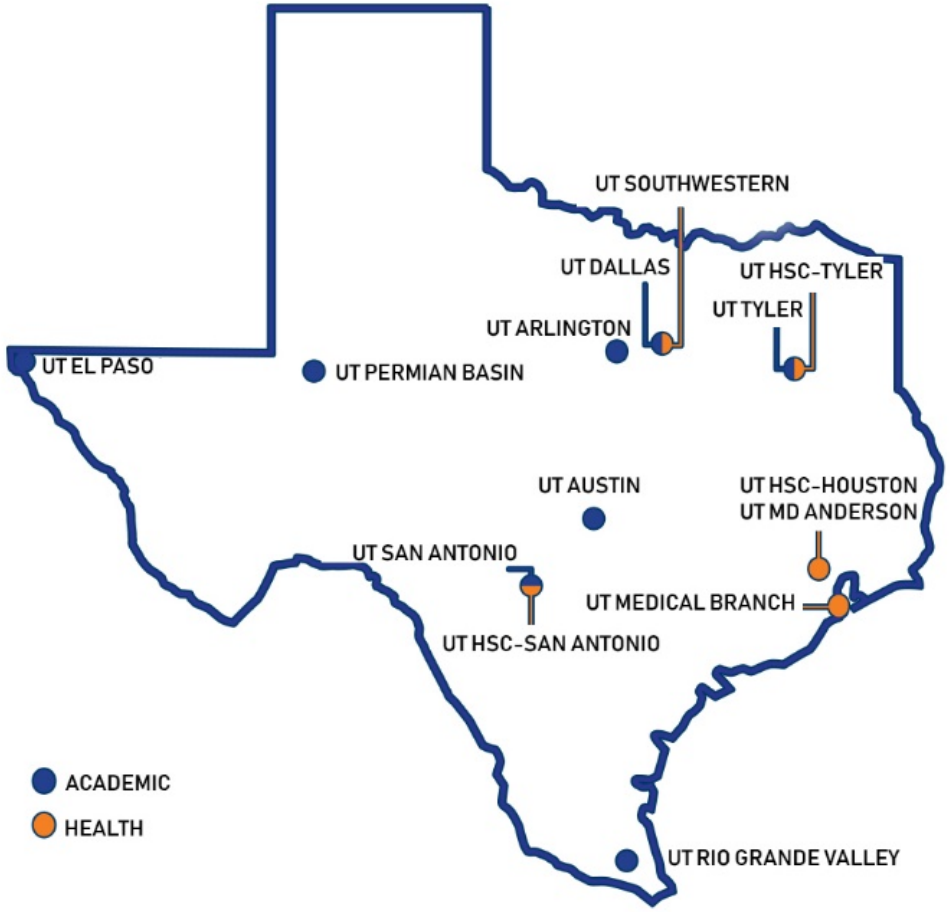
THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Herding Cats, Not Driving Cattle: Developing a Common Risk Reporting Framework Across a Diverse System

Helen Mohrmann, CISSP
Chief Information Security Officer
The University of Texas System

