



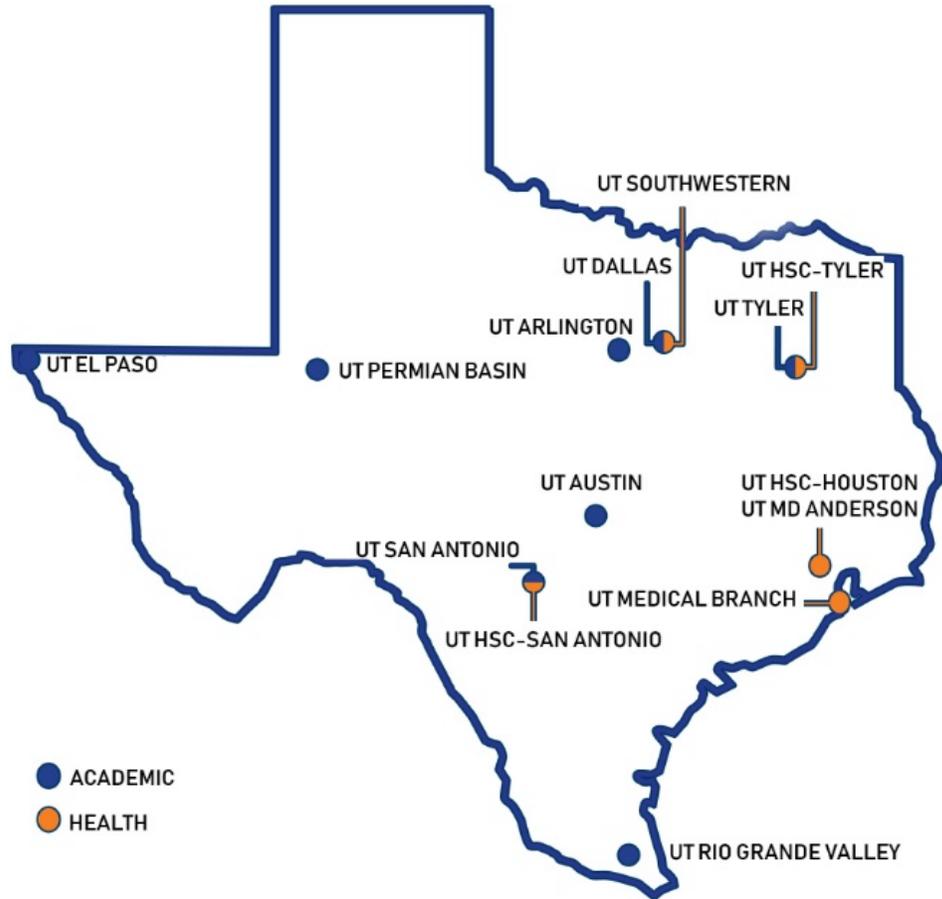
THE UNIVERSITY of TEXAS SYSTEM  
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

