ICMA | conference

BUILDING A CULTURE OF UNSHAKEABLE SECURITY

Brian A. Engle
CISO & Managing Directory of Cybersecurity Advisory Services
CYBERDEFENSES

October 21, 2019

Unshakeable Security

1

STRATEGIC PLAN

Chart the Course, Define the Initiatives, and Execute

2

CYBERSECURITY READINESS

Continuous Monitoring, Detection, Response and Recovery

3

MANAGED RISK

Identify Threats, Evaluate Risks and Adjust the Course

CYBERDEFENSES

#ICMA2019

STRATEGIC PLAN

An investment strategy that develops cybersecurity capabilities aligned to the business risks.

Not a shopping list of technologies.

STRATEGY IS…

Not Budget Wish List

Not a Technology Roadmap

Not a To-do List

Nothing Without Execution

CYBERSECURITY MADE EASY
AND WHY IT'S STILL SO HARD

Building a security program is like building a new business.

Or it should be.

- Define your core competencies and maximize your investments.
- Spend like it's your money and measure the impact of the investment.
- By taking ownership at the top, leadership defines a culture that makes security a priority.

CORE CHALLENGES FOR CITIES

Minimal IT Resources, Max Security Demands

- Limited budget and few dedicated security staff
- Same control requirements as larger organizations

+

Equal Opportunity Threats and Attackers

- Threat actors don't discriminate by size
- Criminals don't wait for you to improve your security

=

Cities Have Big Business Challenges

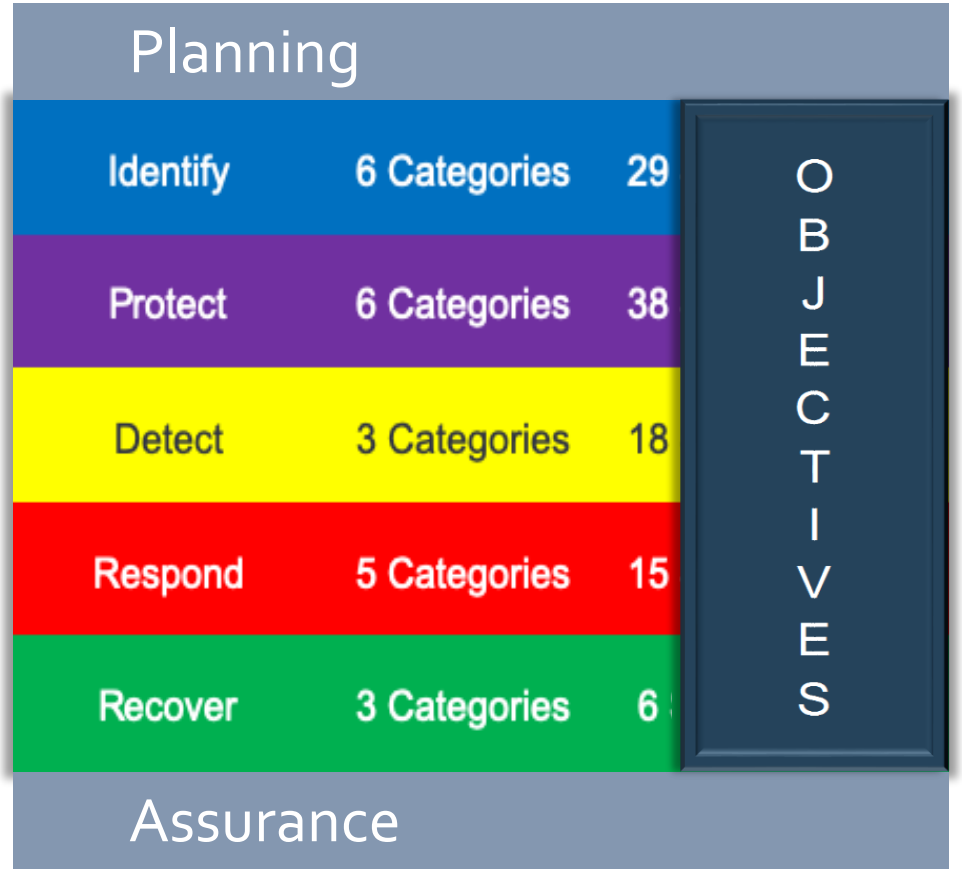
- Shared need to increase security capabilities faster
- Cities require even more value and efficiency