The University of Texas System



$2.9B IN RESEARCH

236K STUDENTS ENROLLED

8.2M OUTPATIENT VISITS

105K EMPLOYEES IN TX

No Actual Cats Were Harmed in the Execution of This Project

Let the Cat Herding Commence…

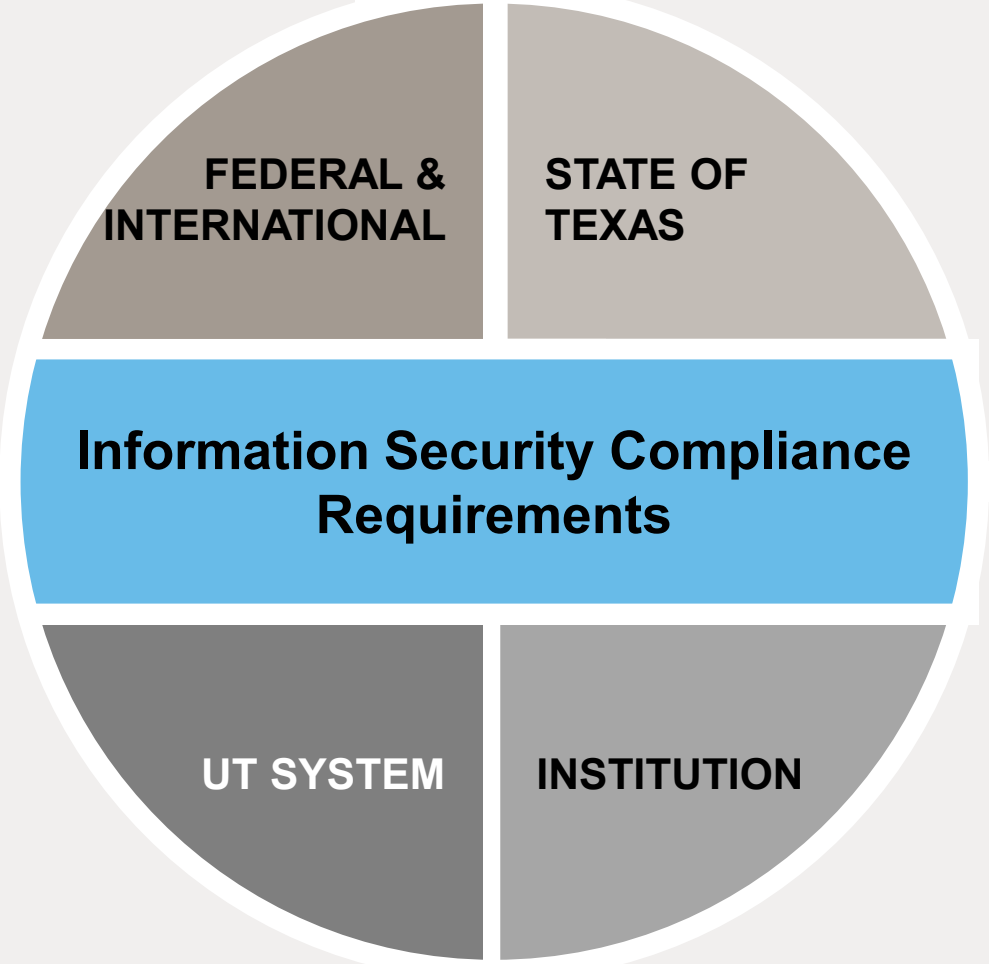
2 Institution CAEs

2 Institution CISOs

2 Institution CIOs

Part One: Reference Guide

DFARS
FERPA
FISMA
GDPR
GLBA
HIPAA
ITAR



TAC 202
TX Cyber Act
ITEPA

UTS 165
System Directives

Policies
Standards

Overview of Information Assets

Mission Critical or High Risk Asset	Custodian	Owner	Data Records	Potential Black Market Value
Description: *Blackboard Courses Website*	*School of Nursing*	*Dean*	*8,000*	$160,000 [see values below]