# **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<sup>2</sup>

# No Actual Cats Were Harmed in the Execution of This Project





# Let the Cat Herding Commence...



2 Institution CAEs



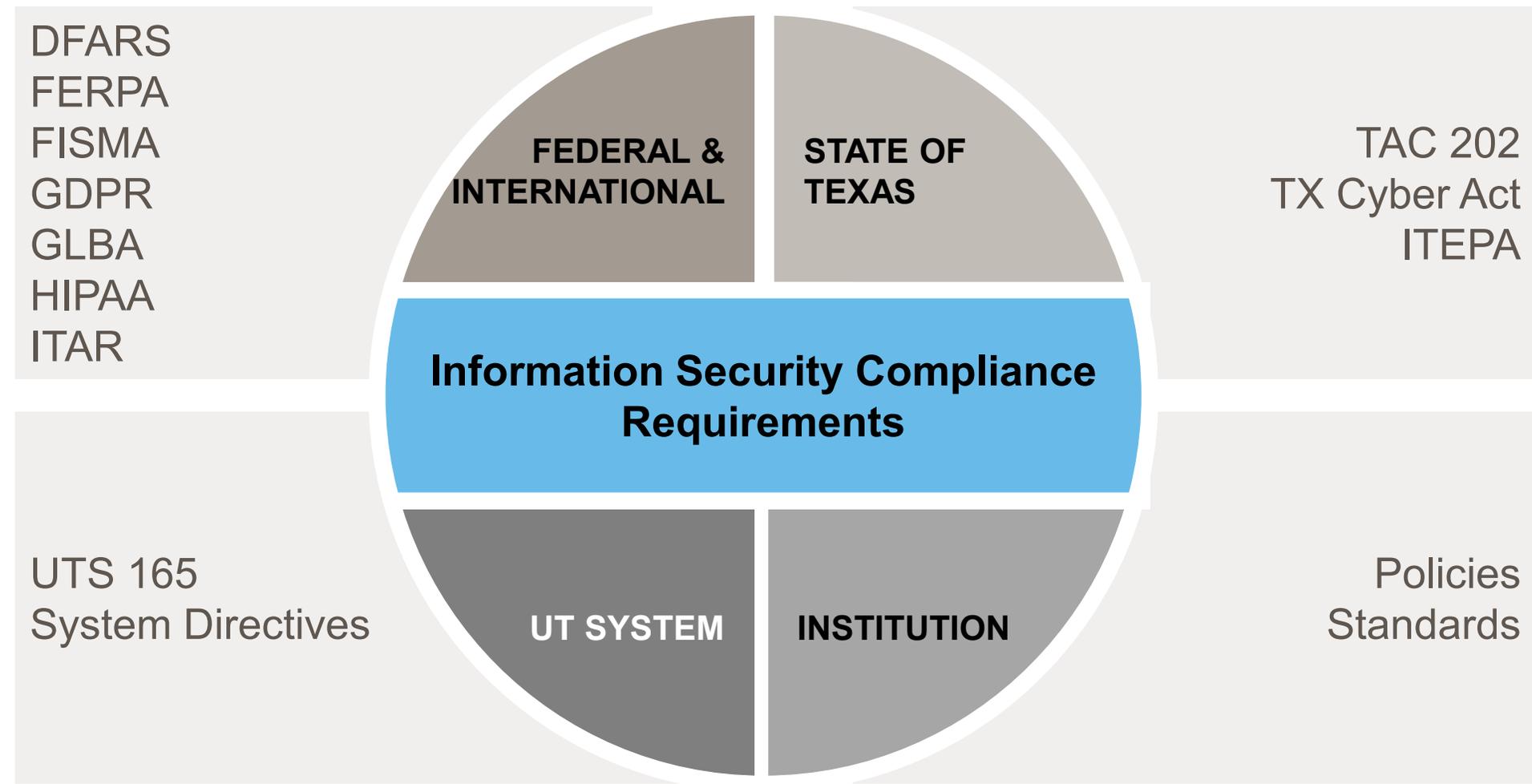
2 Institution CISOs



2 Institution CIOs



# Part One: Reference Guide





# Overview of Information Assets



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



# Overview of Computing Environment



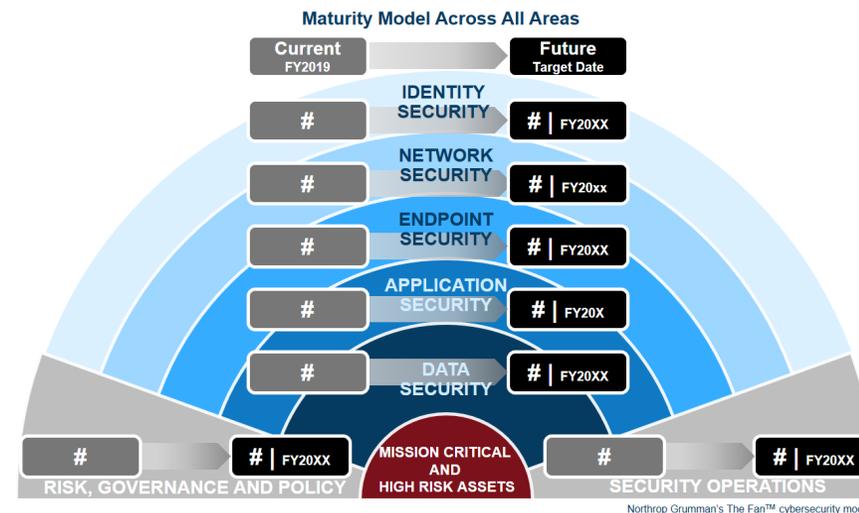
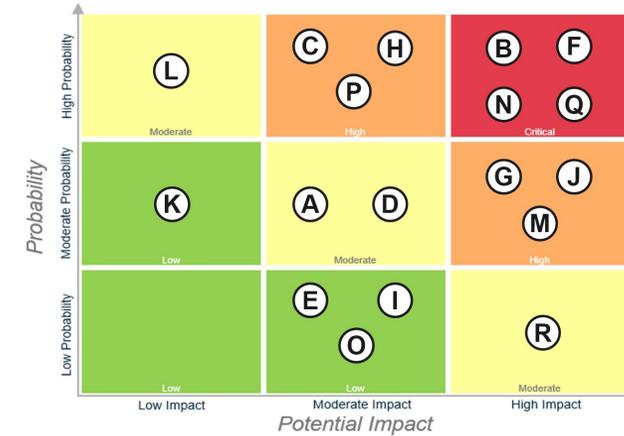
Device Type	Percent (%) of Devices Centrally Managed	# of Centrally Managed Devices	# of Decentrally Managed Devices
Workstations	75%	7,500	2,500
Servers			
Network Controllers			
Domain Controllers			



