RISK CLOUD CYBER TESTED

Healthcare Security / BioTeam

Securing the Healthcare Ecosystem

September 19th – The Markley Center

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

@coderrem

Mark Coderre

National Practice Director, CISO

CISM, CRISC

OPENSKY A TÜV Rheinland Company

Digital Enterprise – Protected.

The Security Continuum

Risk Management

Threat Detection & Response

Security Testing

Security Architecture

Must-Do's for Healthcare

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

That feeling when you followed all the healthcare regulations and were compromised anyways

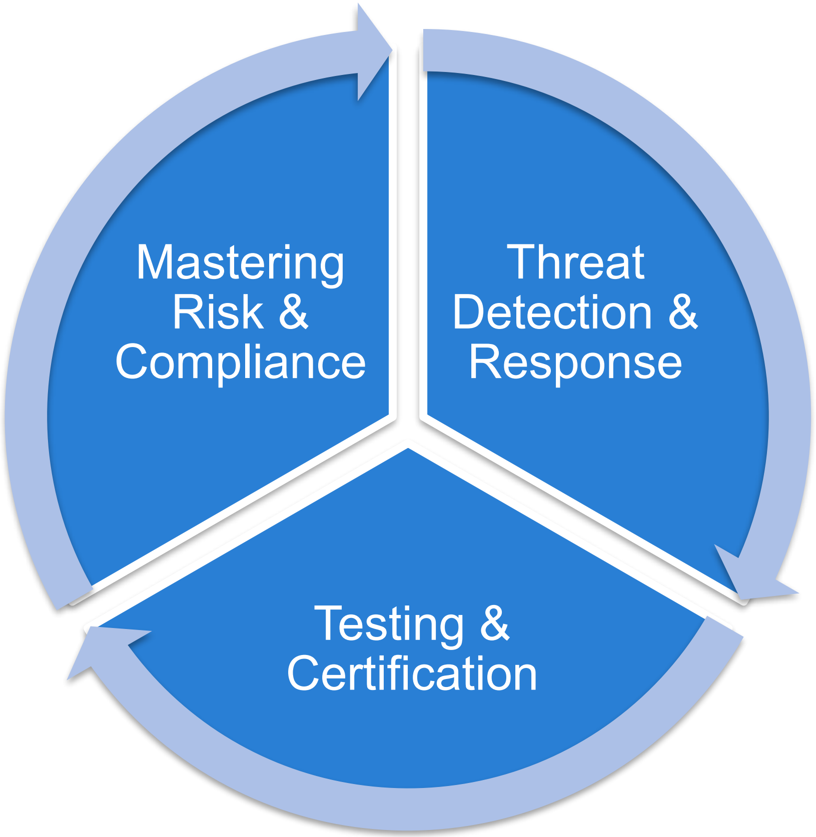
OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

When we say "Healthcare" we mean…

- ✓Payers
- ✓Providers/HDO –Partners
- ✓Pharmaceuticals
- ✓Pharmacy /Wholesale (PBM)
- ✓Retail(Rx)
- ✓Biotech
- ✓Laboratories
- ✓Diagnostics

- ✓ Medical Device Manufacturers
- ✓ Technology Vendors
- ✓ ACO
- ✓ PHR Services
- ✓ ePrescribing
- ✓ HIE
- ✓ HIX