GET THE FULL PICTURE

LEVERAGE FRAMEWORKS THAT DEFINE A COMPREHENSIVE PROGRAM

NIST Cybersecurity Framework → Defines **Objectives**

NIST 800-53, ISO27001, COBIT, etc. → Defines **Controls**



SECURITY PROGRAM STRATEGIC PLAN

Goals		Objectives	Activities
PL	Plan	Objective A	Activity A
		Objective B	Activity B
		Objective C	Activity C
ID	Identify	Objective D	Activity D
		Objective E	Activity E
		Objective F	Activity F
PR	Protect	Objective G	Activity G
		Objective H	Activity H
		Objective I	Activity I
DE	Detect	Objective J	Activity J
		Objective K	Activity K
		Objective L	Activity L
RE	Respond	Objective M	Activity M
		Objective N	Activity N
		Objective O	Activity O
RC	Recover	Objective P	Activity P
		Objective Q	Activity Q
		Objective R	Activity R
AS	Assure	Objective S	Activity S
		Objective T	Activity T
		Objective U	Activity U

Maturity Level	Short Definition
5 – Optimized	Efficient, Optimized, Economized
4 – Advanced	Risk-Based, Measured
3 – Strong	Managed, Consistent
2 – Moderate	Compliant, Defined, Repeatable,
1 – Basic	Ad-hoc, Initial
0 – Minimal	None, Non-Existent

Goals Defined by Framework Objectives

Activities that Develop Capabilities

Capabilities That Work to Reduce Risks

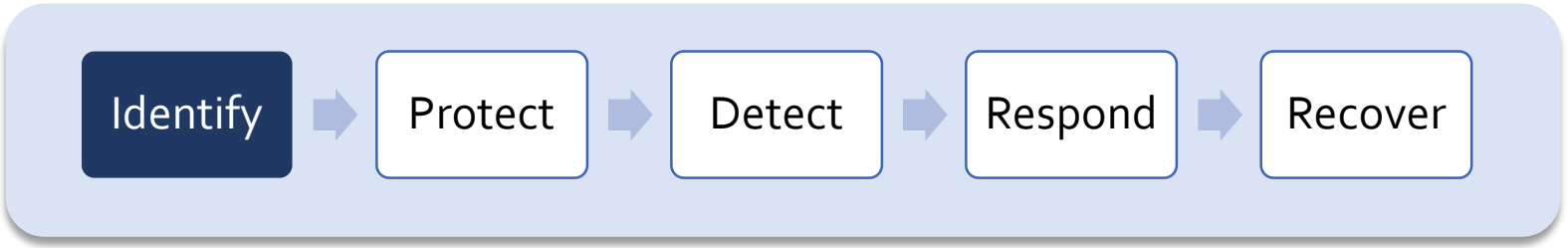
People that Actuate ***Process*** Supported by ***Technology***

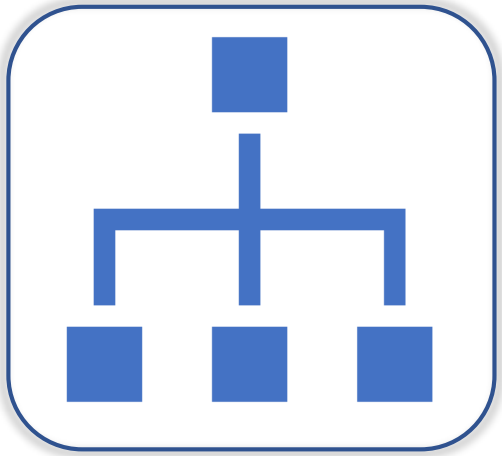
Capability Maturity Evolved Over Time

CYBERSECURITY READINESS

Cybersecurity Operations that enable ongoing protection against attacks, detection of attempts and incidents, response to attacks, and recovery once incidents are mitigated.

