Unlocking Cybersecurity:
What Business Analysis Professionals Need to Know

IIBA® International Institute of Business Analysis™

About International Institute of Business Analysis

International Institute of Business Analysis™ (IIBA®) is a professional association dedicated to supporting business analysis professionals to deliver better business outcomes. IIBA connects almost 30,000 Members, over 100 Chapters, and more than 500 training, academic, and corporate partners around the world. As the global voice of the business analysis community, IIBA supports recognition of the profession, networking and community engagement, standards and resource development, and comprehensive certification programs.

For more information visit iiba.org

Connecting the Global Community

30,000+ MEMBERS WORLDWIDE

120+ CHAPTERS GLOBALLY IN 40+ COUNTRIES

300+ CORPORATE MEMBERS

240+ ENDORSED EDUCATION PROVIDERS

26,500+ CERTIFICATIONS ISSUED

AAC CBAP® CBDA CCBA® CCA CPOA ECBA™

IIBA®

Meet Today's Speakers

Bindu comes with 15 years of experience in Business Analysis and is qualified from IIBA and BCS. Recognizing the need for Cybersecurity analysis, Bindu, proactively studied Security Management and since has become a keen advocate to make Cybersecurity inclusive within the mainstream business analysis.

She is part of the Cybersecurity Certification team authoring IIBA's Cybersecurity Certification curriculum and exam. Bindu also has taken this imperative message to several countries and delivering speeches and workshops at various Business Analysis and Cybersecurity conferences.

Bindu Channaveerappa

Meet Today's Speakers

Terry Baresh, CBAP, is a Principal Business Analyst leading teams of BAs in a cybersecurity organization, writing business cases, managing stakeholder expectations, performing enterprise business analysis, and providing support and recommendations to the Chief Information Security Officer and her team of cybersecurity experts.

Terry Baresh

BIG SCARY SLIDE [1]

☹ Cybercrime has increased by 600% since the beginning of the global pandemic.

☹ Ransomware made history in 2020 contributing to the first reported death related to a cyber attack.

☹ If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

☹ As cyber warfare continues to heat up it's clear that training security professionals will become more valuable than building nuclear weapons.

1. https://purplesec.us/recent-cyber-security-attacks/

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

How many passwords do you have?

TYPE YOUR ANSWER IN THE CHAT WINDOWS

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

> Learn about our methodology at hivesystems.io/password

What is your password scheme?

1) 1234567890   **Instantly**

2) mypetsname   **4 minutes**

3) Abc1230&!   **2 days**

4) ABCD1289zxyw   **200 years**

5) Pa$$drow2022   **3,000 years**

6) AppleMousePlant   **3M years**

7) Apple-Yellow-4465   **7 Tn years**

https://businesstech.co.za/news/it-services/572976/how-long-it-takes-hackers-to-crack-your-password-based-on-how-many-characters-it-has/

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

What is Cybersecurity?

TYPE IN YOUR DEFINITION IN THE CHAT

Change in mindset

Change in results

How do you protect your home?

TYPE IN YOUR DEFINITION IN THE CHAT

Is this bike parked ✓

Is it locked ✓

Is it the right lock ✓

Is the bike SECURED?

