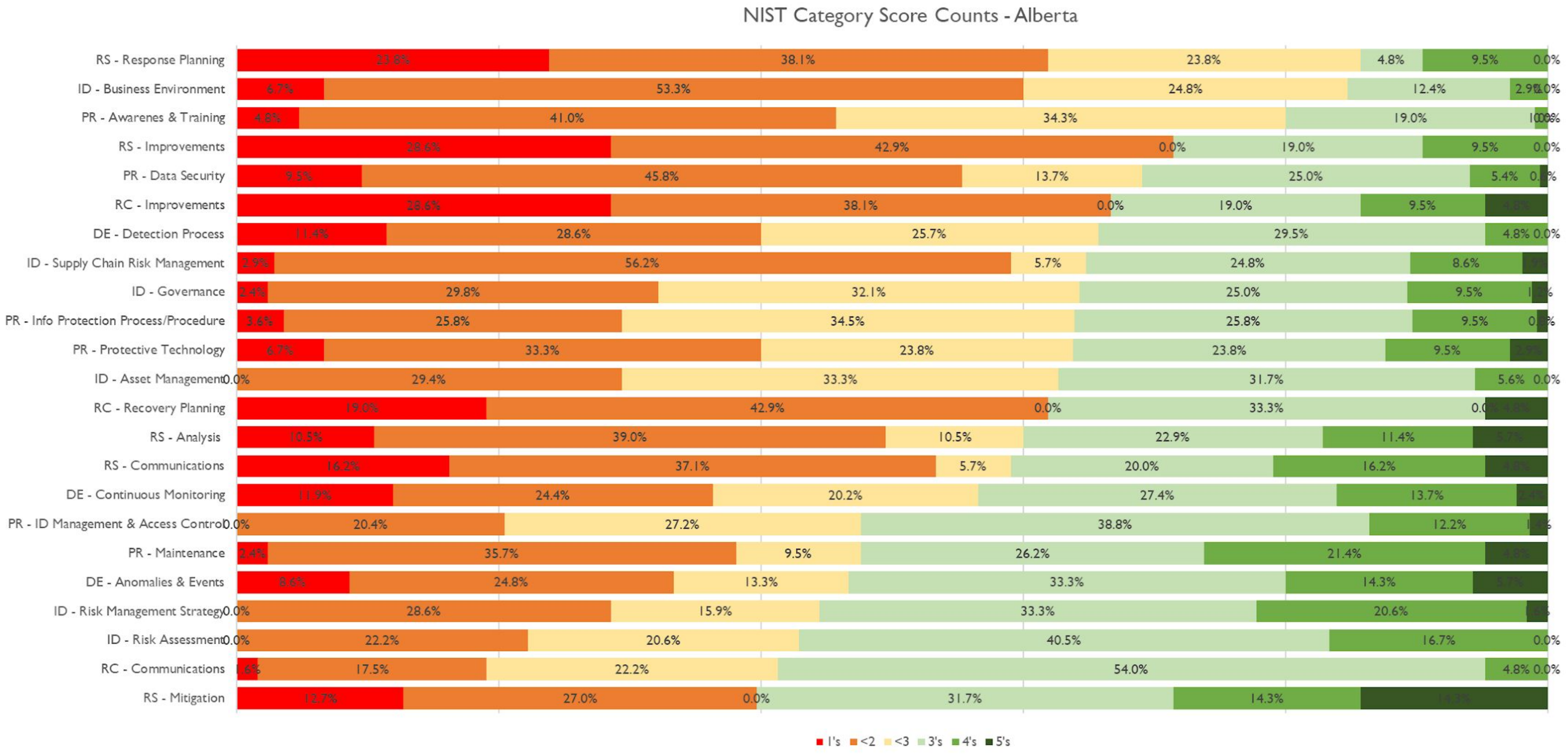
RS - Communications

RS - Analysis

RS - Improvements

RC - Improvements

Maturity Score Counts



Potential Provincial Focus Areas

BY TYPE OF INSTITUTION SORTED

RS - Response Planning
ID – Business Environment
PR - Awareness and Training
RS - Improvements
PR – Data Security
RC - Improvements
DE - Detection process
ID - Supply Chain Risk Mgmt.