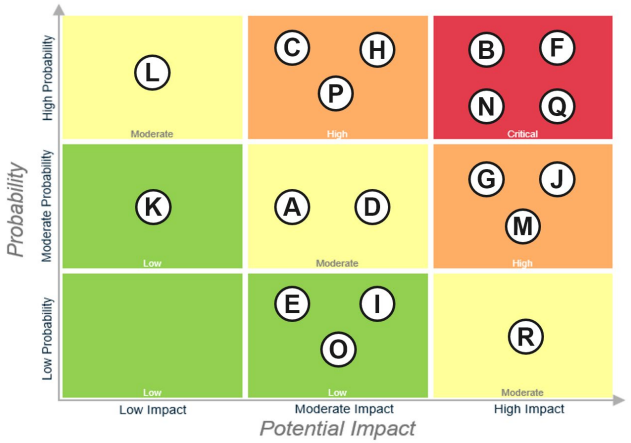
Overview of Computing Environment

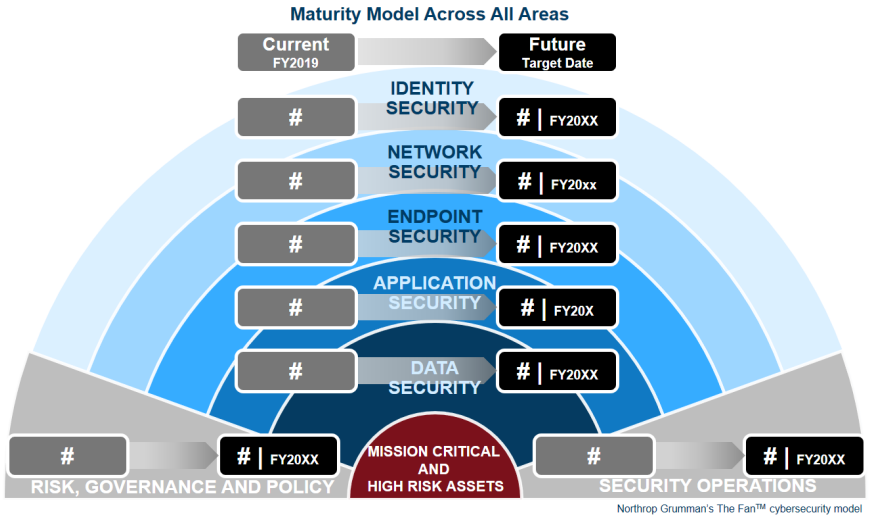
Device Type	Percent (%) of Devices Centrally Managed	# of Centrally Managed Devices	# of Decentrally Managed Devices
Workstations	*75%*	*7,500*	*2,500*
Servers			
Network Controllers			
Domain Controllers			

Part Two: Periodic Risk Update

ID	General Risk (category consistent across the System)	Risk Rating
A	Involvement of security staff in important processes	
B	Vulnerability and patch management	
C	Funds for necessary equipment or application upgrades	
D	Network security	
E	Overall security strategy	
F	Management of systems and assets	
G	Security risk assessments	
H	Security and/or IT staff	
I	Threat management	

ID	General Risk (category consistent across the System)	Risk Rating
J	Access control management	
K	Incident response plans	
L	Third party risk management process	
M	IIT lifecycle processes	
N	Inventory information	
O	Security culture or security awareness	
P	Data management and protection	
Q	Insider threats	
R	Physical and environmental security around critical IT infrastructure	





Consistent Risk List

Common Risk List

ID	General Risk (category consistent across the System)
A	Involvement of security staff in important processes
B	Vulnerability and patch management
C	Funds for necessary equipment or application upgrades
D	Network security
E	Overall security strategy
F	Management of systems and assets
G	Security risk assessments
H	Security and/or IT staff
I	Threat management

