A Masterclass In
Security And Quality Requirements Engineering

A Masterclass In Security And Quality Requirements Engineering

Presented by
Mark Cross from Envista Consulting
18th August 2024

ABOUT THE SPEAKER

MARK CROSS
PRINCIPAL CONSULTANT
ENVISTA CONSULTING

Mark Cross has been working in IT transformation for twenty-five years. He spent ten years as a network engineer in leading telcos before switching to a career in business analysis. As a business analyst, his areas of specialism include cloud transformation, data migration, information protection and cybersecurity. He has a passion for helping organisations to reduce their security debt and their exposure to cyber-risk.

He holds an MBA from Alliance Manchester Business School, the International Diploma in Business Analysis and Chartered IT Professional status from the British Computer Society. He also holds the Certified Business Analysis Professional (CBAP) and Certified Cybersecurity Analyst (CCA) credentials from the International Institute of Business Analysis and the Certified Information Systems Security Professional (CISSP) credential from ISC2.

He is the founder and principal consultant of Envista Consulting, the regional lead for Yorkshire Cybersecurity Cluster in North Yorkshire and serves on the committee of the IIBA UK North Branch.

A CYBERSECURITY JOURNEY IN FOUR PARTS

Business Analysis Circa 2000
Focused on Utility, Interoperability and Quality

Business Analysis Circa 2010
Focused on Agility, Efficiency and Speed to Market

Business Analysis Circa 2020
Focused on Scalability, Mobility and User Experience

Business Analysis Circa 2030
Focused on Security, Resilience and Intelligence.

Find out more at https://envistaconsulting.com

AGENDA FOR TODAY

9:30 AM: First Part Begins

- Current Threats
- What Is Quality in Security?
- The Delivery Lifecycle
- What can go wrong, and what we can do about it?

11:00 AM: Morning Break

11:30 AM: Second Part Begins

- The SQUARE Method
- Common Definitions
- Cyber-Risk Assessments
- Prioritisation 2.0

13:00 PM: Lunch

Part 1

UNDERSTANDING THE THREAT

WHY IS EVERYTHING “CYBER” NOW?

Is this just another buzzword?