Let’s talk about a continuum for Healthcare IT that focuses on <u>threat</u>

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

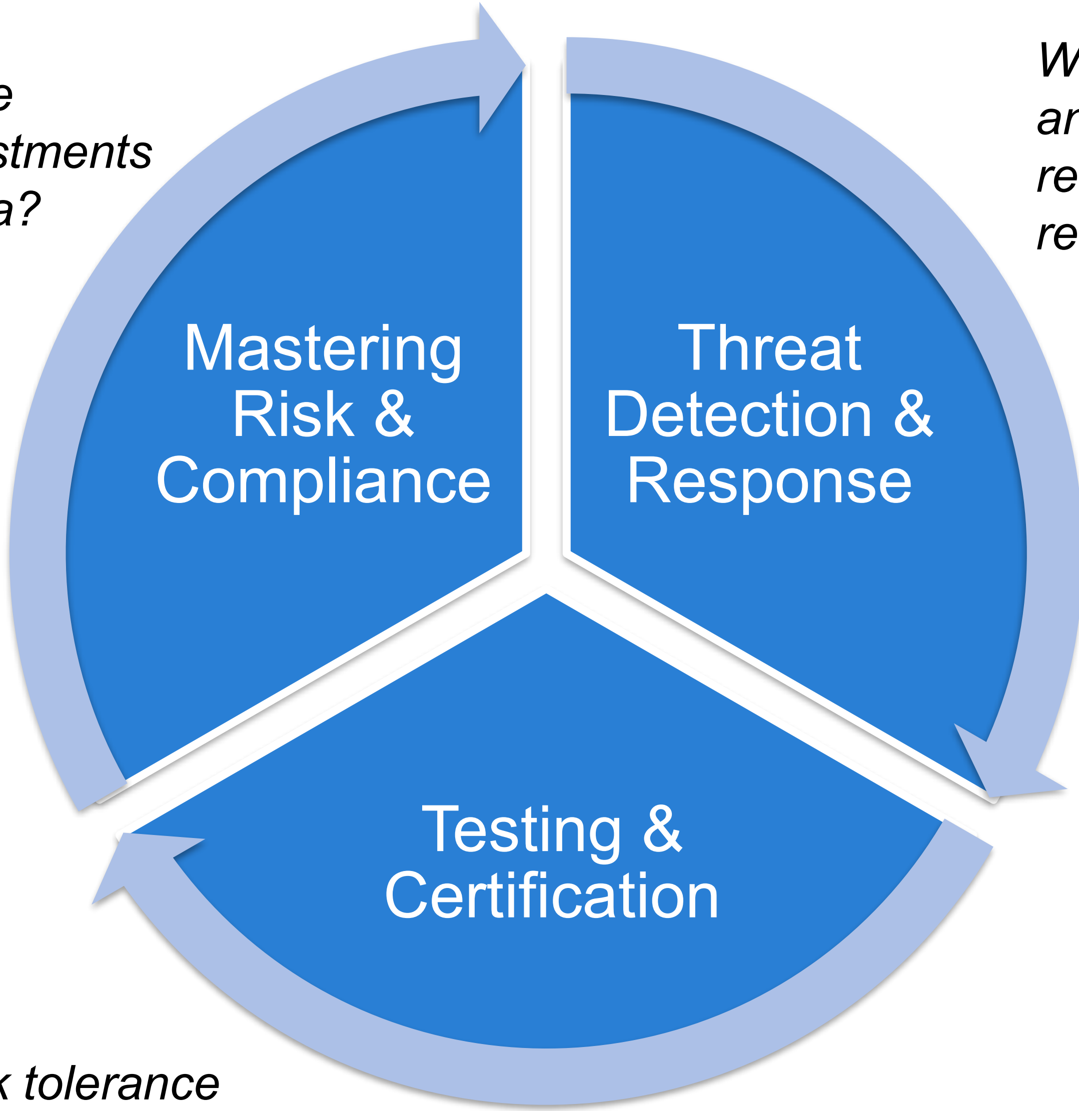
How do I Determine best investments using data?

How does this relate To my compliance Obligations?

How quickly should remediation be completed?

What are the key controls?

What risk tolerance Is appropriate?



What data and analytics are required for business resilience?

What events and behaviors are threatening?

What scenarios Should be tested on various assets

Test what components?