# Part Two: Periodic Risk Update



ID	General Risk (category consistent across the System)	Risk Rating	ID	General Risk (category consistent across the System)	Risk Rating
A	Involvement of security staff in important processes	Green	J	Access control management	Green
B	Vulnerability and patch management	Yellow	K	Incident response plans	Yellow
C	Funds for necessary equipment or application upgrades	Red	L	Third party risk management process	Yellow
D	Network security	Yellow	M	IT lifecycle processes	Yellow
E	Overall security strategy	Green	N	Inventory information	Red
F	Management of systems and assets	Yellow	O	Security culture or security awareness	Yellow
G	Security risk assessments	Yellow	P	Data management and protection	Yellow
H	Security and/or IT staff	Yellow	Q	Insider threats	Yellow
I	Threat management	Red	R	Physical and environmental security around critical IT infrastructure	Green





# 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





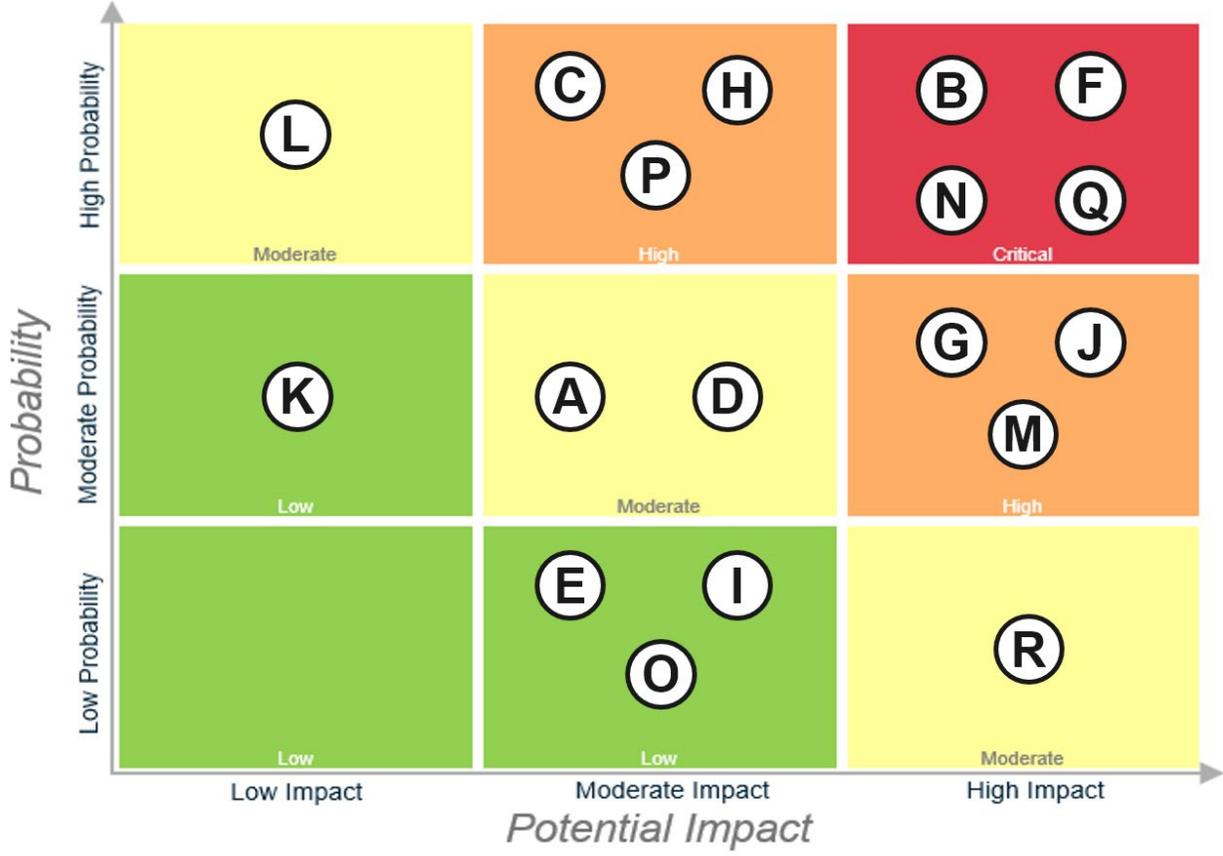
# Risk Components



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	Green
B	Vulnerability and patch management	Yellow
C	Funds for necessary equipment or application upgrades	Red
D	Network security	Yellow
E	Overall security strategy	Green
F	Management of systems and assets	Yellow
G	Security risk assessments	Yellow
H	Security and/or IT staff	Yellow
I	Threat management	Red