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE PRE-DIGITAL ERA

TRADITIONAL INVENTORY

TRADITIONAL INFORMATION STORAGE

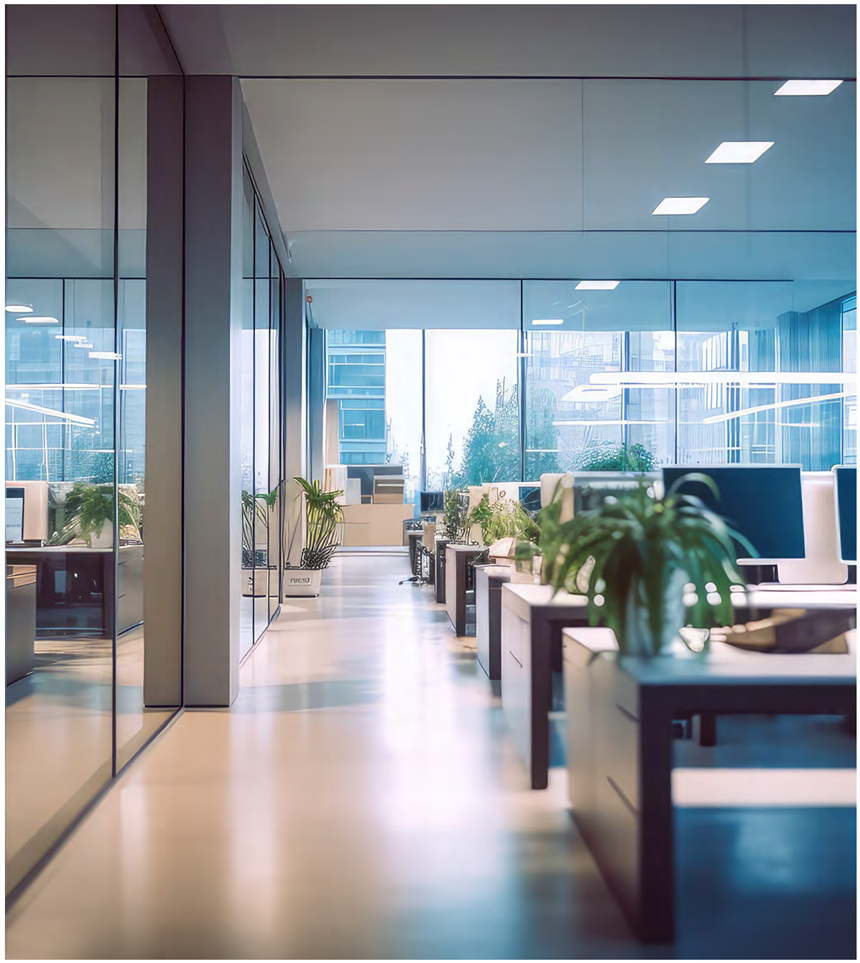
TRADITIONAL BUSINESS

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE DIGITAL ERA

RECENT INVENTORY

RECENT INFORMATION STORAGE



RECENT BUSINESS

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE CYBER ERA

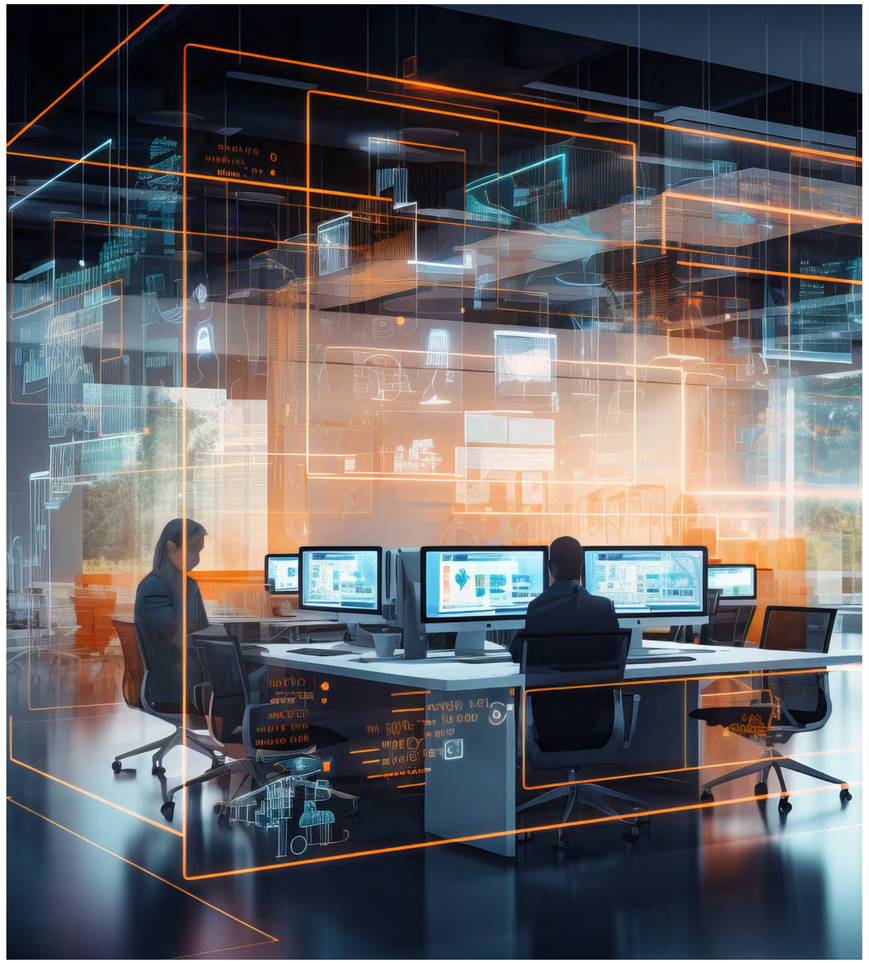
MODERN INVENTORY

MODERN INFORMATION STORAGE

MODERN BUSINESS

THE IMPORTANCE OF CYBER-RESILIENCE

Cash, Clouds and a $125 Billion Dollar Catastrophe



Sources:

https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud

https://cloud.google.com/blog/products/infrastructure/details-of-google-cloud-gcve-incident

SOLARWINDS

How Bad Can Twelve Lines Of Code Possibly Be?

Sources:

https://www.solarwinds.com/sa-overview/securityadvisory/faq

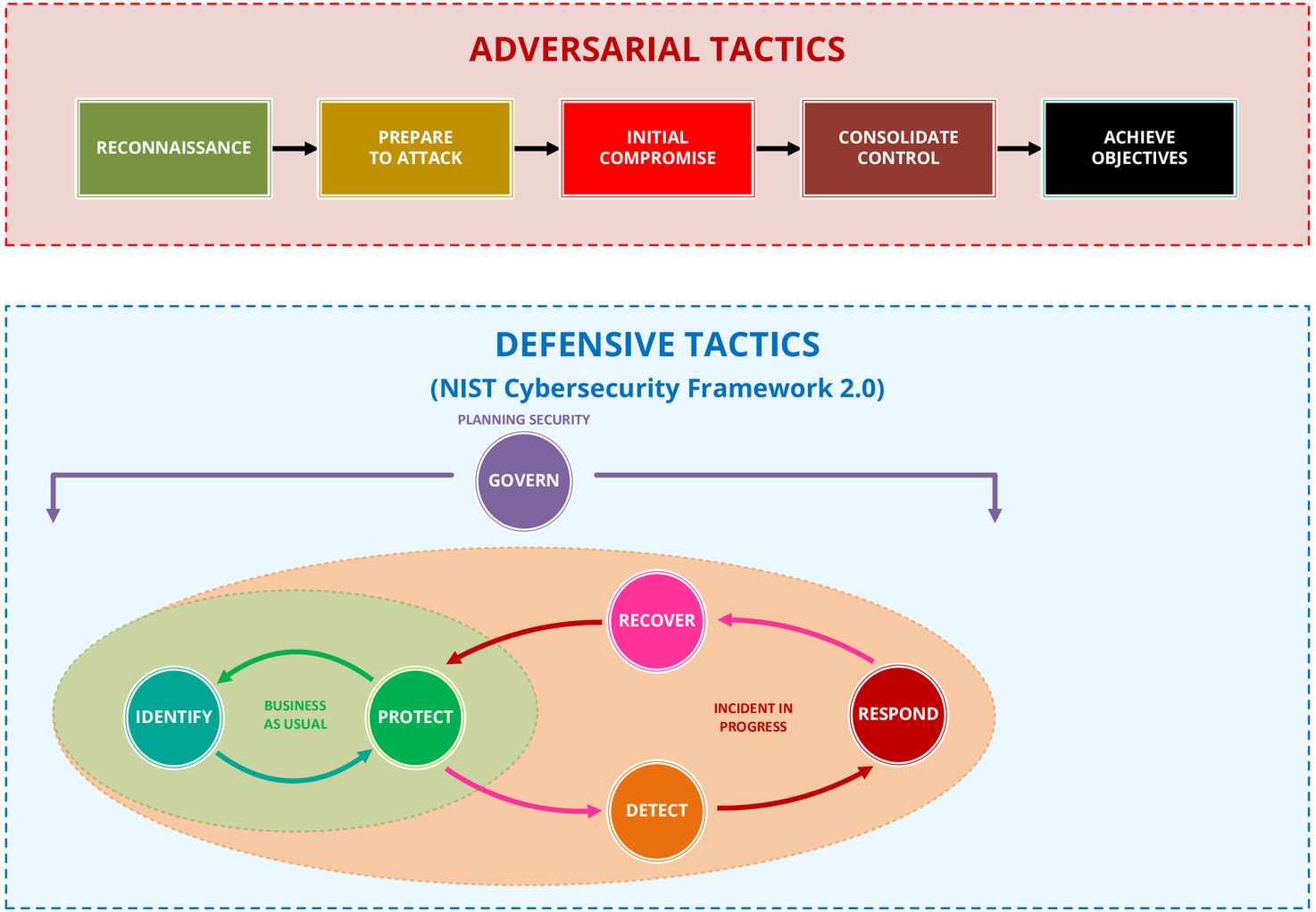
https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds