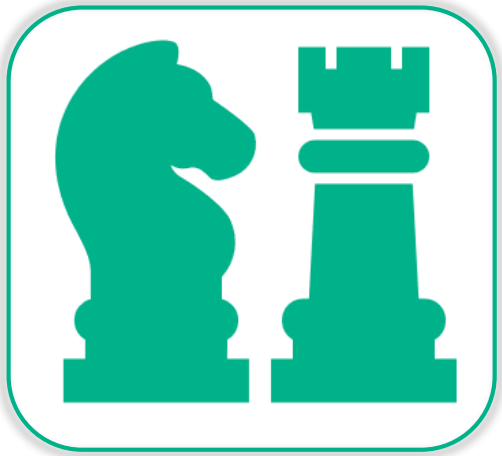
READINESS





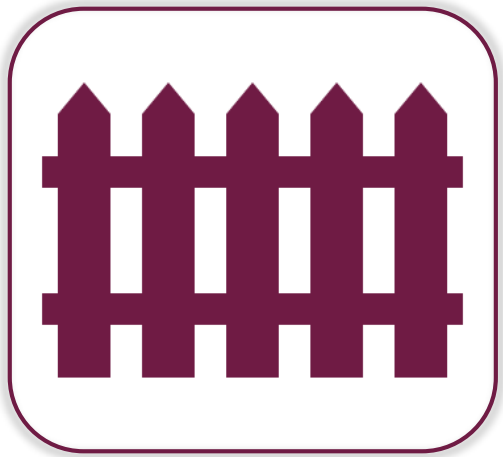
IDENTIFY THE ASSETS

Plotting the Battlefield



IDENTIFY THE THREATS

Understanding What to Defend Against

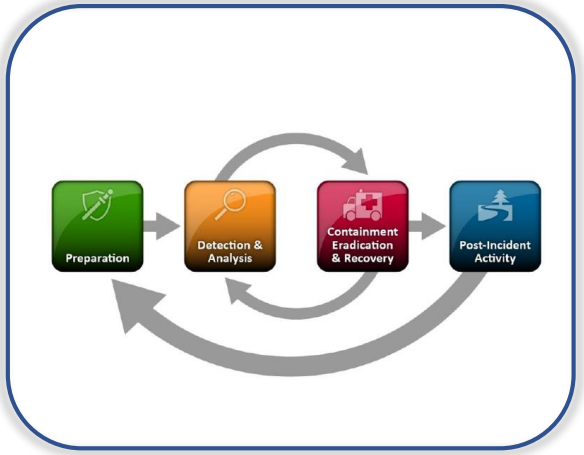


IDENTIFY THE PROTECTIONS

Understanding the Gaps, Vulnerabilities and Blind Spots

READINESS – CONTINUOUS MONITORING

Identify → Protect → Detect → Respond → Recover

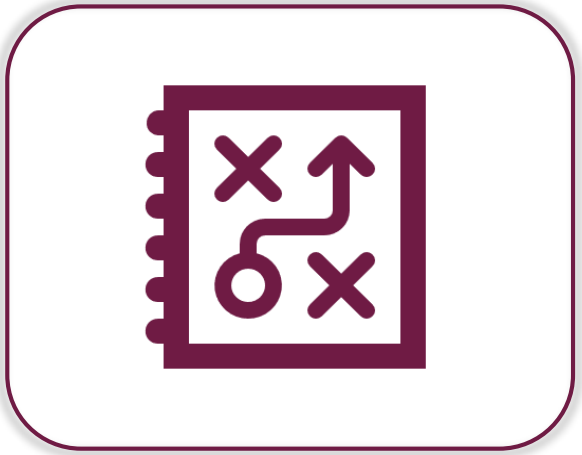


PLAN AND PREPARE

Anticipating that Protections will Break Down

COMMUNICATION

Notifications, Escalations, and Keeping Stakeholders Informed



BATTLE TESTED

Exercises and Drills Develop Military-Grade Cybersecurity

TABLE-TOP EXERCISES AND CYBERSECURITY DRILLS

SCENARIO OBJECTIVES

General Preparedness

Specific Threats (*RANSOMWARE*)