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

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



# Risk Mitigation Strategies





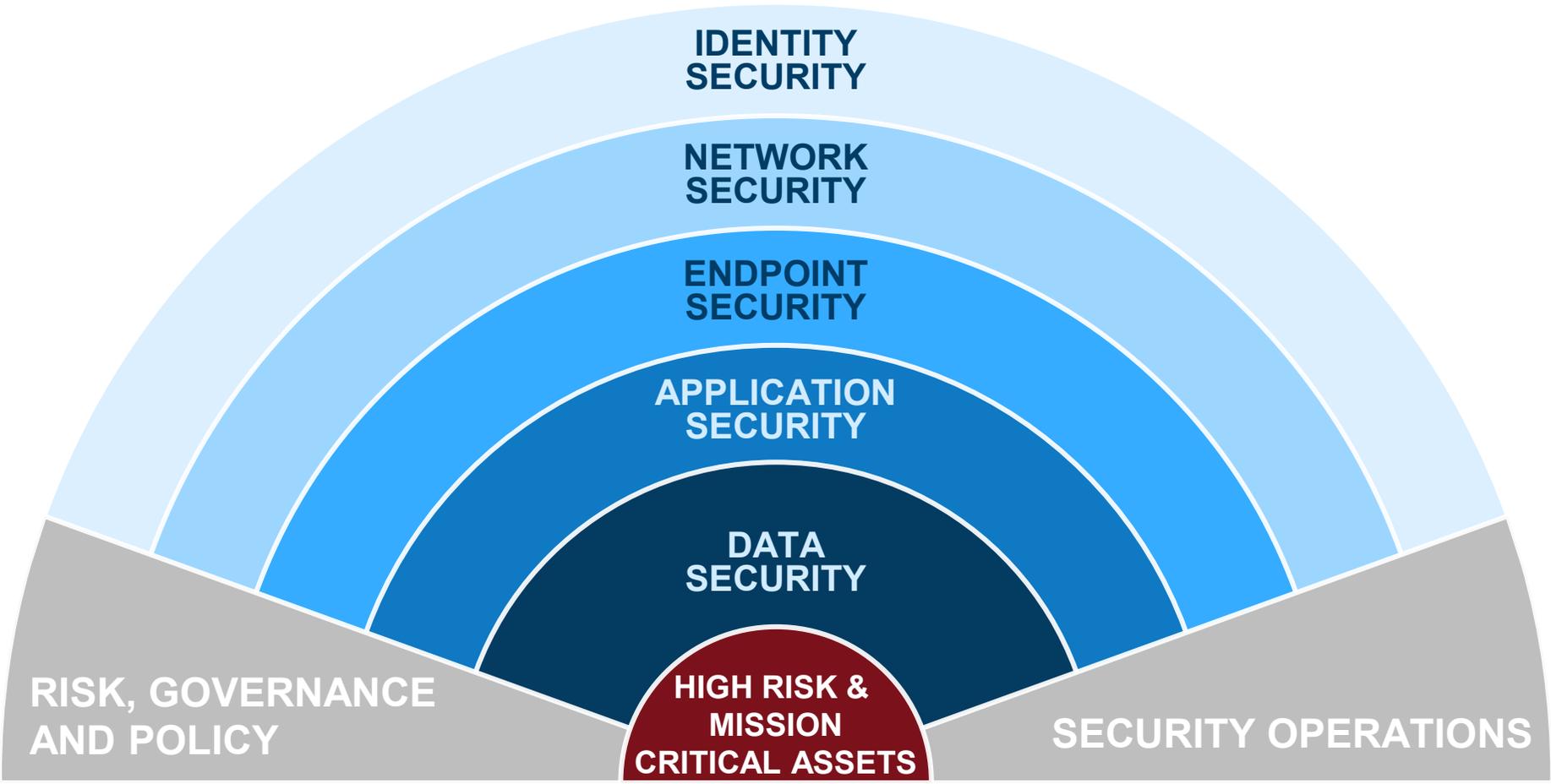
# Risk Mitigation Strategies\*

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.*

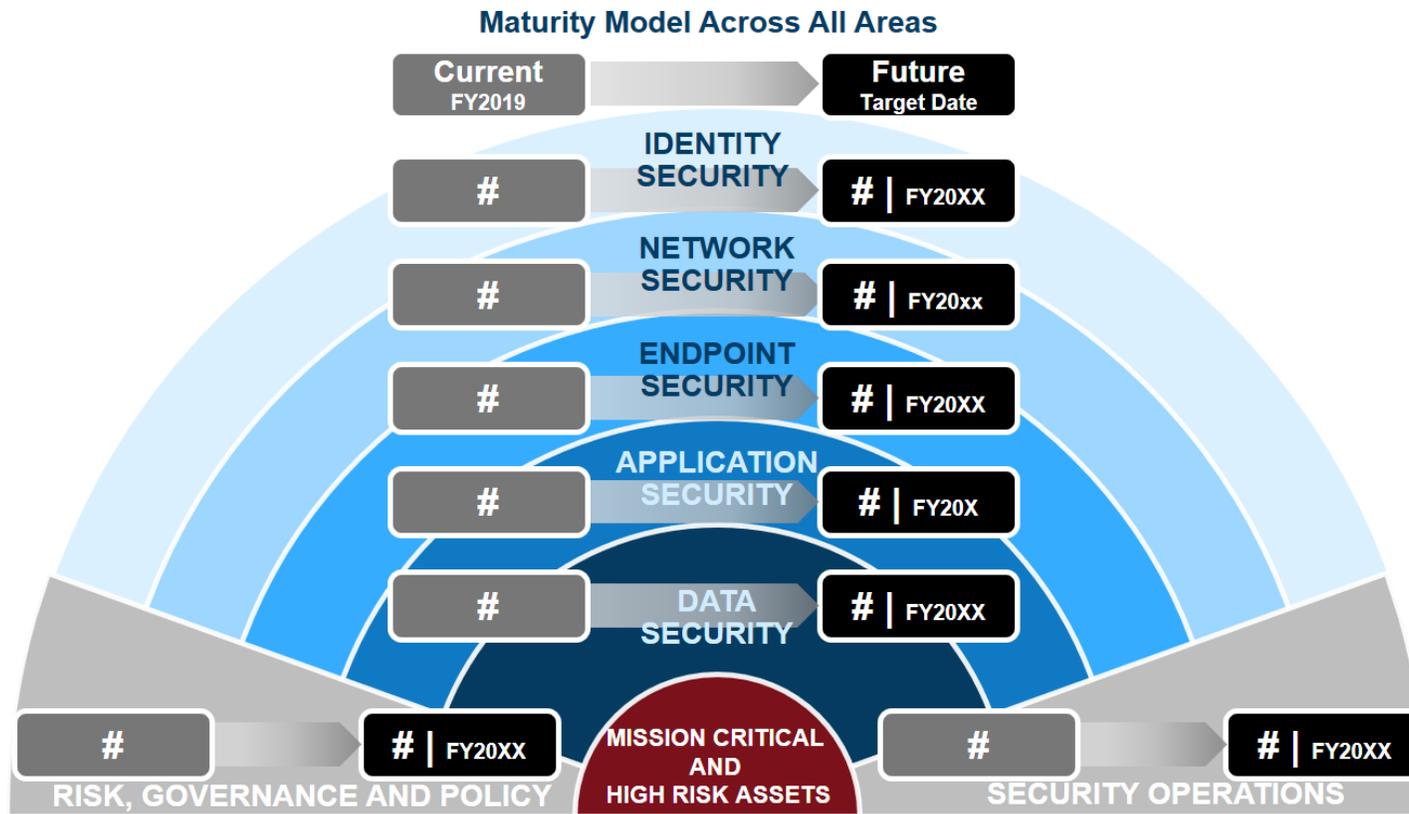


# Protective Layers



Northrop Grumman's The Fan™ cybersecurity model

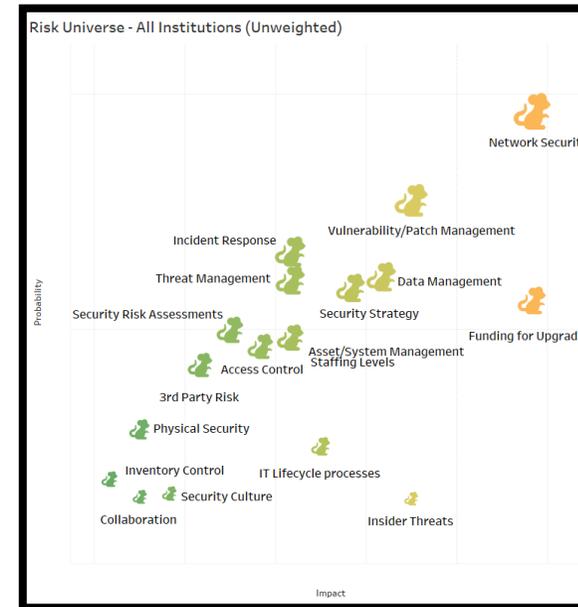
# Maturity



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	Red														
Vulnerability/Patch Management	B	Red														
Funding for Upgrades	C	Red	Red	Red	Yellow	Yellow	Red	Yellow	Yellow	Red	Red	Red	Red	Red	Red	Yellow
Network Security	D	Yellow														
Security Strategy	E	Yellow														
Asset/System Management	F	Yellow														
Security Risk Assessments	G	Yellow														
Collaboration	H	Yellow	Yellow	Yellow	Green	Yellow	Orange	Orange								
Threat Management	I	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Orange	Yellow	Yellow	Yellow	Yellow
Access Control	J	Yellow														
Incident Response	K	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green	Green	Yellow
3rd Party Risk	L	Yellow	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Yellow	Yellow	Yellow	Yellow