MEET YOUR OPPONENTS…

Motivated By An Ideology

Motivated By Financial Reward

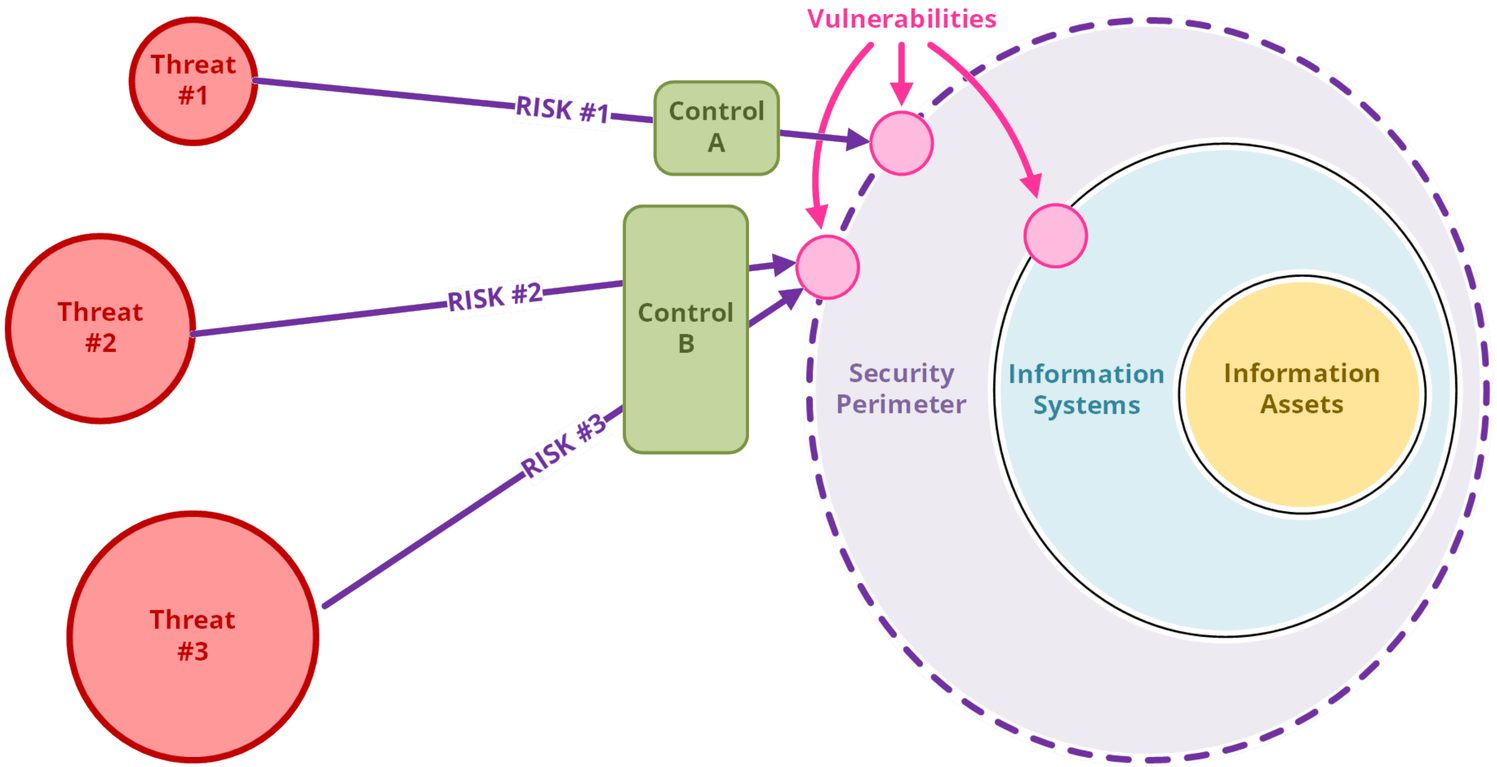
HOW AN ATTACK HAPPENS...



Source: https://www.nist.gov/cyberframework

ABOUT RISKS, VULNERABILITIES AND CONTROLS

TBC...



THE BUSINESS CASE OF CYBERCRIME

TBC...

It's simple math!

Cost to develop ransomware
- 160 hours at $200/hour

Cost of disposable infrastructure
- 10 servers at $500 ($50/server)

Cost of launching ransomware attack
- Push "button" to start
- Monitor for 10 days (240 hours at $150/hour)

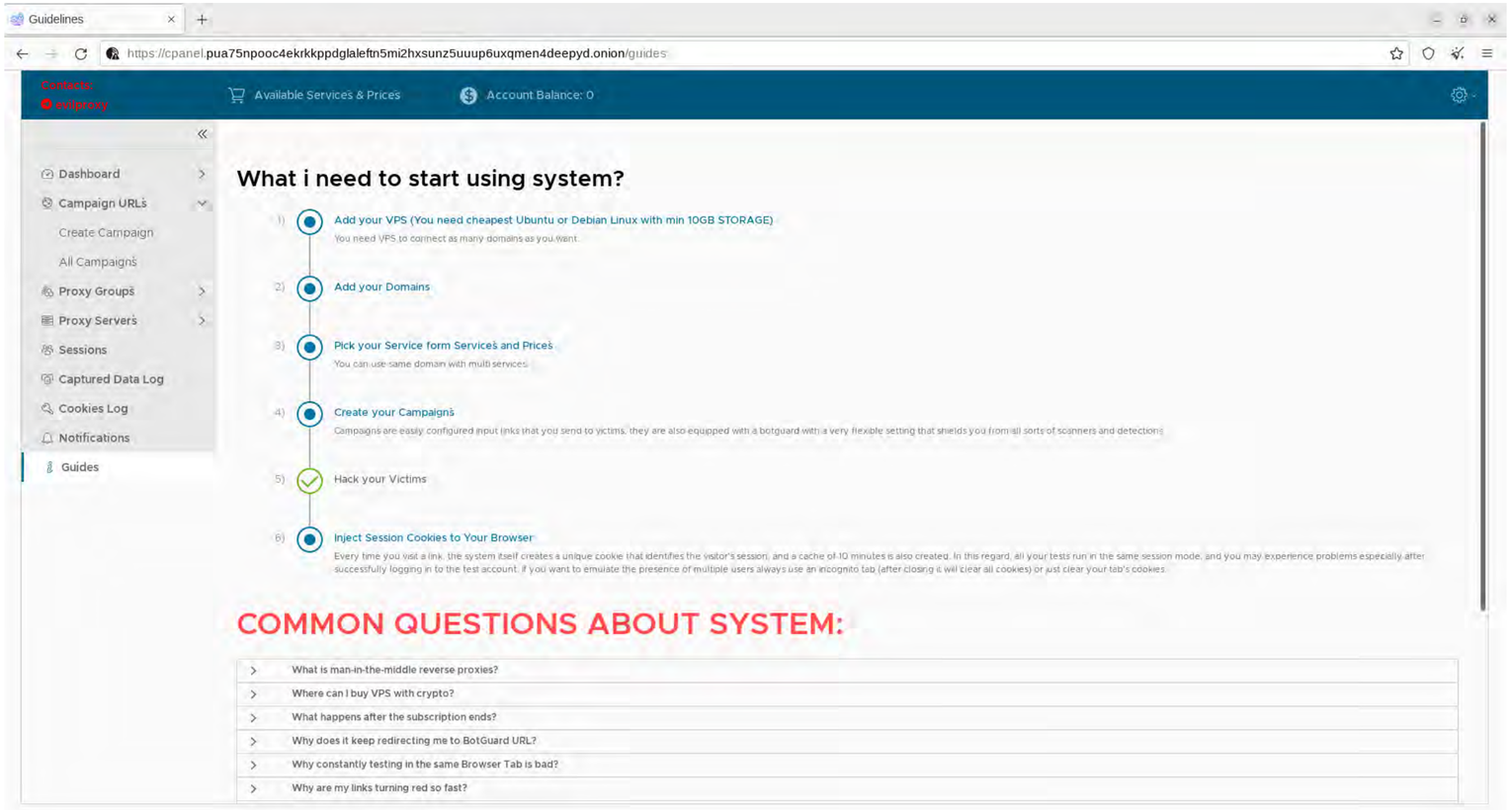
Attack 1,000,000 targets
- 1% pay the ransom at $300/system