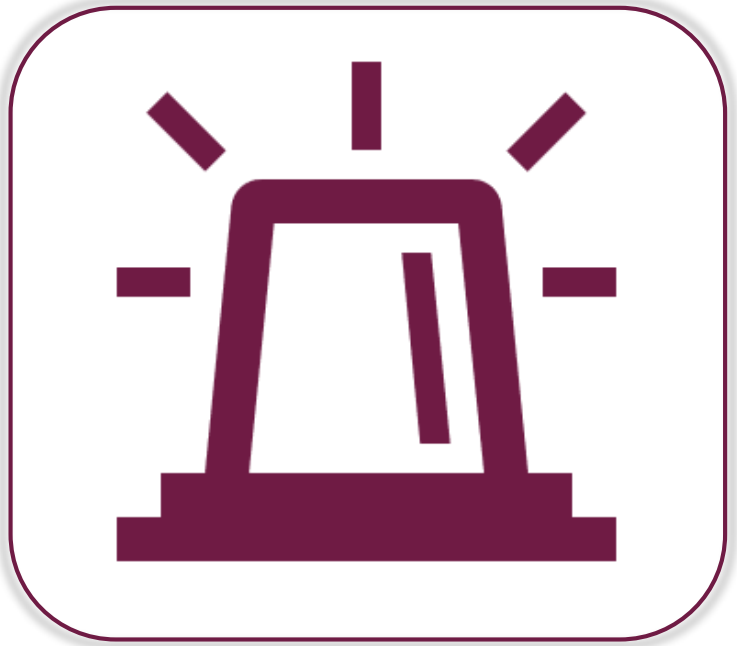
Third Party Risk

Communications – Public Disclosure

Insider Threat

Critical Personnel Dependencies

Executive Communications and Escalations



TRAINING PERSONNEL

Invest Time In Training

Have a Training Plan for All Levels of Employees

- User Awareness Training
- Leadership and Executive Risk Management Training
- IT and Security Staff Technical Training

Drill Like It's the Real Thing

Use Real-world Events to Create Scenarios

Build Hunting Into Exercises

MANAGED RISKS

Prioritized progress towards maturity and capability goals aimed at reducing risks, illuminating gaps, and clarifying uncertainty.