PR - Info Protection Proc/Procedures

ID - Asset Management

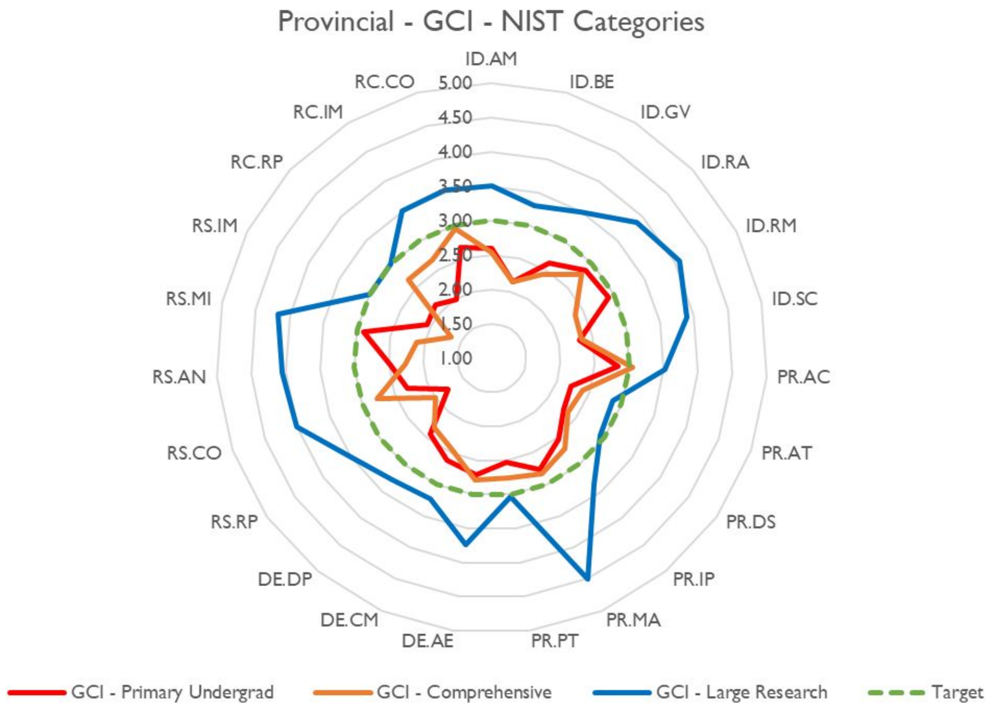
BY LOW MATURITY COUNTS

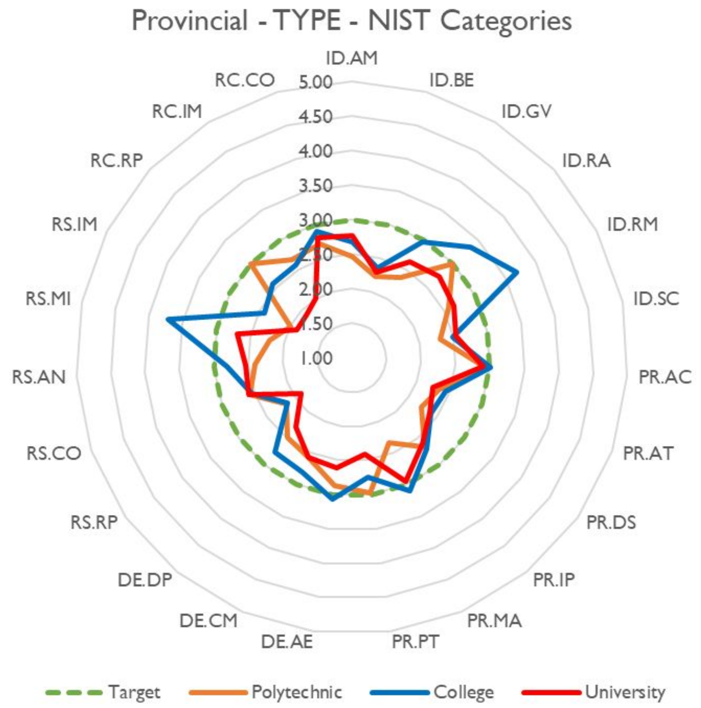
RS - Response Planning	85.7%
ID – Business Environment	84.8%
PR - Awareness and Training	80.0%
RS – Improvements	71.4%
PR – Data Security	69.0%
RC – Improvements	66.7%
DE - Detection process	65.7%
ID - Supply Chain Risk Mgmt.	64.8%
ID – Governance	64.3%
PR - Info Protection Proc/Procedures	63.9%
PR – Protective Technology	63.8%
ID - Asset Management	62.7%
RC – Recovery Planning	61.9%