	Cost
Developer	$32,000
Infrastructure	$500
Launch attack	$50
Help desk	$36,000
Investments	$68,550
1% target market share	$3,000,000
Return on investment	**$2,931,450**

Source: https://www.isaca.org/resources/white-papers/blueprint-for-ransomware-defense

THE RISE OF CYBERCRIME as a SERVICE

TBC...



THE UK RESPONSE TO THIS THREAT...

In July 2024, the incoming UK government announced a new Cyber Security and Resilience Bill

The Bill updates the existing regulatory framework by expanding the regulations to protect more digital services and supply chains. This may also include new powers to proactively investigate potential vulnerabilities, mandatory incident reporting and cost recovery mechanisms (fines).

These steps are intended to give the government better data on cyber attacks, including where a company has been held to ransom - improving our understanding of the threats and alert us to potential attacks.

Sources:

https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf

https://www.ncsc.gov.uk/blog-post/legislation-help-counter-cyber-threat-cni

Part 2

WHAT IS QUALITY IN SECURITY TERMS?

THE BASICS OF THE CIA TRIAD

The simplest and most fundamental properties of security are defined by a model called the “CIA Triad”.

The letters “CIA” stand for:

- Confidentiality
- Integrity
- Availability

When people think of information security, the most common one that they think about is confidentiality. Although a loss of any of these qualities would devalue of an information asset and may expose the organisation to undesirable consequences.

TBC

What Is CONFIDENTIALITY?

Confidentiality is the quality of knowing that your data cannot be and has not been read by anyone other than authorised users for legitimate reasons.

Examples of failures of confidentiality include:

- Documentation being placed in a file share an exposed to people who do not have authorisation to view it, or
- Changing permissions of a file share that already contains sensitive information in a way that allows unauthorised people to view it.
- A member of staff looking up the records of a specific individual without having a business justification to do so.
- Someone looking at sensitive information on an exposed computer screen or printed document.
- Disposing of sensitive information without it being destroyed securely.

What Is INTEGRITY?

Integrity is the quality of your data remaining intact and unmodified after creation unless it is intentionally changed.

Failures of integrity can include issues such as:

- Data on magnetic storage devices can become corrupted due to exposure to electromagnetic interference.
- Optical storage media can be affected by scratches or residue on the media.
- Corruption due to system failures or synchronisation errors.

What is AVAILABILITY

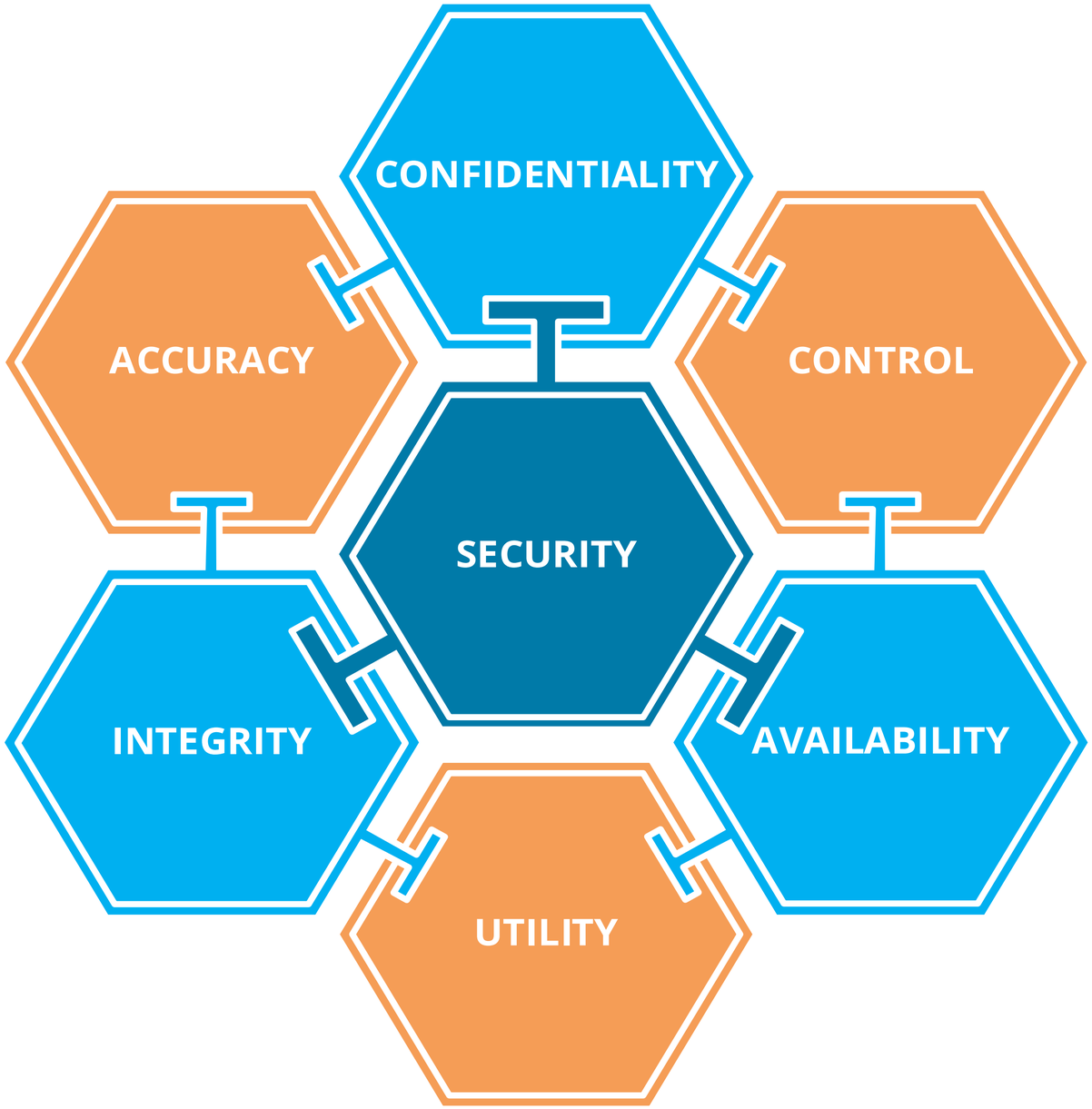
Availability is the quality of knowing that your data and services will be accessible and functional when you need them to be.