DEFINING RISK

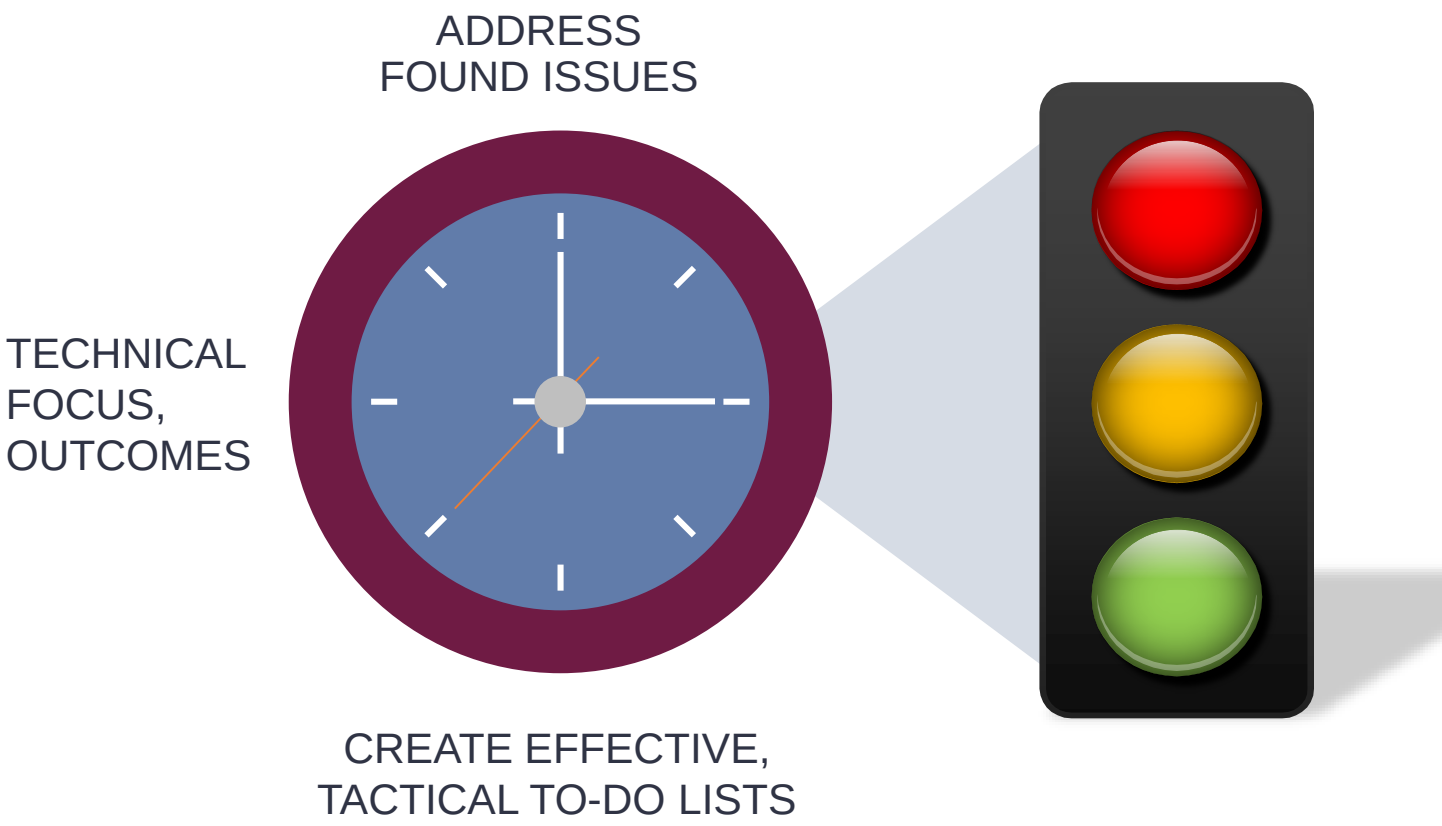
Threat of damage, injury, liability, loss, or other negative occurrence

- Caused by external or internal vulnerabilities
- May be neutralized through preemptive action

In Finance: The probability that an actual return on an investment will be lower than the expected return

SO MANY ASSESSMENTS
SO LITTLE TIME

- Vulnerability Scans
- Penetration Tests
- Framework Gap Analysis
- Compliance Audits
- Third-party Reviews
- Application Threat Modeling
- Risk Assessment
- And Many More…



FACTORS OF RISK

PROBABILITY	Likelihood of Occurrence
FREQUENCY	Rate of Occurrence
THREAT	Threat Agent, Threat Actor, Motivation, Capability
VULNERABILITY	Exposure, Weakness
IMPACT	Damage, Injury, Liability, Loss
ASSET	Item, Valuables
PREEMPTIVE ACTIONS	Protections and Capabilities

DEEP DIVE INTO RISK FACTORS

IMPACT

Asset Value

- Incident Frequency
- Loss Magnitude
- Financial Value
- Confidentiality/Disclosure
- Integrity

Service Dependencies

- Availability Requirements

PROBABILITY

- Threat
- Vulnerability
- Attacker Motivation
- Attacker Capability
- Preemptive Actions