IT Lifecycle processes	M	Green	Green	Green	Green	Green	Green	Yellow	Green							
Inventory Control	N	Green														
Security Culture	O	Green														
Data Management	P	Green	Yellow	Green	Green	Green	Green	Green	Yellow							
Insider Threats	Q	Green														
Physical Security	R	Green	Green	Green	Green	Yellow	Green									

\*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	Yellow	Yellow	Yellow	Orange	Orange	Orange	Green	Red	Yellow	Green	Green	Green	Yellow	Yellow	Orange
Vulnerability/Patch Management	B	Orange	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Red	Green	Yellow	Yellow	Yellow	Yellow	Orange
Funding for Upgrades	C	Yellow	Orange	Yellow	Red	Red	Orange	Red	Red	Orange	Green	Green	Yellow	Yellow	Green	Red
Network Security	D	Red	Orange	Red	Orange	Orange	Orange	Orange	Orange	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Orange
Security Strategy	E	Orange	Yellow	Green	Yellow	Yellow	Yellow	Red	Orange	Orange	Yellow	Green	Green	Yellow	Yellow	Yellow
Asset/System Management	F	Orange	Yellow	Orange	Yellow	Yellow	Yellow	Green	Yellow	Orange						
Security Risk Assessments	G	Orange	Green	Green	Yellow	Orange	Orange	Green	Red	Orange	Green	Green	Yellow	Yellow	Yellow	Green