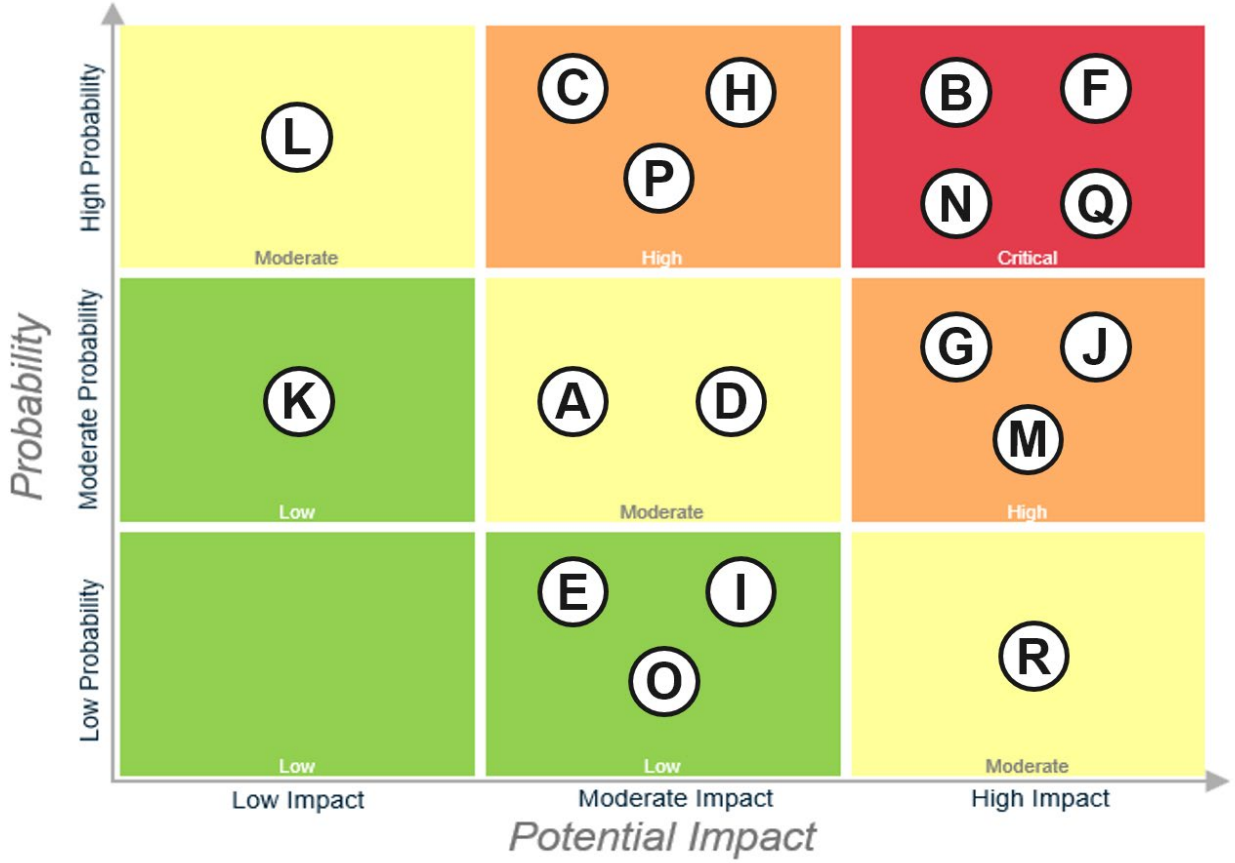
ID	General Risk (category consistent across the System)
J	Access control management
K	Incident response plans
L	Third party risk management process
M	IIT lifecycle processes
N	Inventory information
O	Security culture or security awareness
P	Data management and protection
Q	Insider threats
R	Physical and environmental security around critical IT infrastructure




Risk Components

General Risk	Specific Risk	Business Impact
Access control	2FA should be in front the student financial aid portal	Potential unauthorized access or modifications to student financial information
Access control	Erratic follow through on disabling access after staff terminations	Potential unauthorized access to a wide variety of systems

Risk Heat Map



Rate All Risks Table

ID	General Risk (category consistent across the System)	Risk Rating
A	Involvement of security staff in important processes	
B	Vulnerability and patch management	
C	Funds for necessary equipment or application upgrades	
D	Network security	
E	Overall security strategy	
F	Management of systems and assets	
G	Security risk assessments	
H	Security and/or IT staff	
I	Threat management	

ID	General Risk (category consistent across the System)	Risk Rating
J	Access control management	
K	Incident response plans	
L	Third party risk management process	
M	IIT lifecycle processes	
N	Inventory information	
O	Security culture or security awareness	
P	Data management and protection	
Q	Insider threats	
R	Physical and environmental security around critical IT infrastructure	