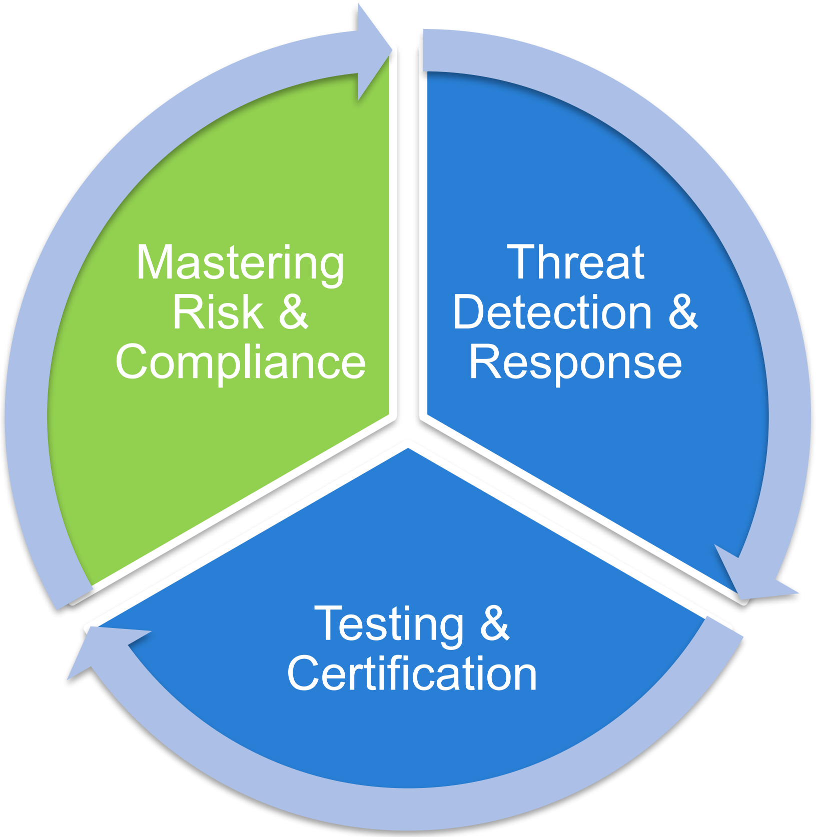
How should we test?

How often?

OPENSKY A TÜV Rheinland Company

TÜVRheinland® Precisely Right.