Collaboration	H	Yellow	Green	Green	Orange	Orange	Green	Orange	Orange	Yellow	Yellow	Green	Green	Green	Green	Orange
Threat Management	I	Orange	Yellow	Yellow	Yellow	Yellow	Orange	Yellow	Orange	Yellow	Yellow	Green	Yellow	Yellow	Green	Yellow
Access Control	J	Yellow	Orange	Yellow	Green	Yellow	Yellow	Yellow	Yellow							
Incident Response	K	Red	Green	Green	Yellow	Orange	Orange	Orange	Orange	Yellow	Yellow	Yellow	Yellow	Green	Green	Orange
3rd Party Risk	L	Orange	Green	Green	Yellow	Orange	Orange	Yellow	Orange	Yellow	Green	Green	Green	Yellow	Yellow	Yellow
IT Lifecycle processes	M	Yellow	Yellow	Yellow	Yellow	Orange	Orange	Red	Yellow	Orange	Green	Yellow	Yellow	Green	Yellow	Orange
Inventory Control	N	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Orange	Green	Green	Green	Yellow	Yellow	Yellow
Security Culture	O	Green	Yellow	Green	Yellow	Orange	Orange	Yellow	Orange	Yellow	Yellow	Green	Yellow	Green	Yellow	Yellow
Data Management	P	Orange	Yellow	Orange	Yellow	Red	Yellow	Red	Orange	Orange	Green	Yellow	Yellow	Green	Green	Yellow
Insider Threats	Q	Yellow	Yellow	Orange	Yellow	Yellow	Yellow	Green	Yellow	Orange	Red	Orange	Yellow	Orange	Yellow	Orange
Physical Security	R	Yellow	Yellow	Yellow	Yellow	Orange	Yellow	Green	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Green	Green