Common causes of loss of availability include:

- Lack of sufficient network or system processing capacity to respond to queries.
- Changes to network configuration that may prevent data from being exchanged between a client and the server.
- Systems being powered down, damaged or under maintenance.

THE SIX QUALITIES OF GOOD SECURITY

(The Parkerian Hexad)



EXPLORING THE PARKERIAN HEXAD

Three New Qualities Of Security For The Digital World

ACCURACY

Accuracy is the quality of information being correct, or at least ensuring that it comes from a legitimate source. This also includes the capability to provide irrefutable evidence of key events such as the exchange of legal contracts or an audit trail surrounding critical decisions.

UTILITY

Utility is the quality of an information system demonstrating the behaviour that is expected of it. The most well-known example of a failure of utility is the classic (encrypytion-only) ransomware attack. All systems are contactable and recoverable, however they are unable to be used for their intended purpose.

CONTROL

Control (also known as possession) is the quality of having the ability to exclusively manage access to or the behaviour of an information system without being subject to another party.

Note: Theft of the system itself is also considered to be a loss of control.

EXERCISE ONE:

UNDERSTANDING THE QUALITIES OF GOOD SECURITY

TBC...

Part 3

THE DELIVERY LIFECYCLE

CREATING CHANGES IN YOUR ORGANISATION

A SIMPLIFIED DELIVERY LIFECYCLE

ANALYSIS AND PLANNING

DESIGN AND BUILD

TESTING AND RELEASE

IN SERVICE

CREATING CHANGES IN YOUR ORGANISATION

THE POINT AT WHICH YOU START THINKING ABOUT SECURITY MATTERS

ANALYSIS AND PLANNING

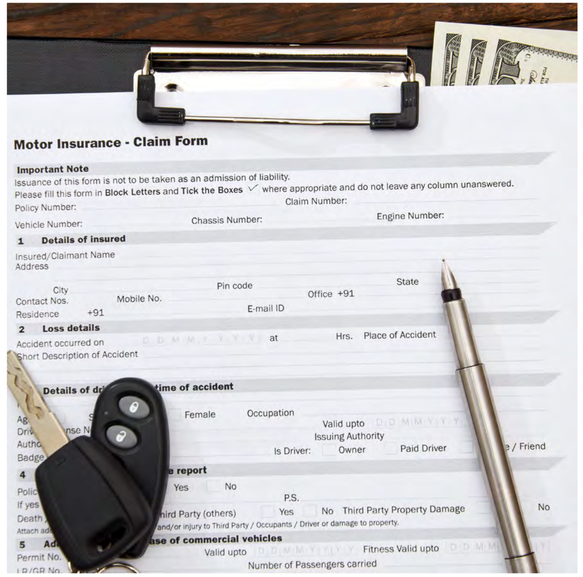
Projects that adopt a “Secure-by-Design” philosophy deliver products that are both secure and functional at little or no extra cost. This is the ideal scenario.

DESIGN AND BUILD

There is still early enough to deliver a secure, working product however it may require adding additional features to secure what has already been built. This can lead to cost overruns and delays.

TESTING AND RELEASE

It is now too late to make major changes to the product without impacting the delivery dates and budget. Fixing any new security issues will likely require a trade-off between limiting unsafe functionality or accepting the risk.