INFORMATION ANALYSIS

RISK ANALYSIS

LEGAL & REGULATORY

STANDARDS

FRAMEWORKS

GATEWAYS

FIREWALLS

CRYPTOLOGY

AUTHENTICATION

MANDATORY ELEMENTS

ACCESS

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST
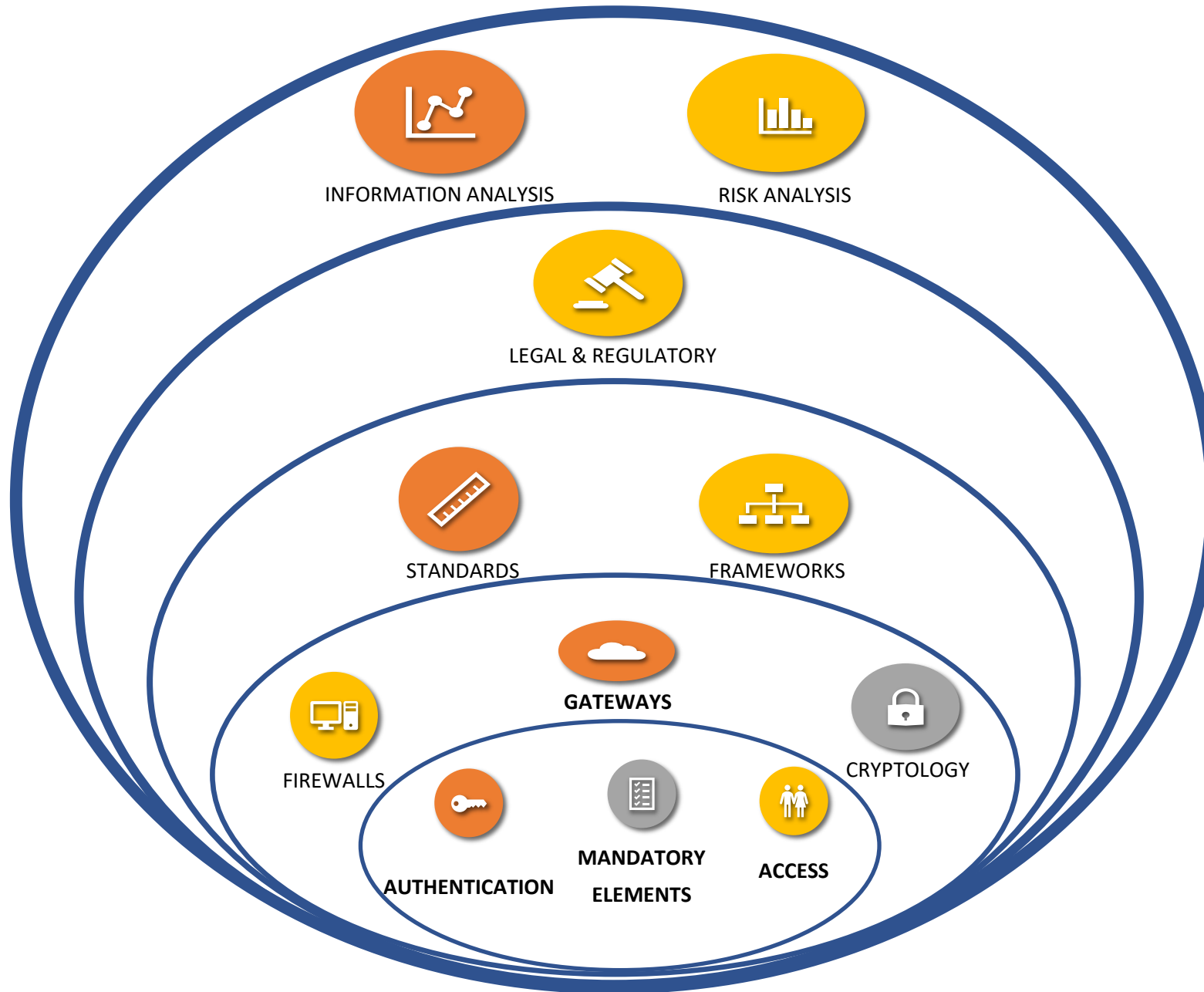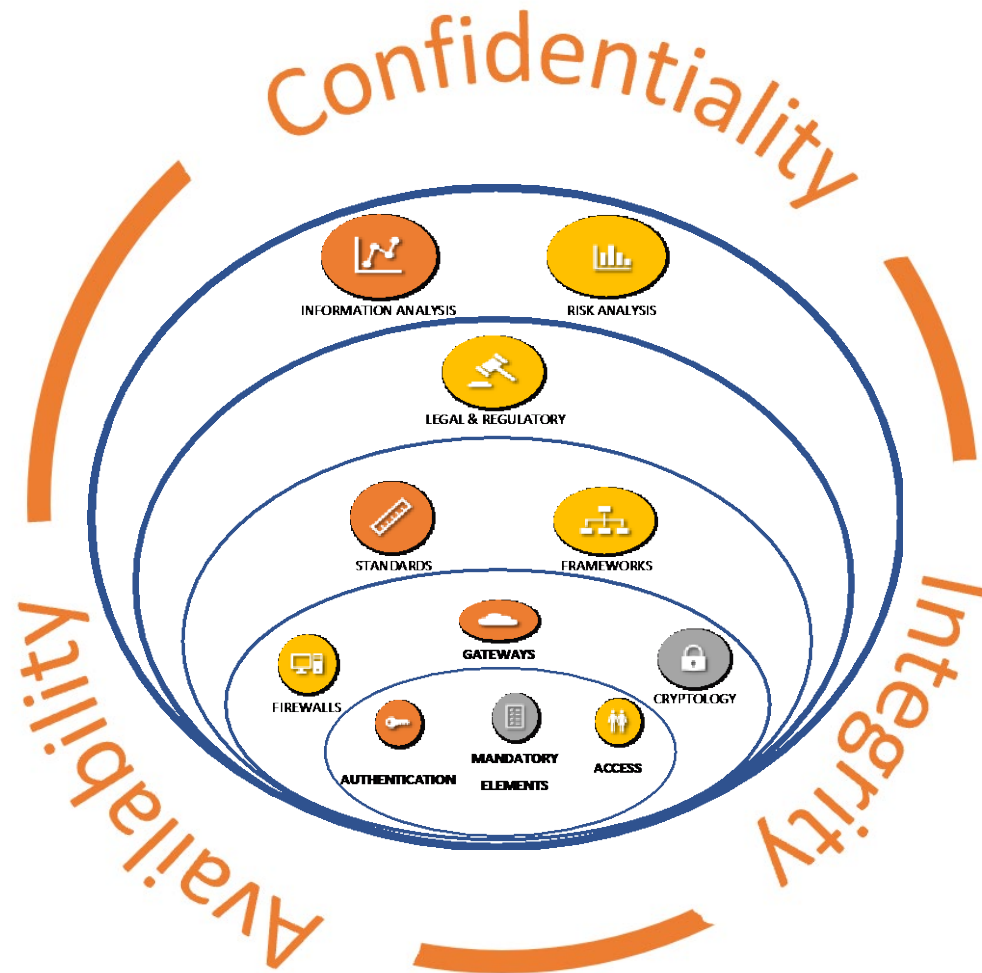
Cybersecurity