DEFINING RISKS FOR **YOUR** BUSINESS

AVAILABILITY	Disruption in 'Key Business' Service
CONFIDENTIALITY	Disclosure of 'Stakeholder' Information
INTEGRITY	Modification or Deletion of 'Key Business' Data
LIABILITY	Lawsuit for Breach of Contract or Harm Caused
PRIVACY	Disclosure or *Breach* of Privacy Protected Data
REGULATORY	Failure to Meet Compliance Mandates
REPUTATION	Public Scrutiny and 'Stakeholder' Distrust
INDIRECT	Issues that Require Cascading Events

ADDING BUSINESS RISK INTO ASSESSMENT OUTPUTS

Business System	Risk	Probability	Impact	Risk Severity
Patient Record System	Disclosure of Patient Records	Possible (62%)	Moderate (62%)	Moderate (41%)
	Disruption of Patient Processing	Probable (80%)	Material (80%)	High (64%)
	HIPAA Violation	Possible (62%)	Material (80%)	Moderate (51%)
	Privacy Breach	Almost Certain (100%)	Material (80%)	High (80%)

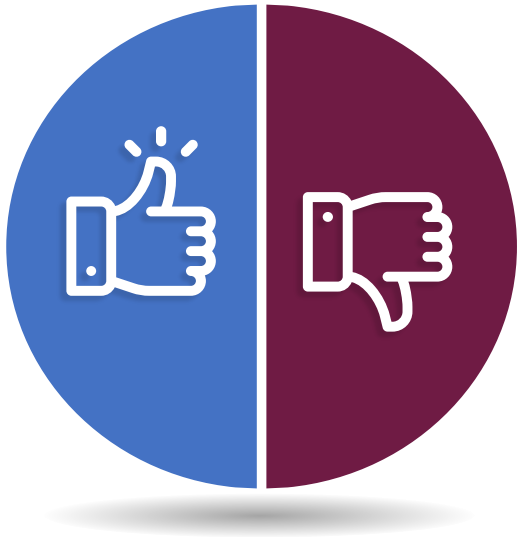
PRO'S

Lightweight, quick and easy to start estimating and quantifying

Provides a better degree of prioritization

Enables 'Apples-to-Apples' comparisons from varieties of assessment inputs

Helps distinguish threat scenarios



CON'S

Lacks granularity (factors) to fully evaluate risks

Only slight improvement over stoplight estimations

Doesn't work well for frequently changing conditions

BONUS CONTENT – BEYOND THE BASICS OF RISK
TAKING RISK FACTORS TO THE NEXT LEVEL OF MEASUREMENT

Business System	Risk	Probability			Impact			Risk Severity
Patient Record System	Disclosure of Patient Records	Possible (38%)			Extreme (100%)			Moderate (38%)
		Threat Capability	Threat Motivation	Vulnerability	Asset Value	Frequency	Loss Magnitude	
		100%	75%	50%	5	35%	100%	
	Privacy Breach	Probable (75%)			Incidental (3%)			Insignificant (2%)
		Threat Capability	Threat Motivation	Vulnerability	Asset Value	Frequency	Loss Magnitude	
		100%	100%	75%	5	35%	5%	

NOTATIONS

- Should be expanded across various threat sources
- Can be used to run modelling
- Finally, place in issue tracking system/risk register

THREAT SOURCES

- Insider Threat
- Privileged Insiders
- Nation-state attackers
- Organized Crime
- Hacktivists
- Novice Attackers