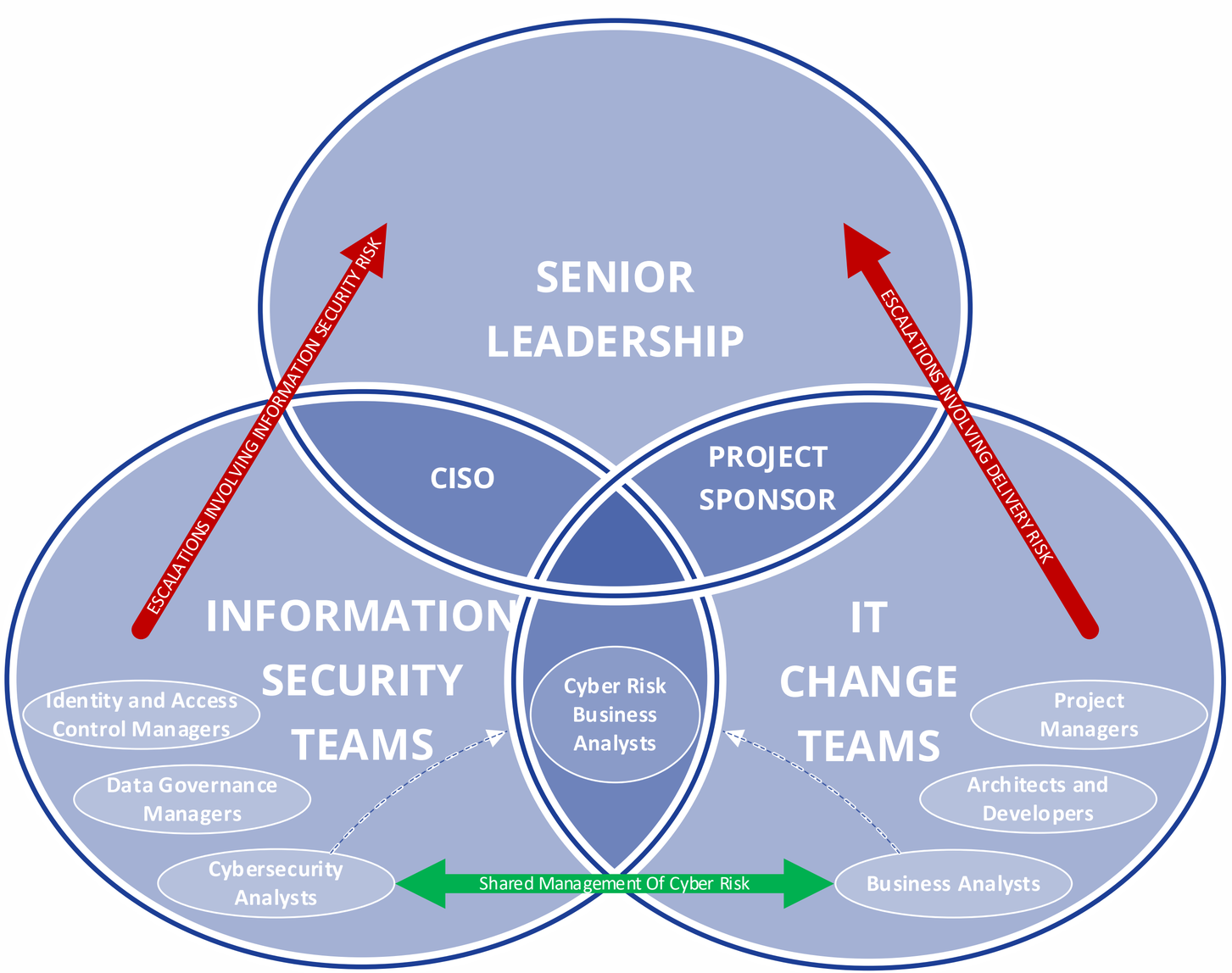


IN SERVICE

Once in service, the risk is immediate and costly to remediate. Security incidents evolve rapidly and if not contained within the first few minutes, they can lead to significant losses.

THE DELIVERY LIFECYCLE

(Simplified)



Find out more at https://envistaconsulting.com

THE SEVEN OPTICS OF CYBERSECURITY

TBC...

Part 4

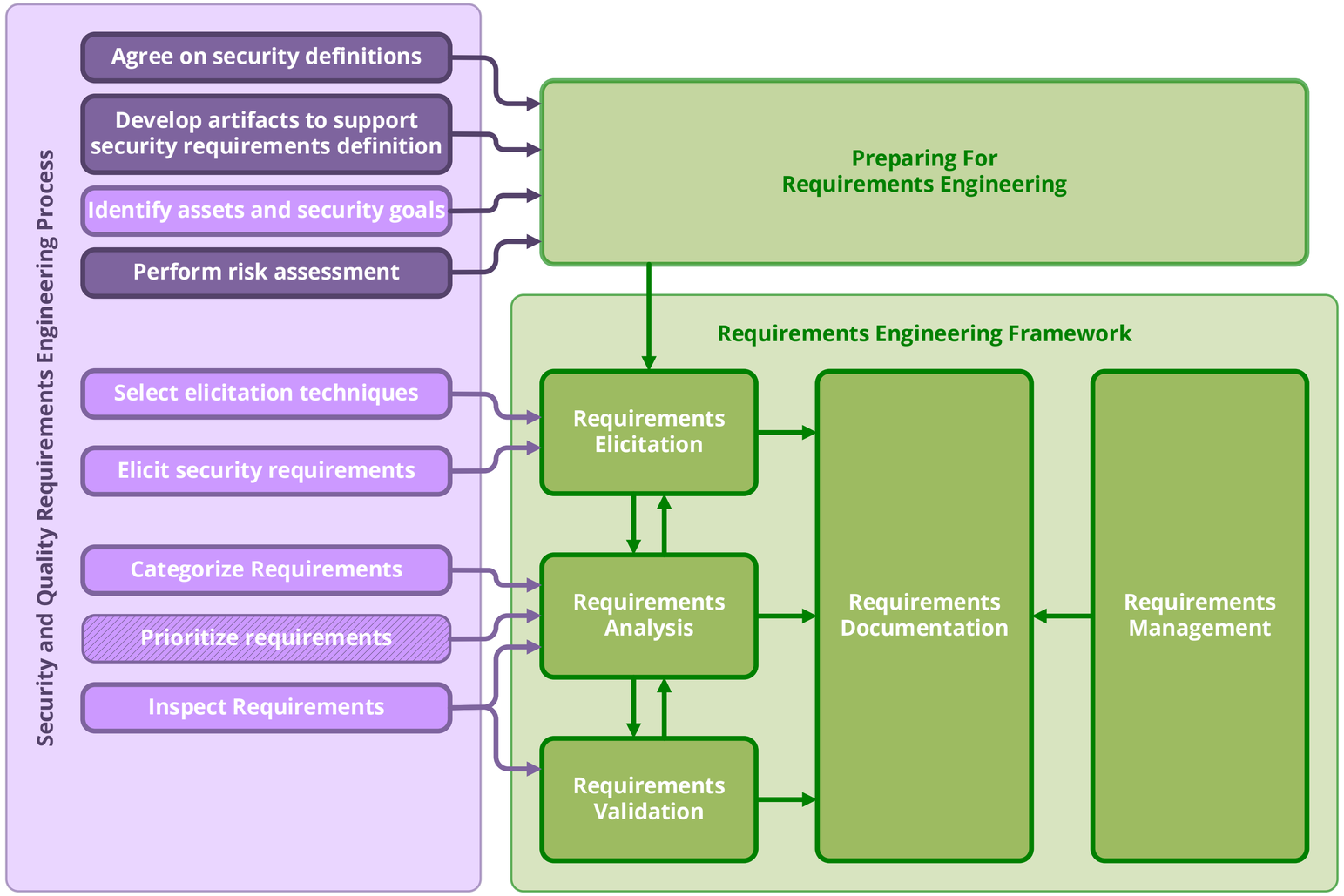
INTRODUCTION TO SQUARE

What is SQUARE?