is the protection of systems, processes, networks and data in cyberspace.

What is security posture?

What is cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring Confidentiality, Integrity, and Availability of information.*

The goal of cybersecurity is to protect inter-networked systems from cyber-threats and known vulnerabilities.
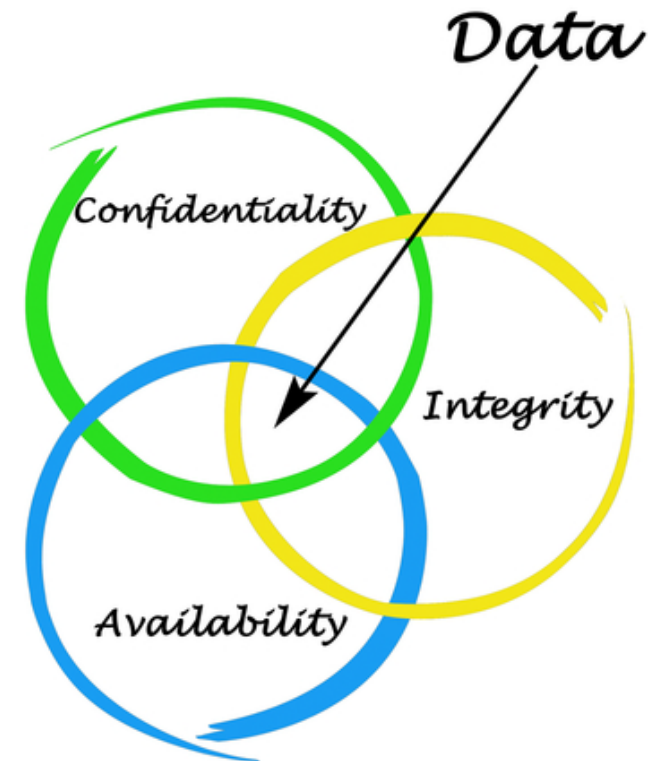
*Cybersecurity and Infrastructure Security Agency (CISA), Dept of Homeland Security

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

Designing for resilience

How does risk management align with cybersecurity capabilities?

We don't know what we don't know!