**Disclaimer: all data is hypothetical and does not represent actual institution risk posture.*

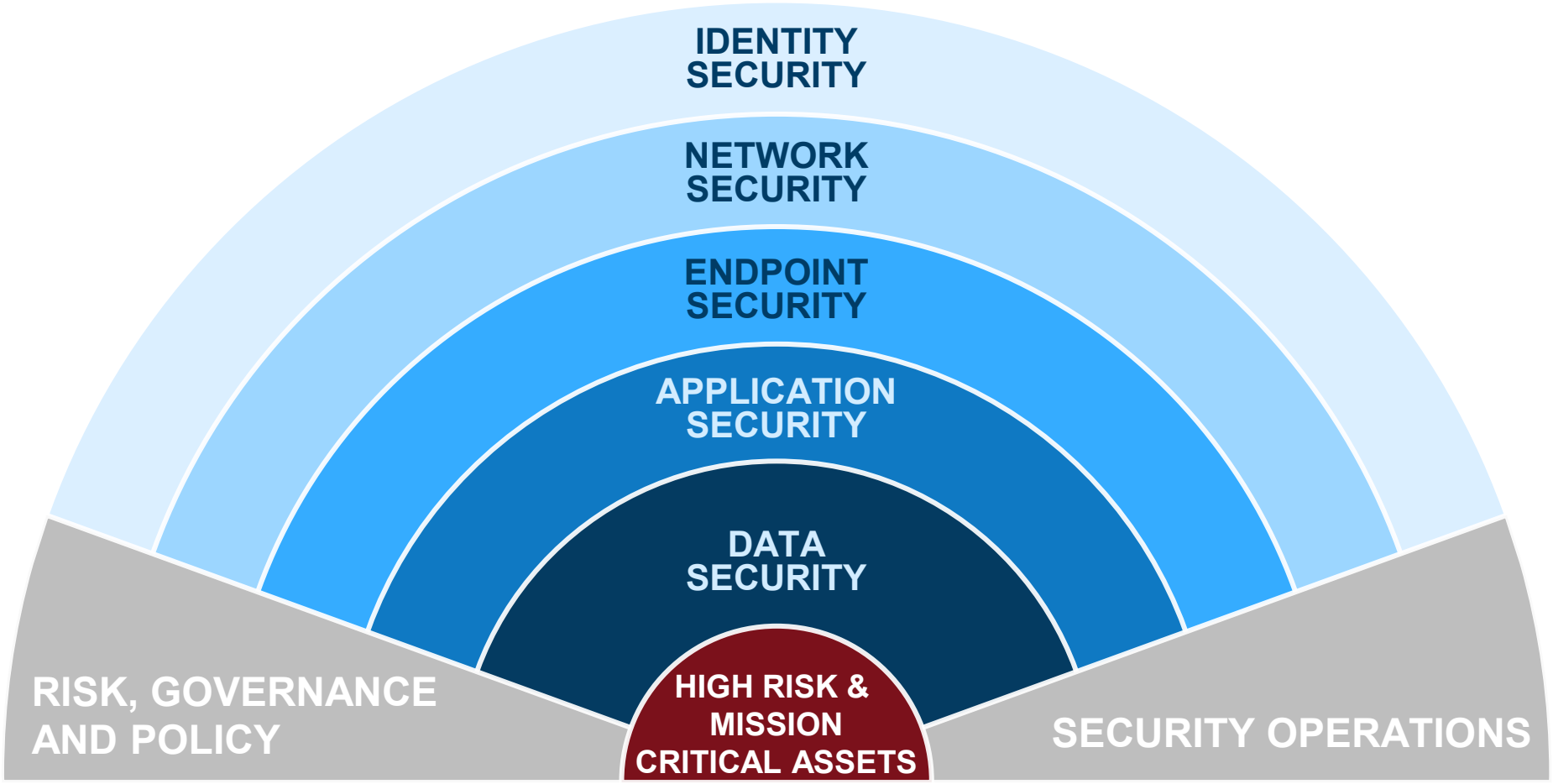
Risk Mitigation Strategies

Risk Mitigation Strategies*

Related Risk	Project Description	Plan Start	Plan Status (Proposed, Approved, In Progress, Complete)	Plan Completion	Issues / Notes
J	[Description in non-technical terms] Two factor authentication for students	[month/year]	Not Started	September 2019	Roll out logistics to students
A	[Description in non-technical terms]				
B	[Description in non-technical terms]				
C	[Description in non-technical terms]				