STEP 1	AGREE ON DEFINITIONS
STEP 2	IDENTIFY ASSETS AND SECURITY GOALS
STEP 3	DEVELOP ARTIFACTS TO SUPPORT SECURITY REQUIREMENTS DEFINITION
STEP 4	PERFORM RISK ASSESSMENT
STEP 5	SELECT ELICITATION TECHNIQUES
STEP 6	ELICIT SECURITY REQUIREMENTS
STEP 7	CATEGORIZE REQUIREMENTS
STEP 8	PRIORITIZE REQUIREMENTS
STEP 9	REQUIREMENTS INSPECTION

https://insights.sei.cmu.edu/library/cybersecurity-engineering-research-security-quality-requirements-engineering-square-collection/

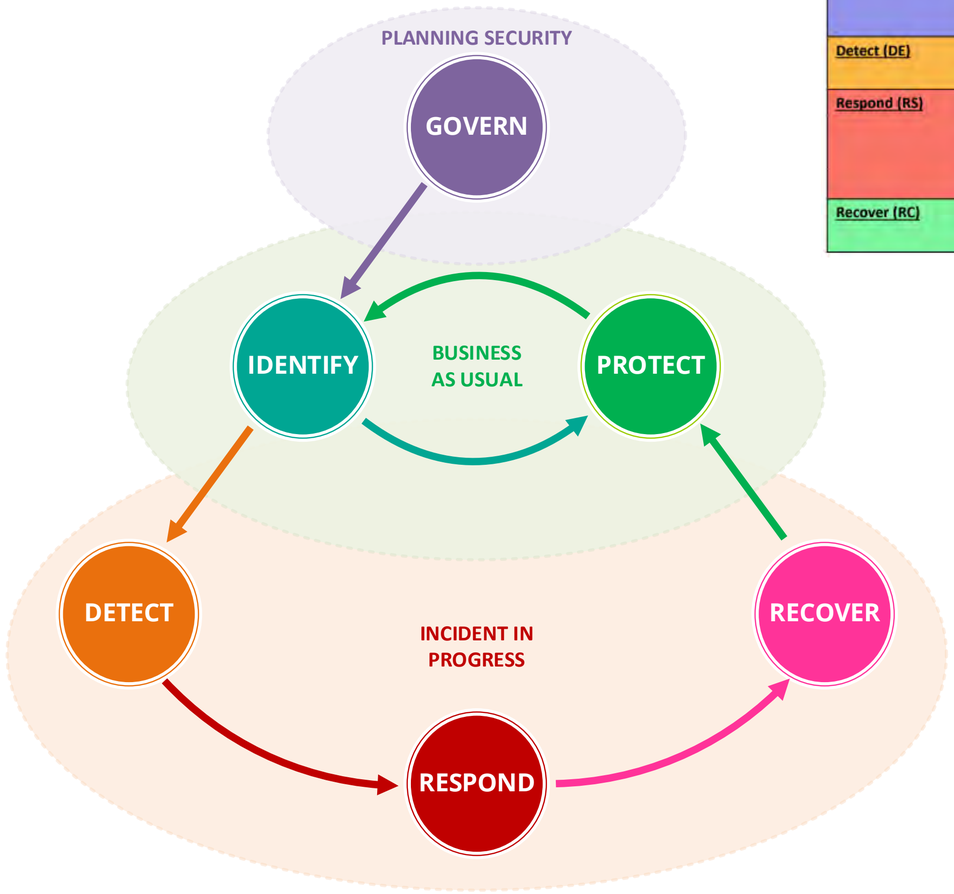
What can go wrong at each stage?



AGREE ON DEFINITIONS

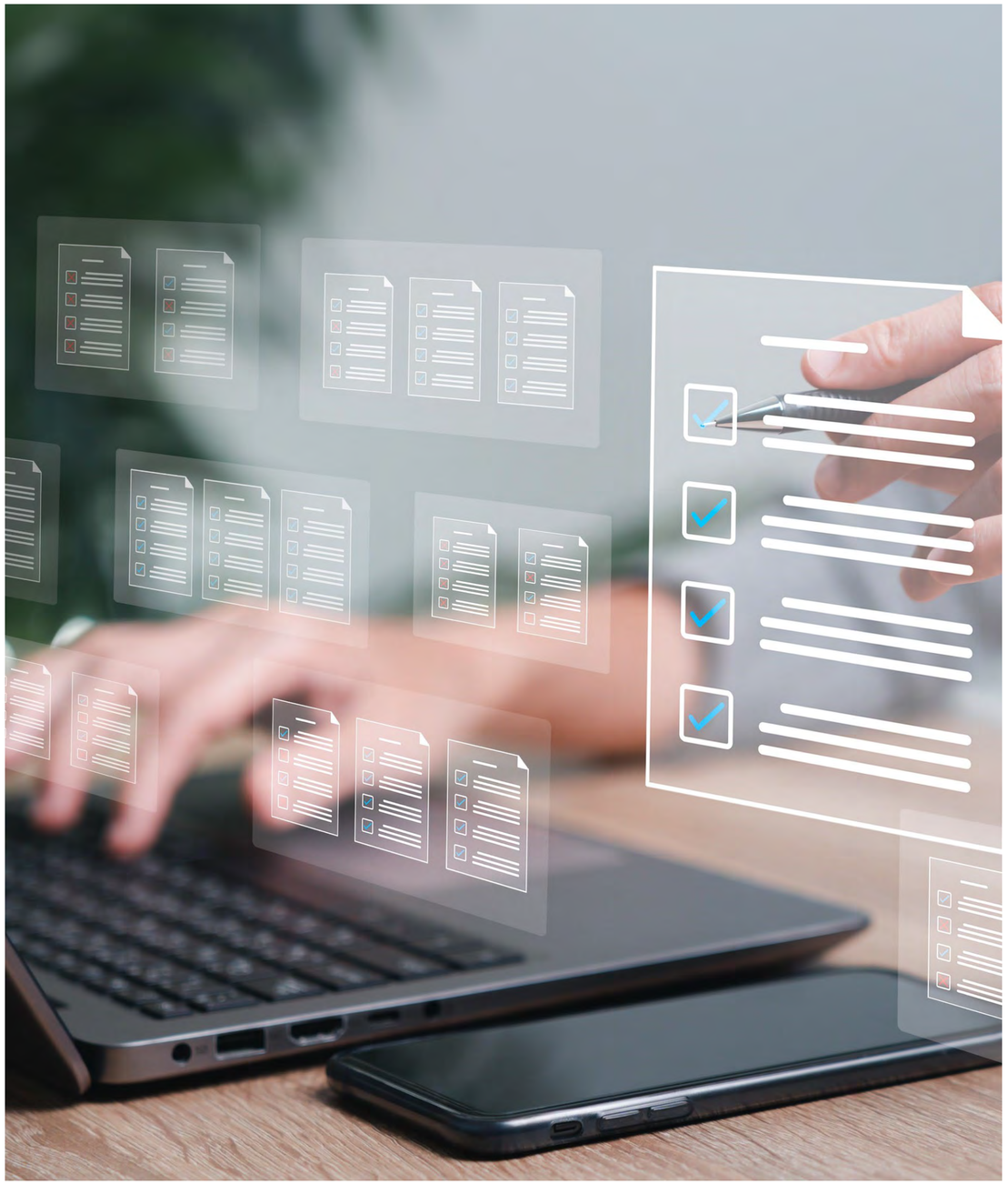
Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