Cybersecurity Risk Management Process -

ISO 31000 defines a general approach to enterprise risk management, involving

- Communication and consultation
- Establishing the context
- Risk assessment
- Solutions are designed to address specific threat
  - Risk identification
  - Risk analysis
  - Risk evaluate
- Risk treatment
- Monitoring and Review

Communication and consultation

Monitoring and review

Establishing the context

Identification

Analysis

Evaluation

Risk treatment

I-PERCEPTIONS

he Cyber BA
SECURITY FIRST
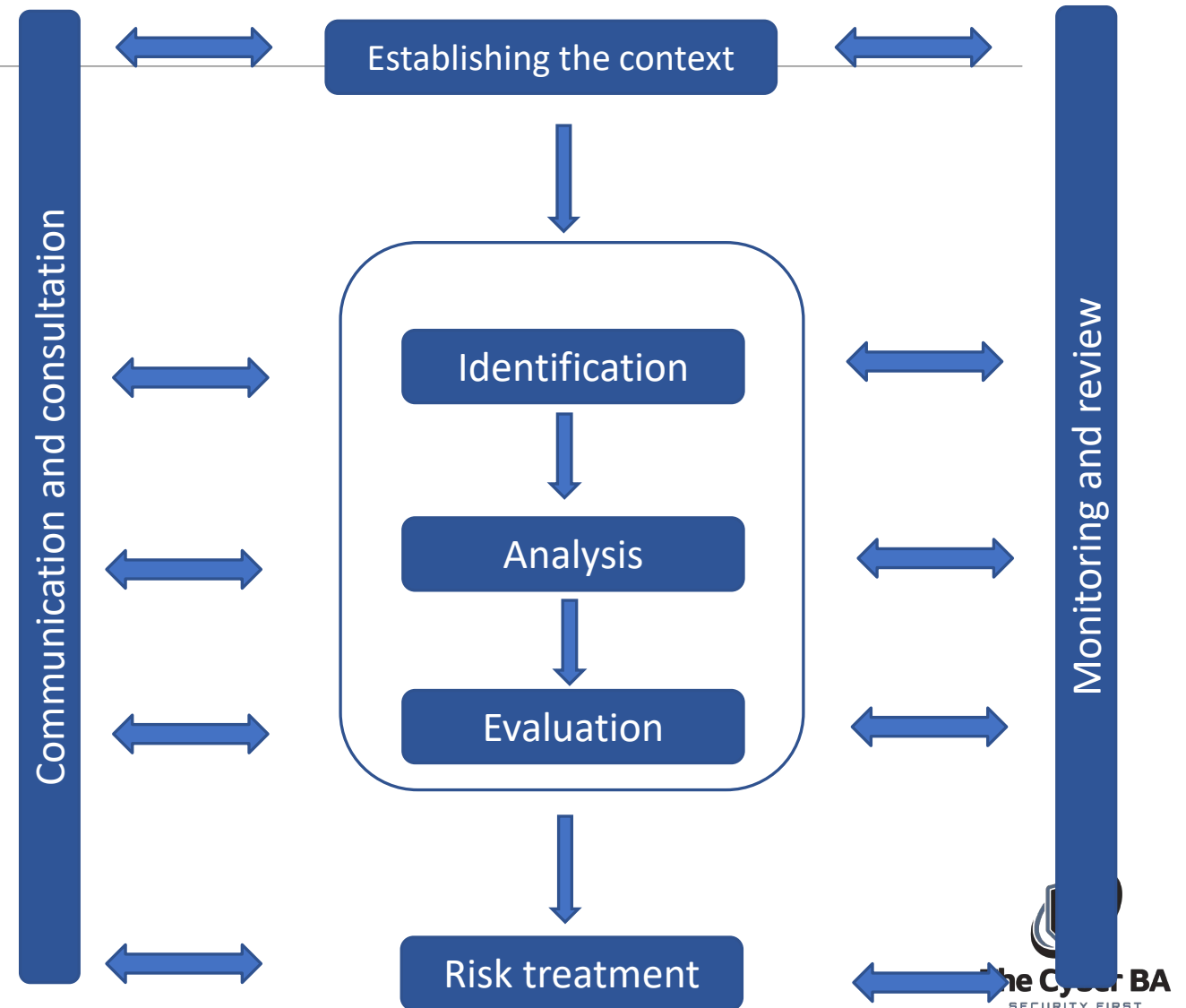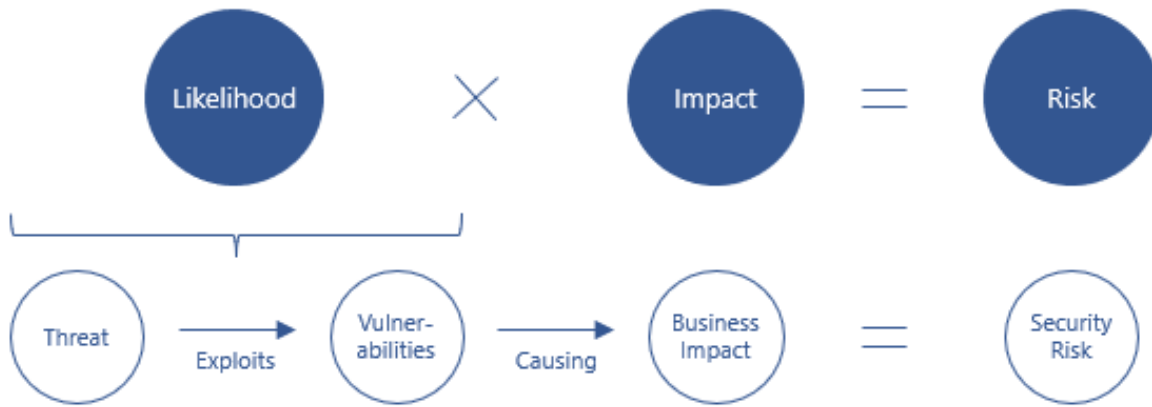
Cyber Risk = Business Risk