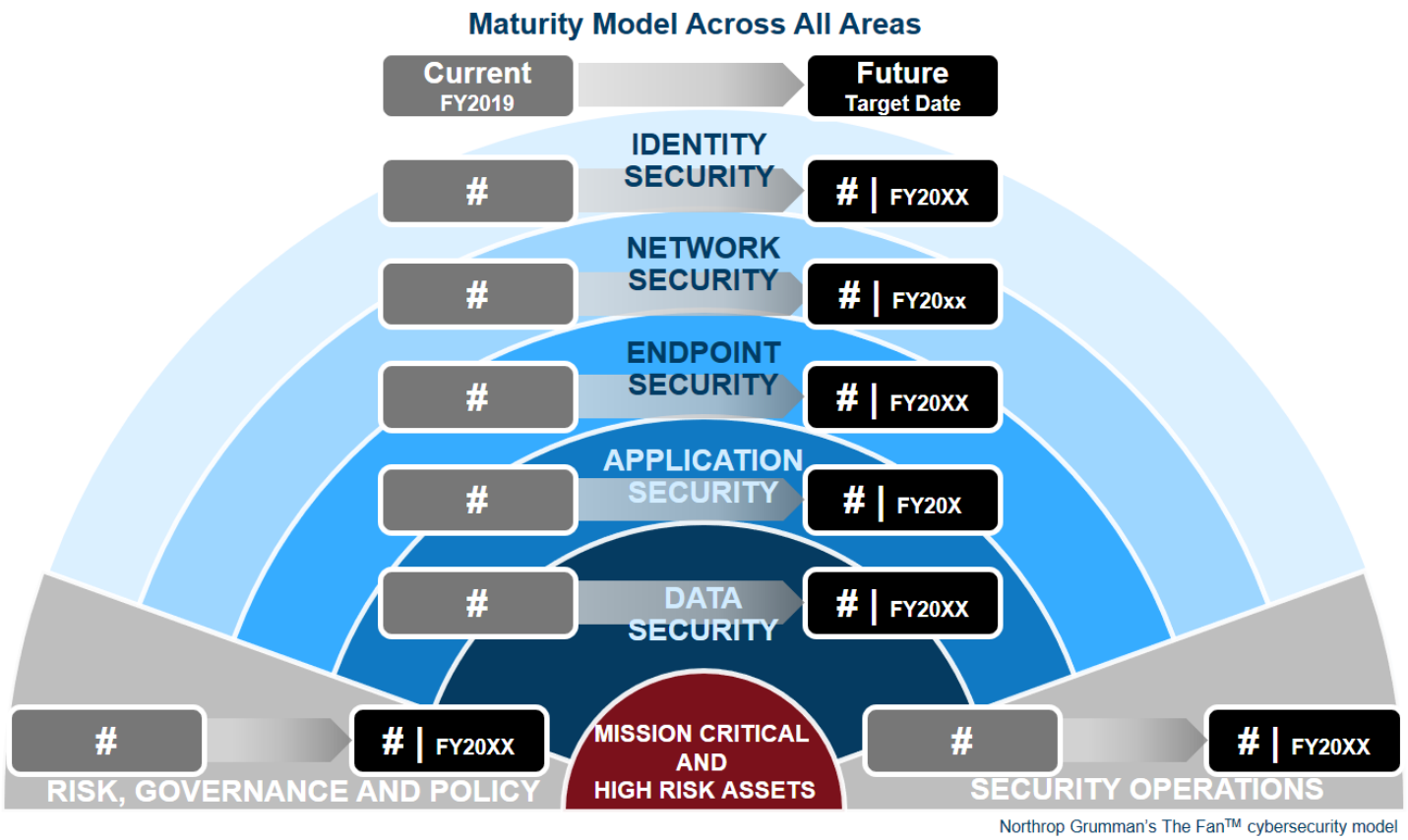
**Disclaimer: all data is hypothetical and does not represent actual institution risk posture.*

Protective Layers



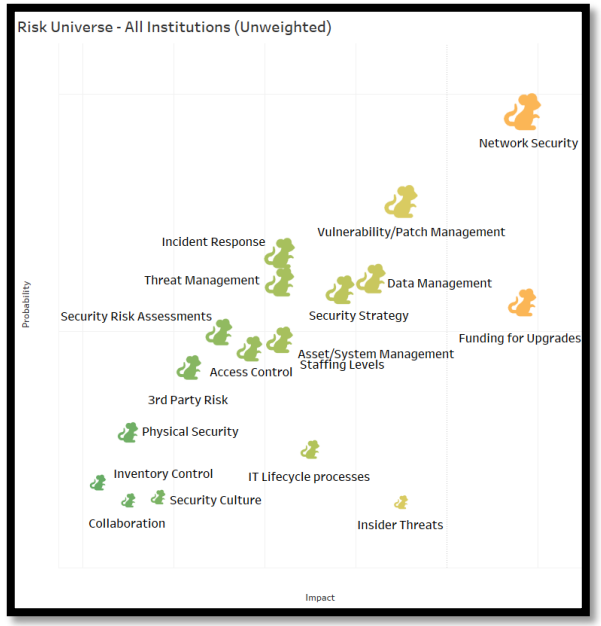
Northrop Grumman's The Fan™ cybersecurity model