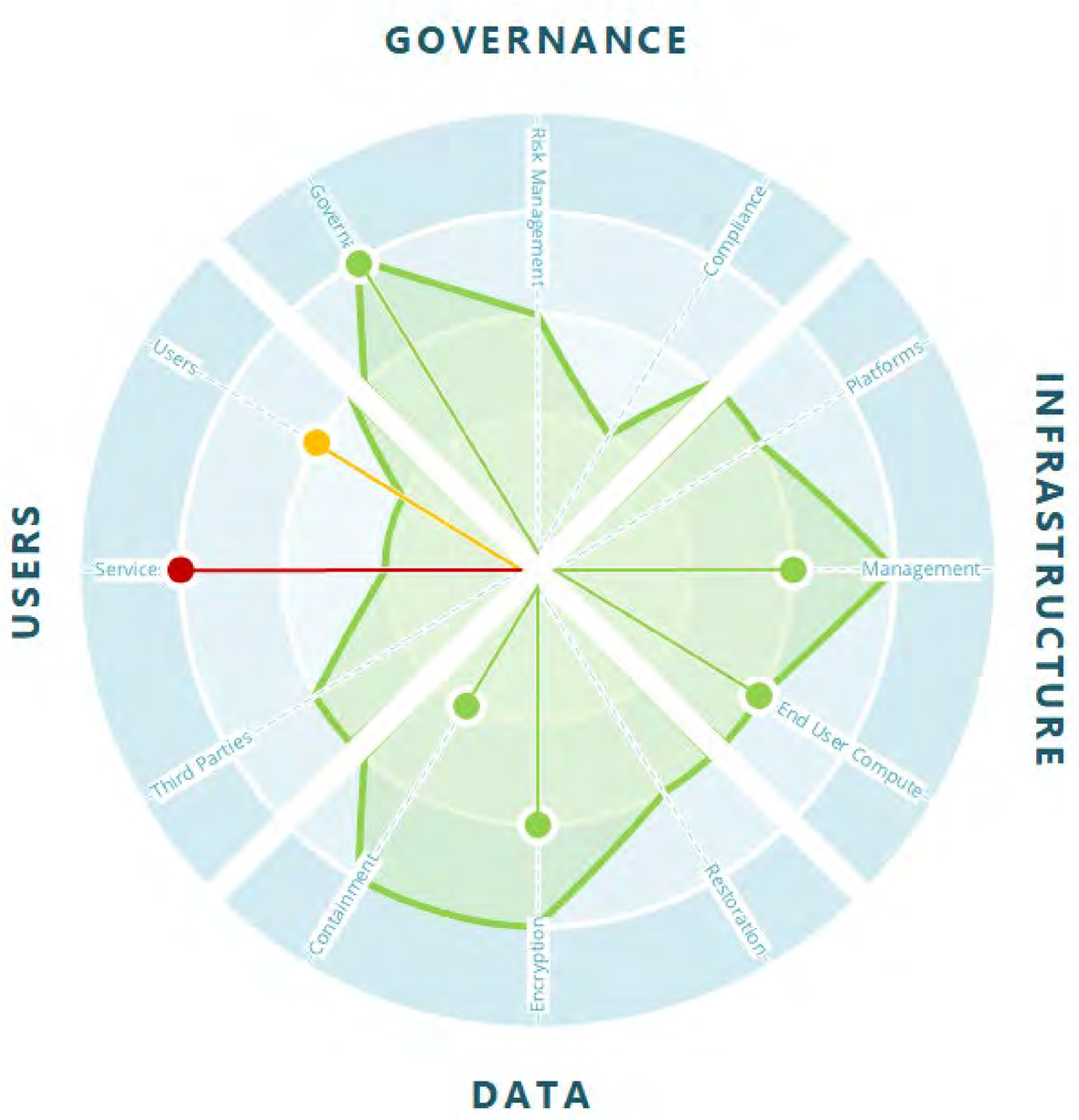


DEVELOP ARTIFACTS TO SUPPORT SECURITY REQUIREMENTS DEFINITION

- Maintain a catalogue of reusable security requirements
- Develop a set of “bad actor” personas to test design assumptions
- Identify appropriate Security SLAs and industry benchmarks



PERFORM RISK ASSESSMENT



Thank Your For Your Participation

Connect with me
on LinkedIn at:
WWW.LINKEDIN.COM/IN/MARKCROSS