COMPLIANCE IS NOT ENOUGH

What roles or activities can BAs play in making your business more secure against cyber threats?
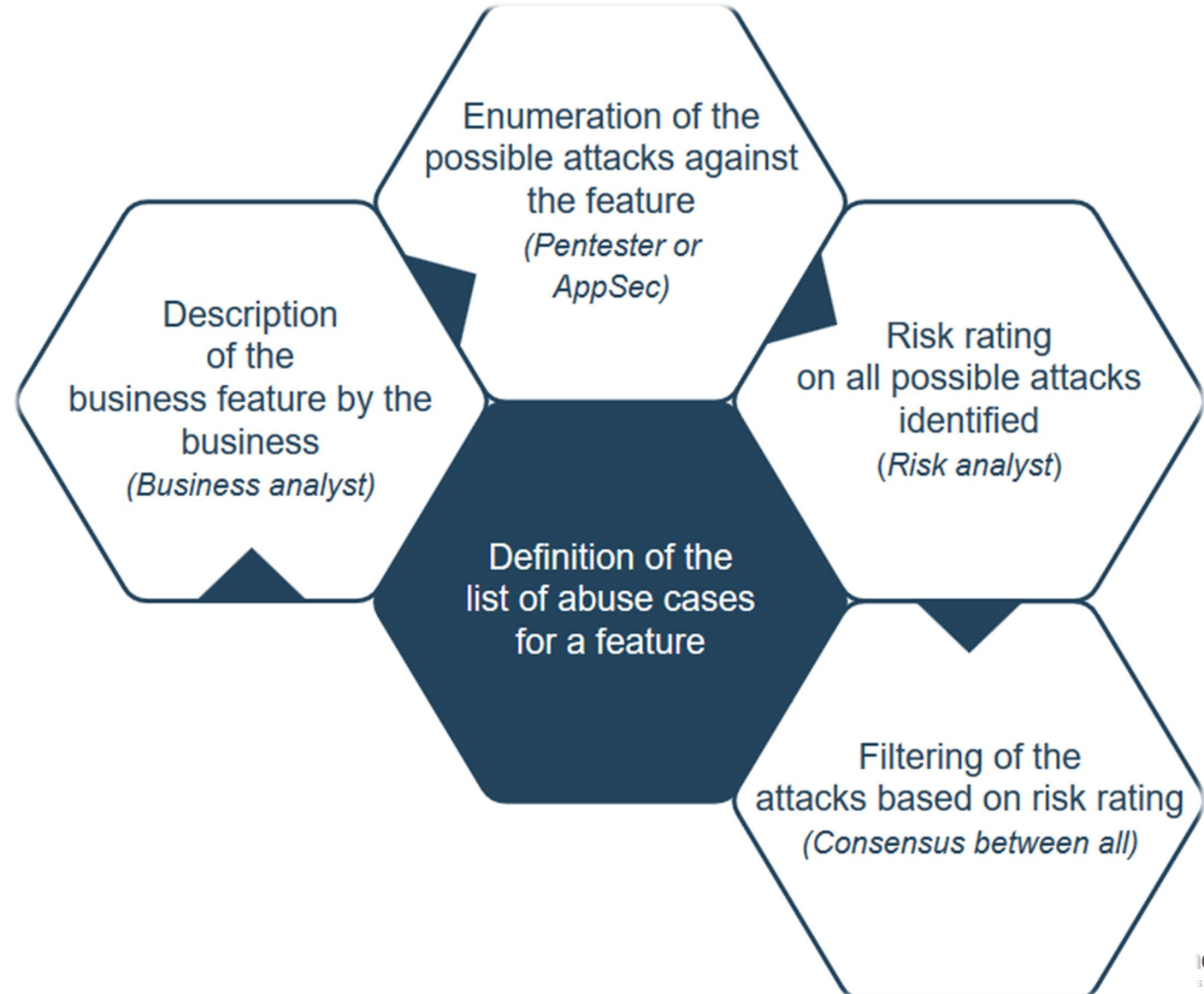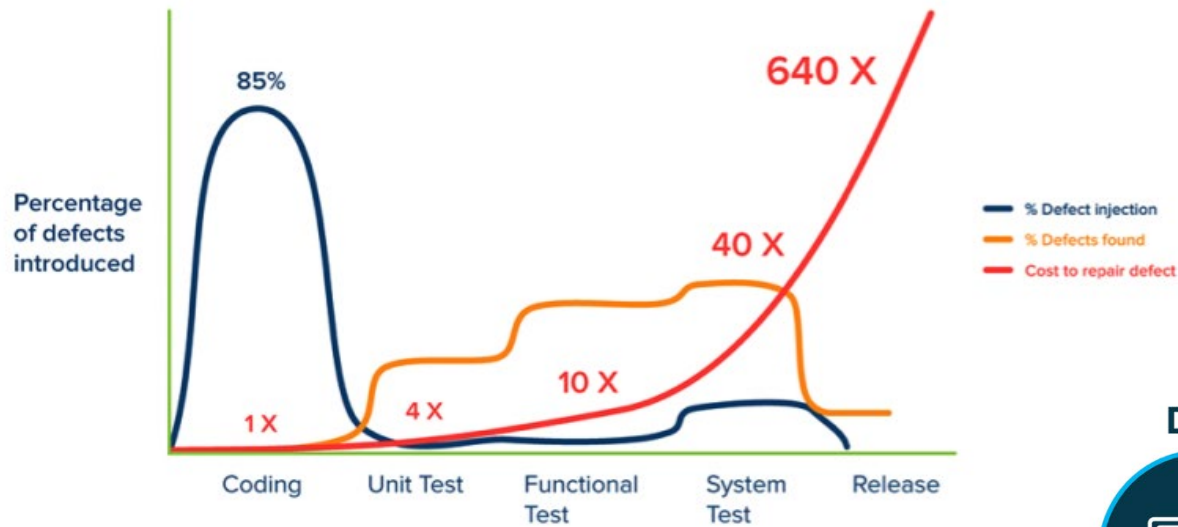
BA's perform risk analysis by…