Provincial/National Focus Areas

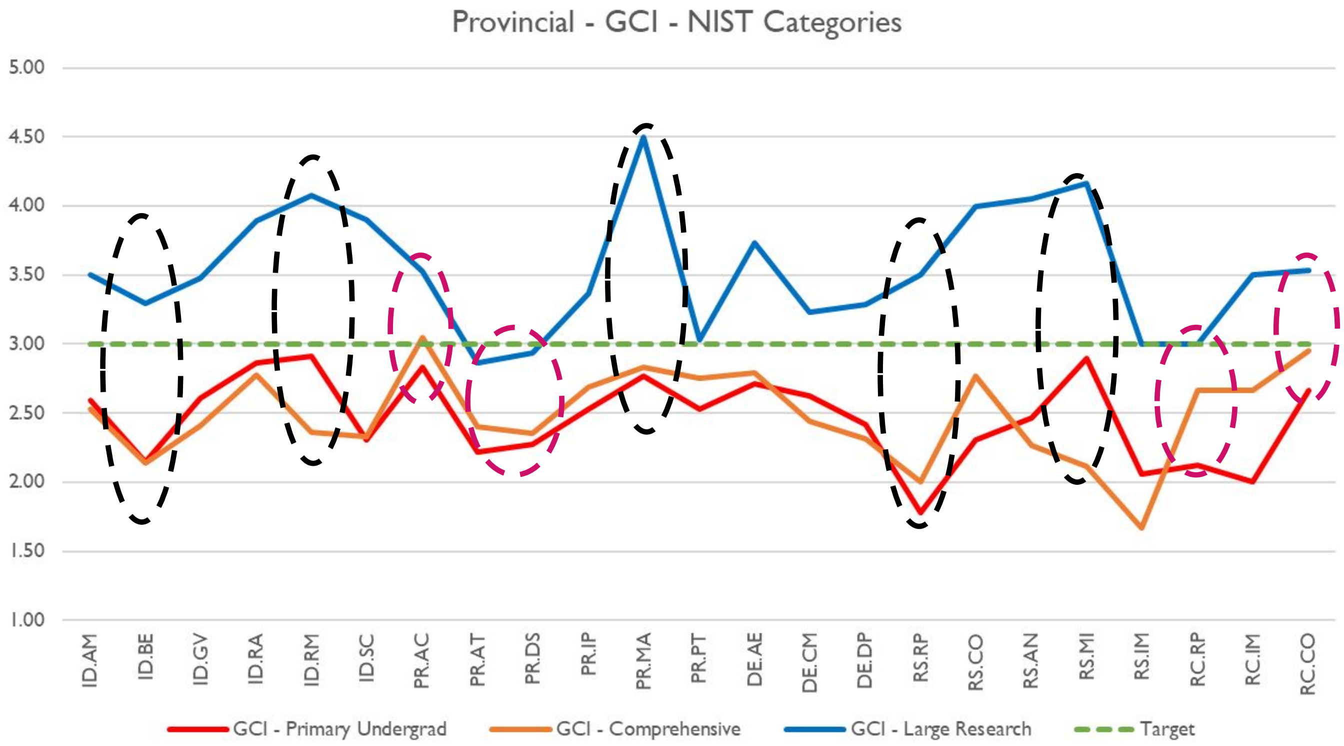
	PROVINCIAL	NATIONAL SORTED
85.7%	RS - Response Planning	RS - Response Planning
84.8%	ID – Business Environment	ID – Business Environment
80.0%	PR - Awareness and Training	PR - Awareness and Training
71.4%	RS – Improvements	RS - Improvements
69.0%	PR – Data Security	PR – Data Security
66.7%	RC – Improvements	RC - Improvements
65.7%	DE - Detection process	DE - Detection process
64.8%	ID - Supply Chain Risk Mgmt.	ID - Supply Chain Risk Mgmt.
64.3%	ID – Governance	
63.9%	PR - Info Protection Proc/Procedures	PR - Info Protection Proc/Procedures
63.8%	PR – Protective Technology	
62.7%	ID - Asset Management	ID - Asset Management
61.9%	RC – Recovery Planning	