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

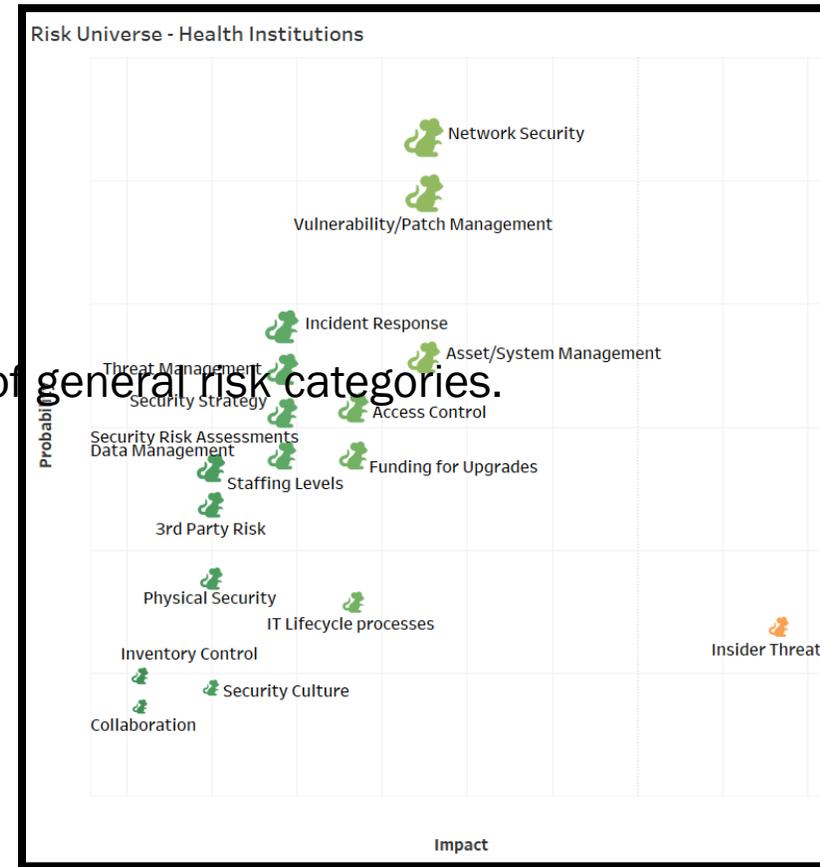
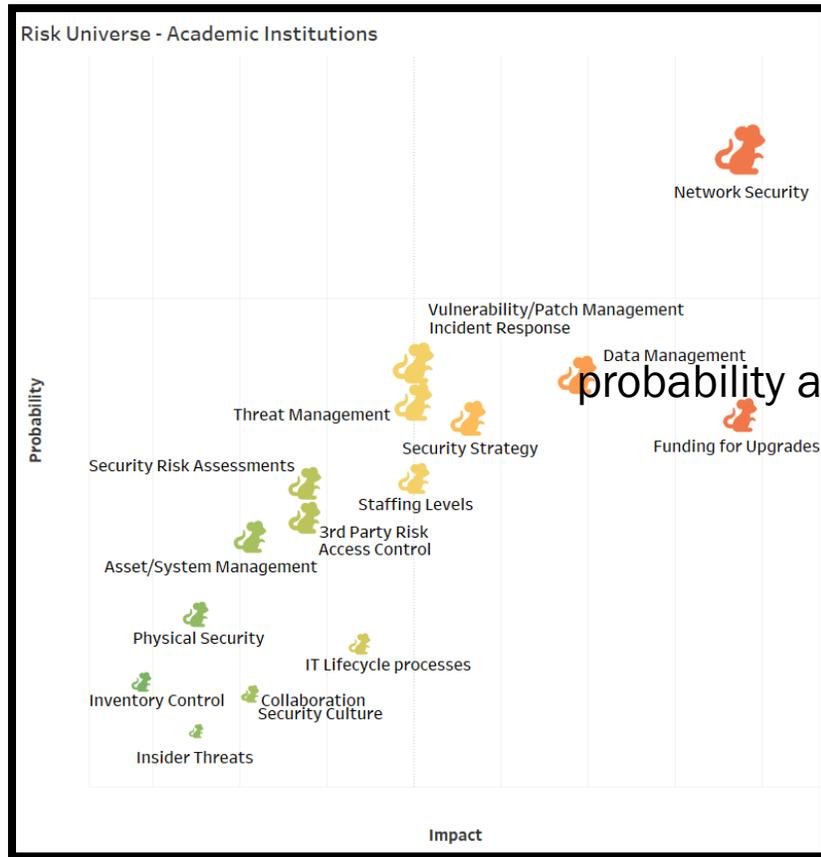
# Risk Universe Map\*