➢ Implementing risk management frameworks

➢ Identifying assets and configurations

➢ Tracking vulnerabilities

➢ Performing risk assessments

➢ Tracking exception cases

➢ Driving prioritization
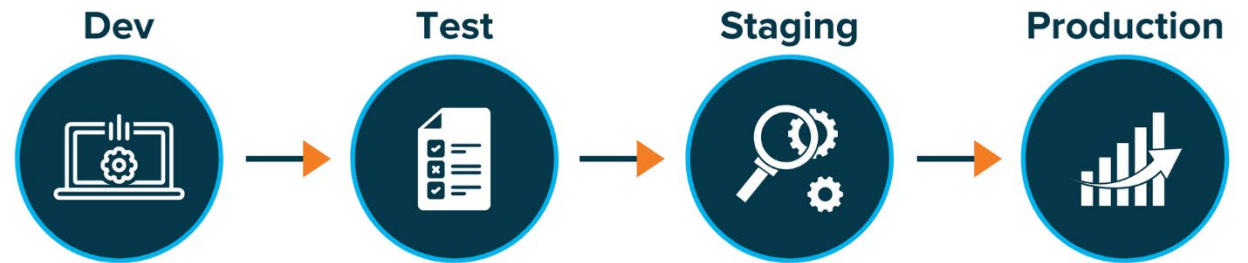
➢ Categorizing mitigating controls

Writing user stories for security

An abuse case can be defined as a way an attacker can exploit a feature that was not expected by the designer or allow an attacker to misuse the feature controls to redirect inputs and outputs.