GCI & Type NIST Categories

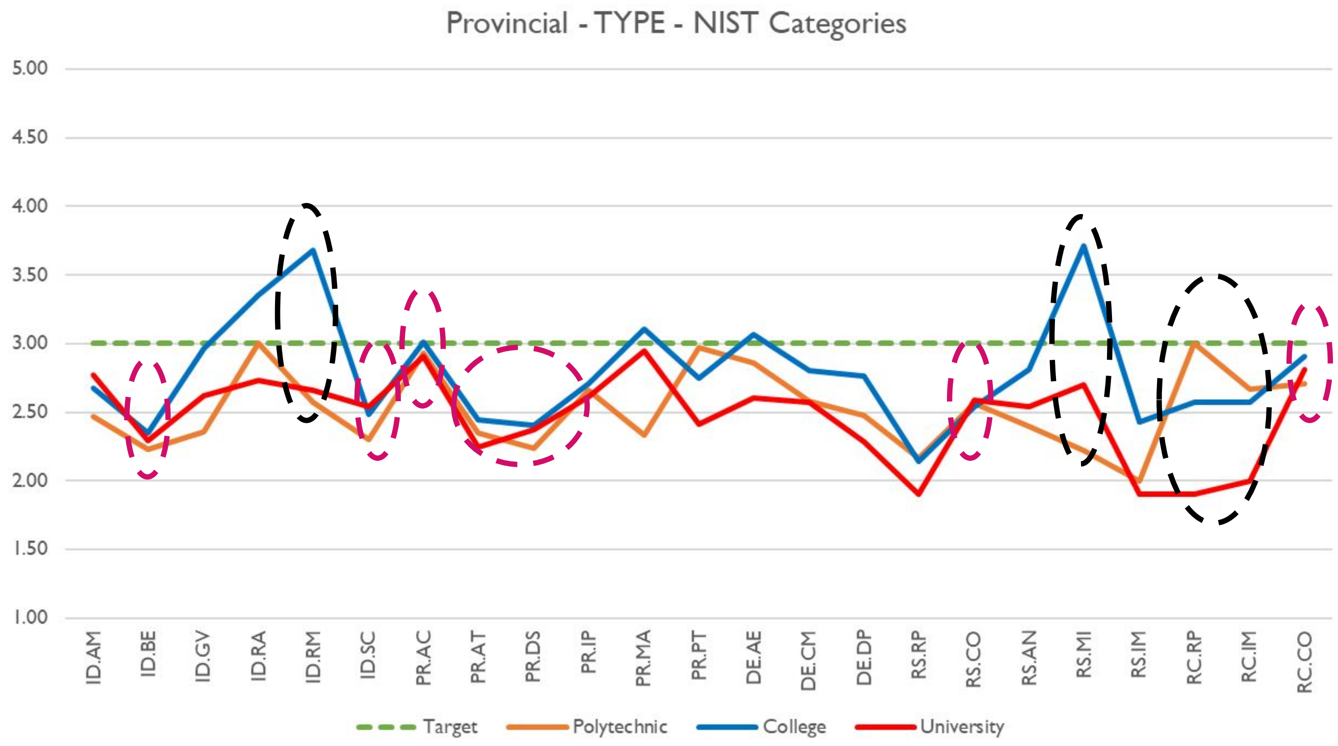




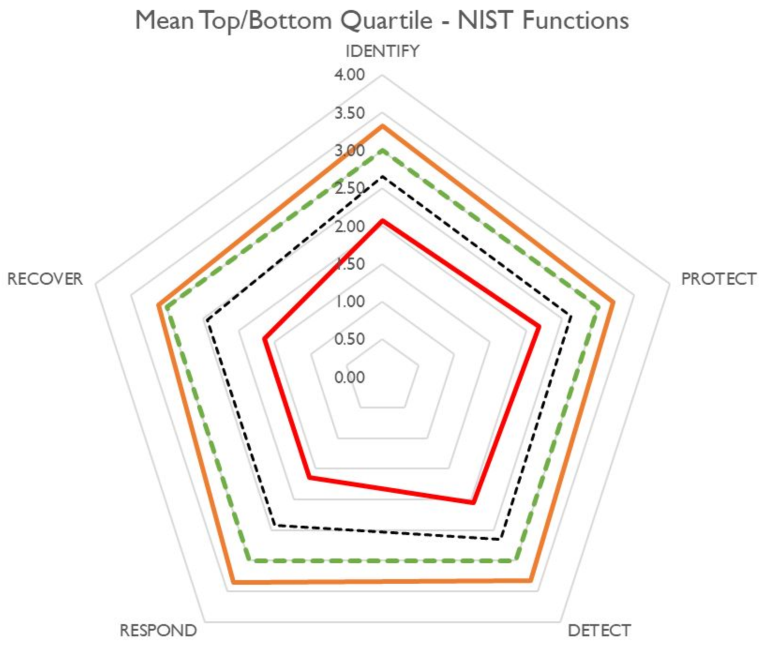
GCI & NIST Categories



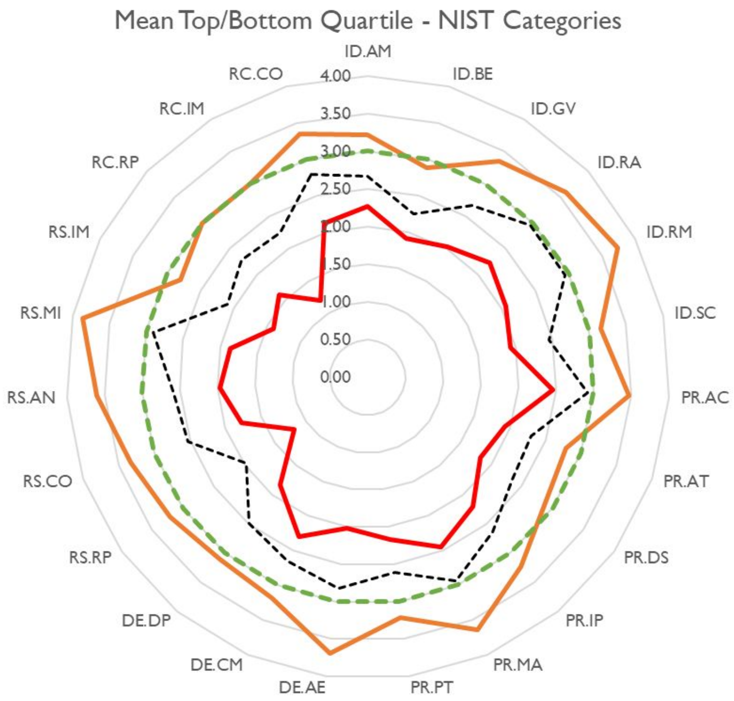
Type & NIST Categories



Top & Bottom Quartiles



Mean Top/Bottom Quartile - NIST Functions



Mean Top/Bottom Quartile - NIST Categories

What Now?

Recommendation

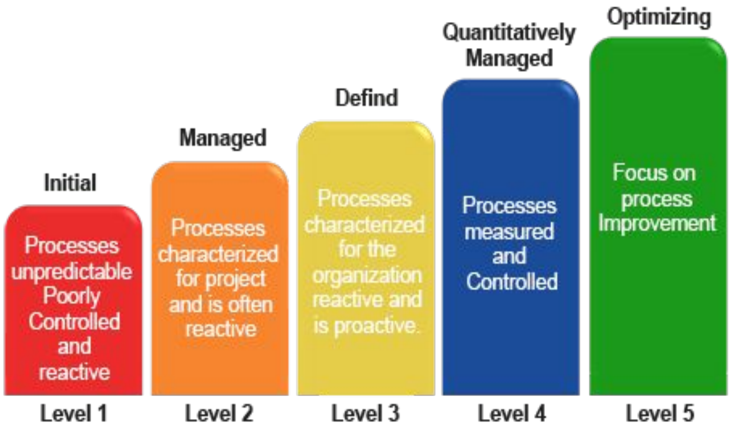
Run a workshop that includes cyber leaders from Alberta's institutions that uses the NCA data to answer the following questions:

- What should we do separately?
- What should we do together?
- What can we expect the Cybera rSOC/CanSSOC to assist with?
- How do we fund the initiatives?
- Can we create an initiatives roadmap?

Appendix

CMMI and Target Description

SCORE	MATURITY LEVEL	DESCRIPTION
1	Initial / Incomplete	Processes are unpredictable or nonexistent, poorly controlled, and reactive.
2	Managed	Processes are defined for projects and are often reactive.
3	Defined	Processes are defined for the organization and are proactive.
4	Quantitatively Managed	Processes are measured and controlled.
5	Optimizing	The focus is on continuous process improvement.


Initial
Processes unpredictable Poorly Controlled and reactive
Level 1
Managed
Processes characterized for project and is often reactive
Level 2
Defind
Processes characterized for the organization reactive and is proactive.
Level 3
Quantitatively Managed
Processes measured and Controlled
Level 4
Optimizing
Focus on process Improvement
Level 5

Characteristics of the Maturity Levels