Maturity



Northrop Grumman's The Fan™ cybersecurity model

Part Three: Systemwide Summary



Institution Risk Map*

Risks	Abbr.	UNI 1	UNI 2	UNI 3	UNI 4	UNI 5	UNI 6	UNI 7	UNI 8	UNI 9	UNI 10	UNI 11	UNI 12	UNI 13	UNI 14	UNI 15
Staffing Levels	A															
Vulnerability/Patch Management	B															
Funding for Upgrades	C															
Network Security	D															
Security Strategy	E															
Asset/System Management	F															
Security Risk Assessments	G															
Collaboration	H															
Threat Management	I															
Access Control	J															
Incident Response	K															
3rd Party Risk	L															
IT Lifecycle processes	M															
Inventory Control	N															
Security Culture	O															
Data Management	P															
Insider Threats	Q															
Physical Security	R															

**Disclaimer: all data is hypothetical and does not represent actual institution risk posture.*

Institution Risk Map*

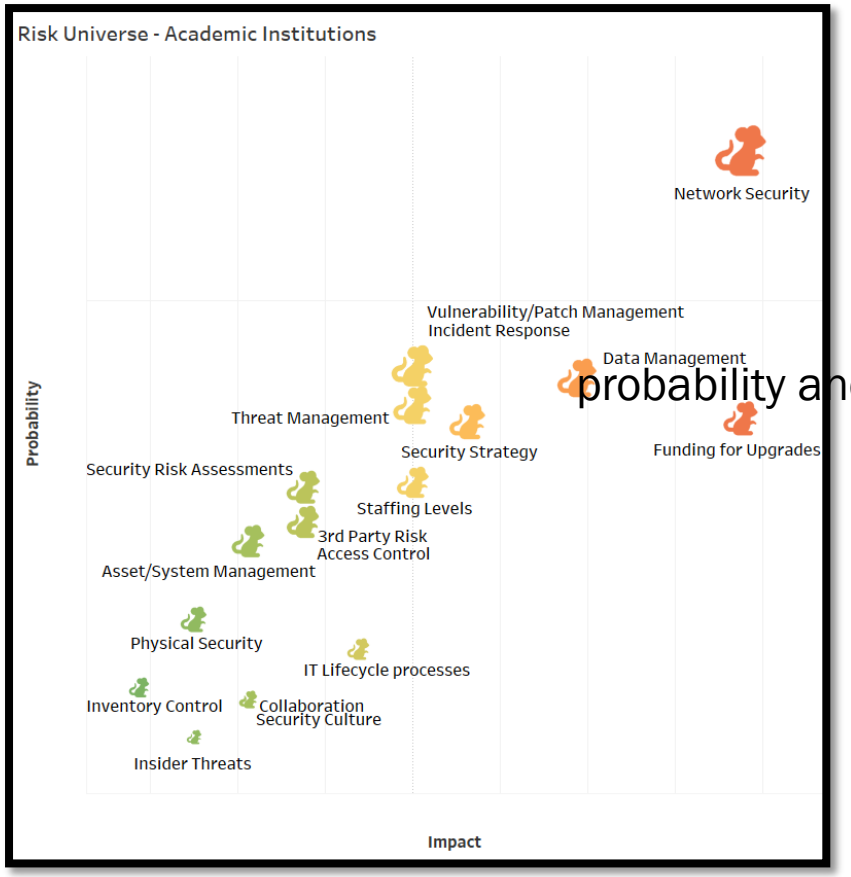
Risks	Abbr.	UNI 1	UNI 2	UNI 3	UNI 4	UNI 5	UNI 6	UNI 7	UNI 8	UNI 9	UNI 10	UNI 11	UNI 12	UNI 13	UNI 14	UNI 15
Staffing Levels	A															
Vulnerability/Patch Management	B															
Funding for Upgrades	C															
Network Security	D															
Security Strategy	E															
Asset/System Management	F															
Security Risk Assessments	G															
Collaboration	H															
Threat Management	I															
Access Control	J															
Incident Response	K															
3rd Party Risk	L															
IT Lifecycle processes	M															
Inventory Control	N															
Security Culture	O															
Data Management	P															
Insider Threats	Q															
Physical Security	R															

Disclaimer: all data is hypothetical and does not represent actual institution risk posture.