Description
of the
business feature by the
business
(Business analyst)

Enumeration of the
possible attacks against
the feature
*(Pentester or
AppSec)*

Risk rating
on all possible attacks
identified
(Risk analyst)

Definition of the
list of abuse cases
for a feature

Filtering of the
attacks based on risk rating
(Consensus between all)

e Cyber BA
ECURITY FIRST

This Photo by Unknown Author is licensed under CC BY-SA-NC

Cybersecurity requirements

BAs can include cybersecurity requirements in…

- Initial Business Case
- Work Breakdown Structure (WBS)
- Concept and design drawings
- Permitting processes
- Project milestones
- Information security, privacy and compliance reviews
- Dev, Test, QA, Pre-prod environment designs
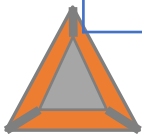- Test plan

Q & A

I-PERCEPTIONS and The Cyber BA®

Resources

Useful resources – Cybersecurity/Risk

Org	Name of agency	URL
IIBA CCA	IIBA Cybersecurity Certificate in Analysis	https://www.iiba.org/certification/iiba-certifications/specialized-business-analysis-certifications/certificate-in-cybersecurity-analysis/
ENISA	European Union Agency for Cybersecurity	https://www.enisa.europa.eu/
GIAC	GIAC Certifications	https://www.giac.org/
CISA	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
NIST	National Institute of Standards and Technology	https://www.nist.gov/cyberframework
NCSC	The National Cyber Security Centre	https://www.ncsc.gov.uk/
ISO	ISO/IEC 27001 Information Security Framework	https://www.iso.org/isoiec-27001-information-security.html
ISO	ISO 31000 Risk Management Standards	https://www.iso.org/iso-31000-risk-management.html
ASD	Australian Cyber Security Centre	https://www.asd.gov.au/cyber
SANS	SANS Institute	https://www.sans.org/
(ISC)^2	The International Information System Security Certification Consortium, or (ISC)²	https://www.isc2.org/
ISACA	Information Systems Audit and Control Association® (nee)	https://www.isaca.org/
ISSA	Information Systems Security Association (ISSA)®	https://www.issa.org/
OWASP	The Open Web Application Security Project®	https://owasp.org/
ISF	Information Security Forum (ISF)	https://www.securityforum.org/
ICMCP	International Consortium of Minority Cyber Professionals	https://www.icmcp.org/
EWF	Executive Women's Forum	https://www.ewf-usa.com/
CSA	Cloud Security Alliance	https://cloudsecurityalliance.org/

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

Research and Reporting - Cybersecurity

ORG	Organization Name	URL
CSIS	The Center for Strategic and International Studies	https://www.csis.org/
DBIR	Verizon Data Breach Information Report	https://enterprise.verizon.com/resources/reports/dbir/
CIR	AT&T Cybersecurity Insights Report	https://www.business.att.com/categories/cybersecurity-insights-report.html
CSCIS	Center for Strategic Cyberspace & International Studies (CSCIS)	https://www.cybersecurityintelligence.com/
	Cybersecurity Ventures	https://cybersecurityventures.com/research/
	McKinsey Insights	https://www.mckinsey.com/business-functions/mckinsey-digital/mckinsey-technology/overview/cybersecurity
NTSC	Checkpoint Software Cybersecurity Report 2020	https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf
CISO MAG	CISO Magazine	https://cisomag.eccouncil.org/
	CPO Magazine	https://www.cpomagazine.com/

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

Cybersecurity Statistics for 2019

- The global cost of online crime is expected to reach $6 trillion by 2021
- By 2021, the number of unfilled cybersecurity jobs is expected to balloon to 3.5 million
- Cybersecurity expenditures are expected to reach $1 trillion by 2024
- IoT attacks were up by 600% in 2017
- A business falls victim to a ransomware attack every 13.275 seconds
- Just 38% of global organizations claim that they are equipped and able to handle a complex cyber attack
- $2.4 million is the average cost of a malware attack in 2017
- 43% of cyber attacks are targeted at small businesses
- 95% of data breaches have cause attributed to human error

Info Source – Cyber Defence Magazine

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST

Certificate in Cybersecurity Analysis

Thank You

You can reach us on LinkedIn or email for any questions

bindu.channaveerappa@gmail.com

terrybaresh@gmail.com

I-PERCEPTIONS

The Cyber BA
SECURITY FIRST