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



# Weighted Risk Universe Maps\*



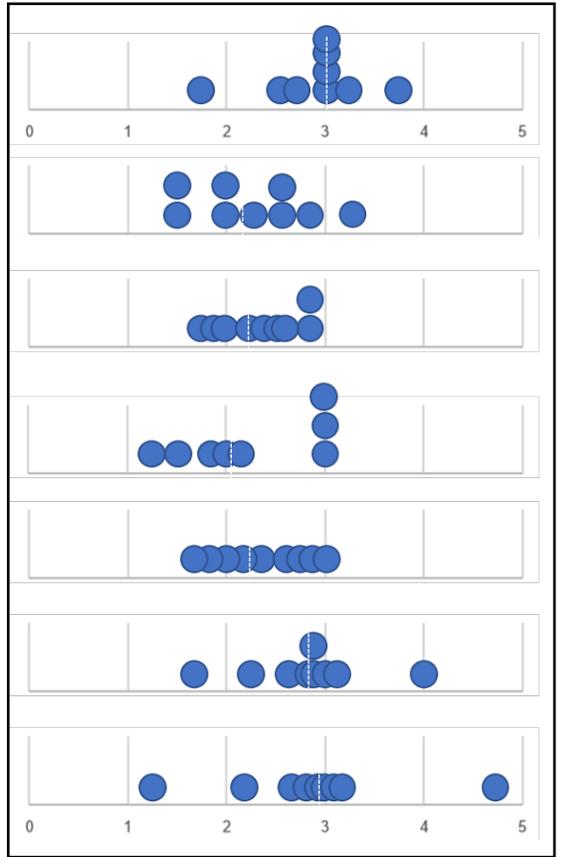
probability and impact of general risk categories.

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

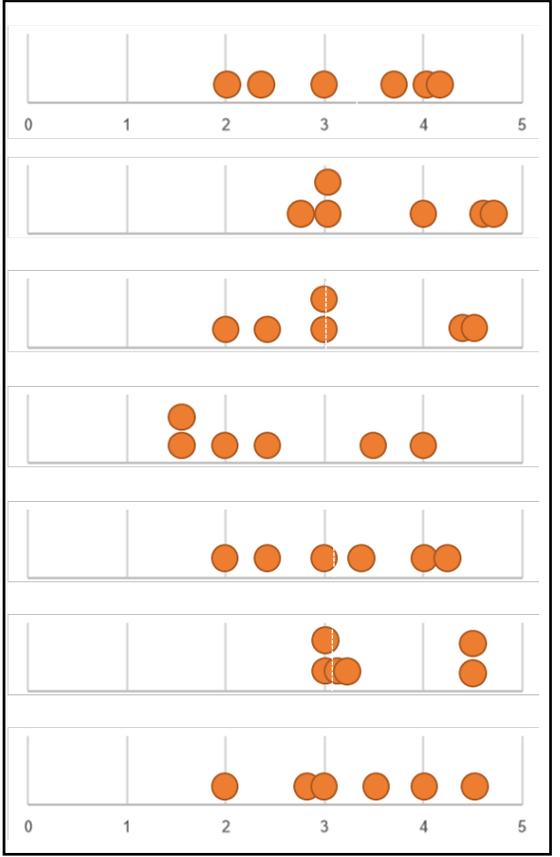


# Current Program Maturity Levels

### Academic Institutions



### Healthcare Institutions



- Identity Security
- Network Security
- Endpoint Security
- Application Security
- Data Security
- Risk, Governance, Policy
- Security Operations

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



# Further Thoughts



# Questions