CAPABILITY REDUCES RISK

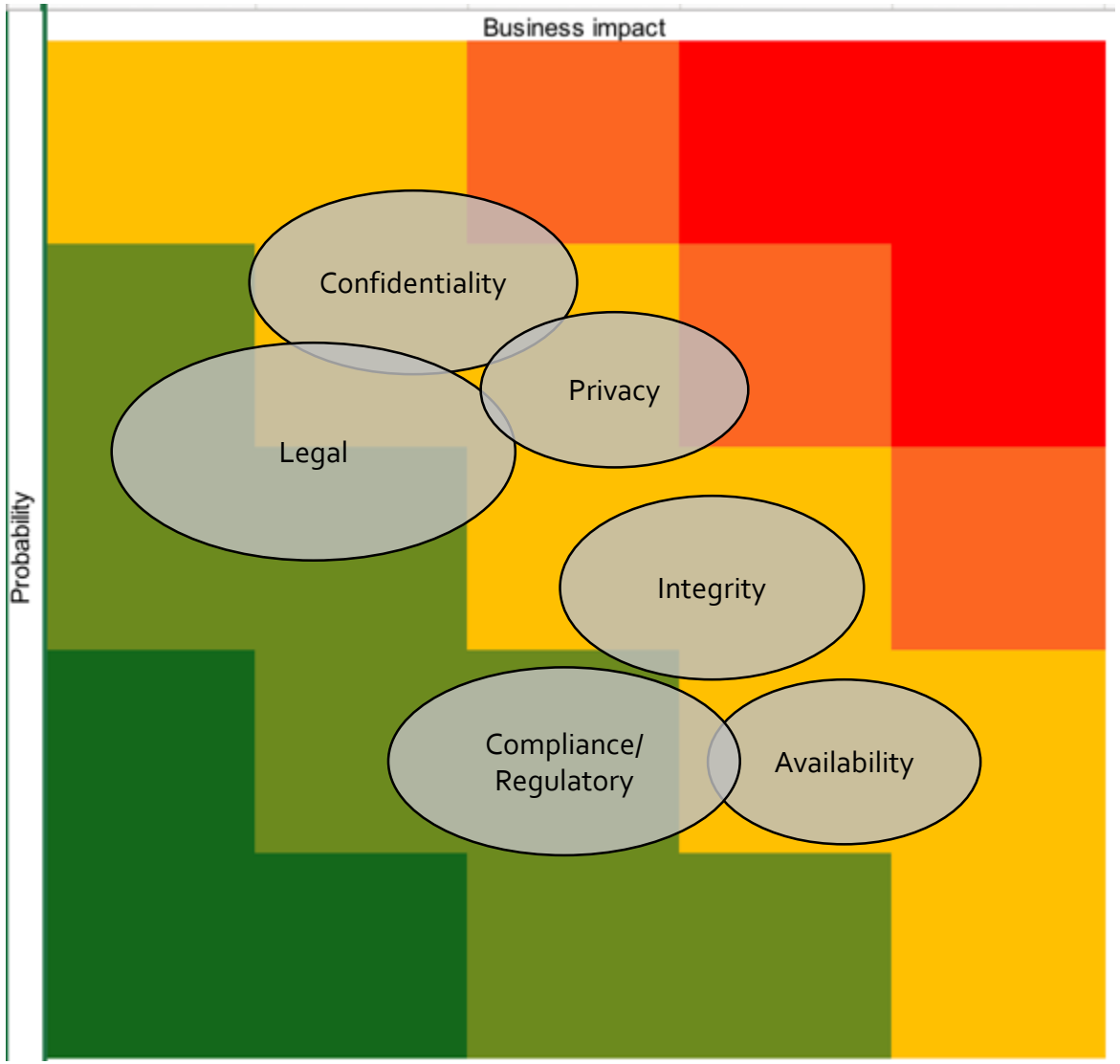
Issues Addressed

Protections Matured

Detection Established

Response Continuously Improved

Recovery Enabled



CAPABILITY REDUCES RISK

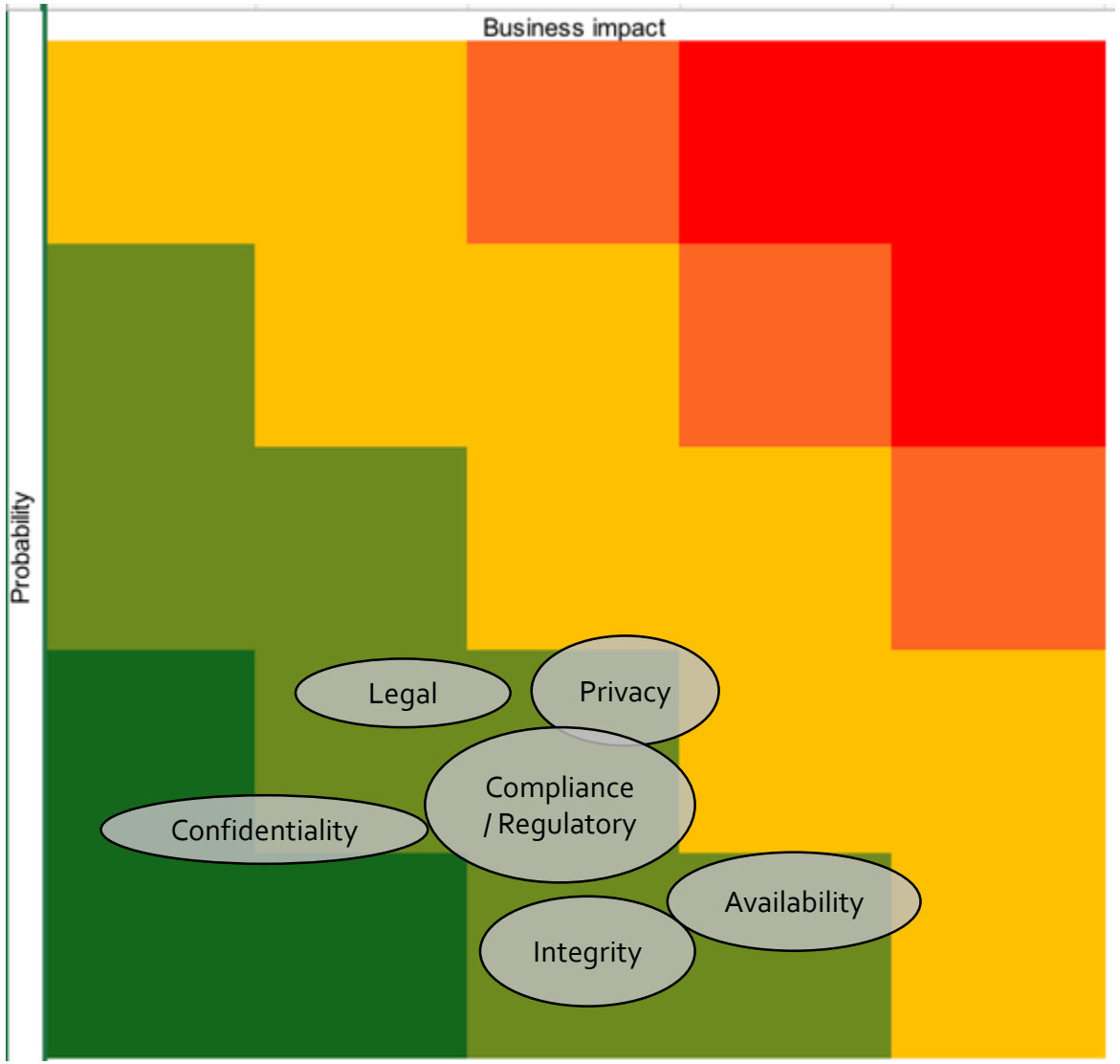
Issues Addressed

Protections Matured

Detection Established

Response Continuously Improved

Recovery Enabled



Unshakeable Security

STRATEGIC PLAN

Chart the Course, Define the Initiatives and Execute

CYBERSECURITY READINESS

Continuous Monitoring, Detection, Response and Recovery

MANAGED RISK

Identify Threats, Evaluate Risks and Adjust the Course

#ICMA2019

Unshakeable Security

#ICMA2019

THANK YOU

Questions?

ICMA | conference