Risk Universe Map*

Disclaimer: all data is hypothetical and does not represent actual institution risk posture.

Weighted Risk Universe Maps*

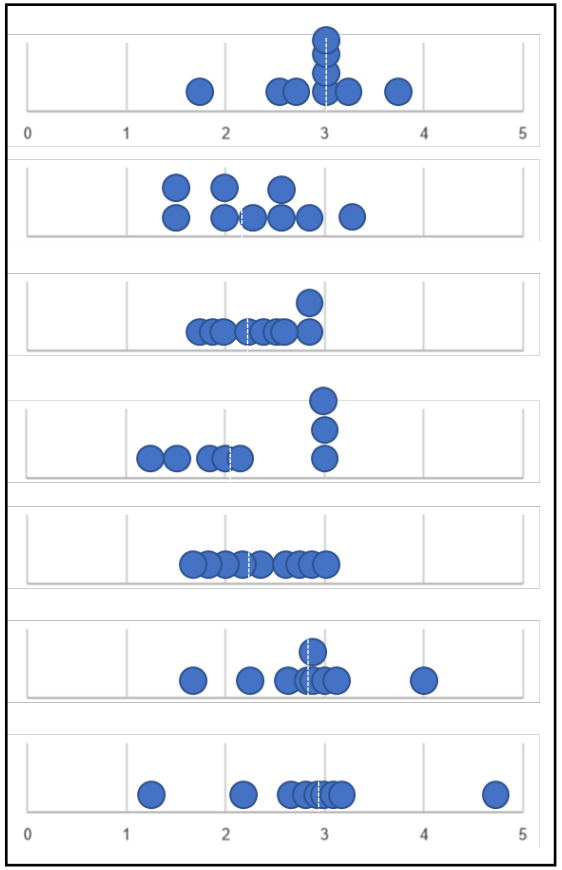


probability and impact of general risk categories.

Disclaimer: all data is hypothetical and does not represent actual institution risk posture.

Current Program Maturity Levels

Academic Institutions



Identity Security

Network Security

Endpoint Security

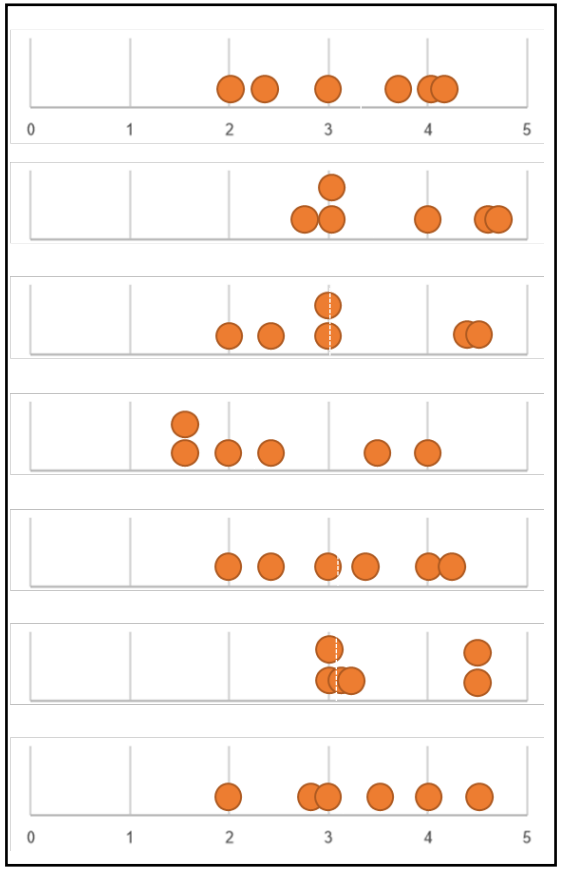
Application Security

Data Security

Risk, Governance, Policy

Security Operations

Healthcare Institutions



0.0	Non-existent
1.0	Ad-hoc
2.0	Repeatable
3.0	Defined
4.0	Risk-based
5.0	Optimized

Further Thoughts

Questions