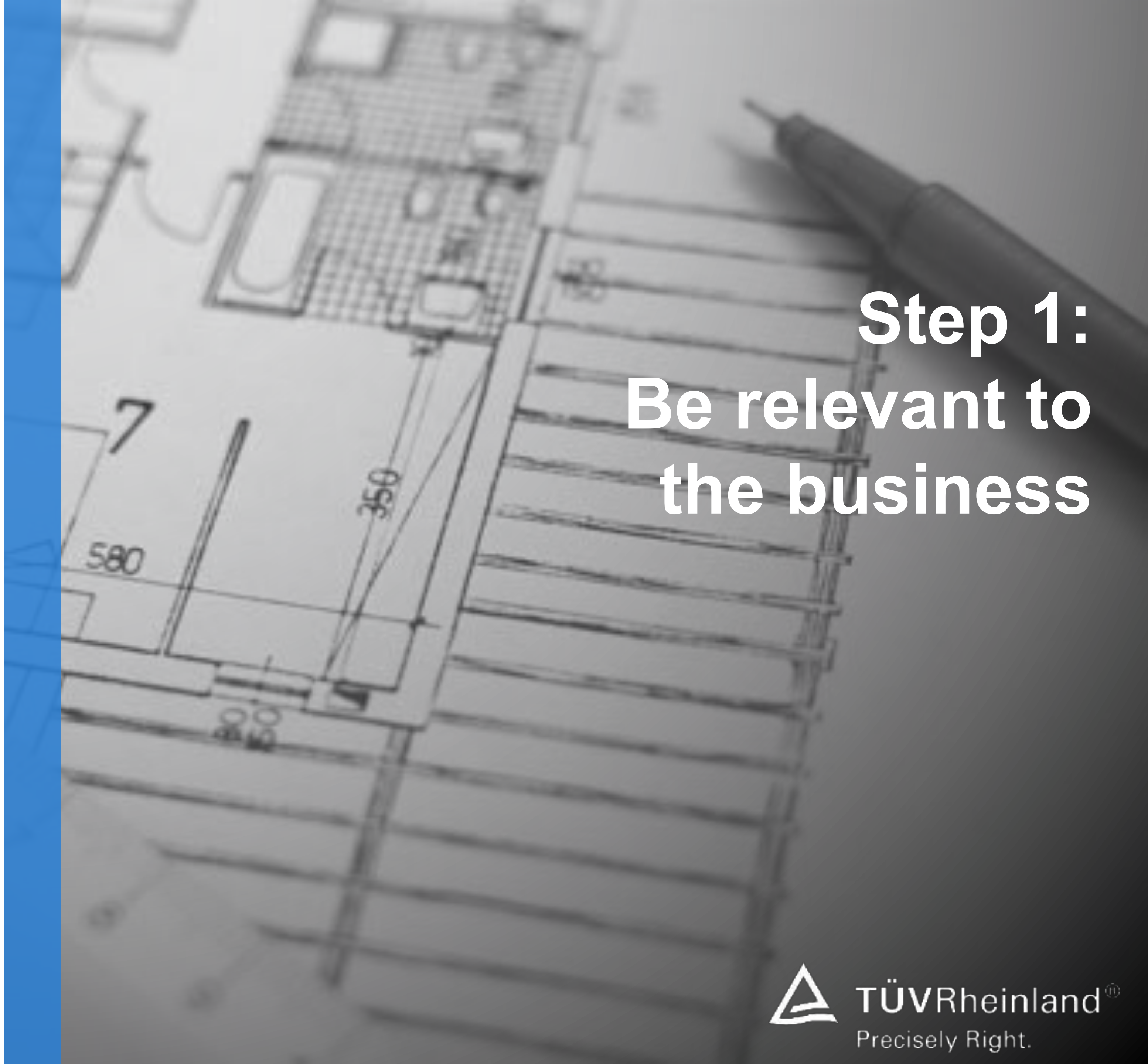
Step 1:
Be relevant to the business



Mastering Risk & Compliance

Threat Detection & Response

Testing & Certification



OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Mastering Risk Translates it all…

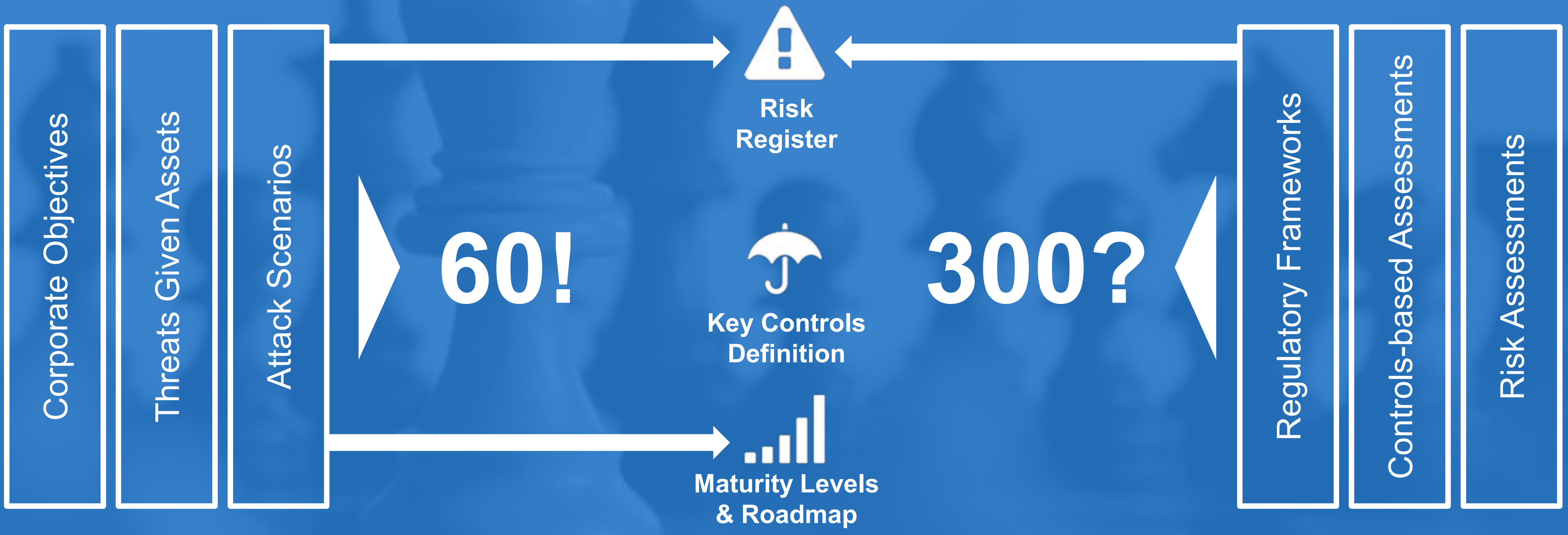
Attacks on Business

Analytics & Machine Learning

Attack-based Testing

The 80/20 Rule of Management applies more than ever in Security

Think left to right, not just right to left



Corporate Objectives

Threats Given Assets

Attack Scenarios

60!

Risk Register

Key Controls Definition

Maturity Levels & Roadmap

300?

Regulatory Frameworks

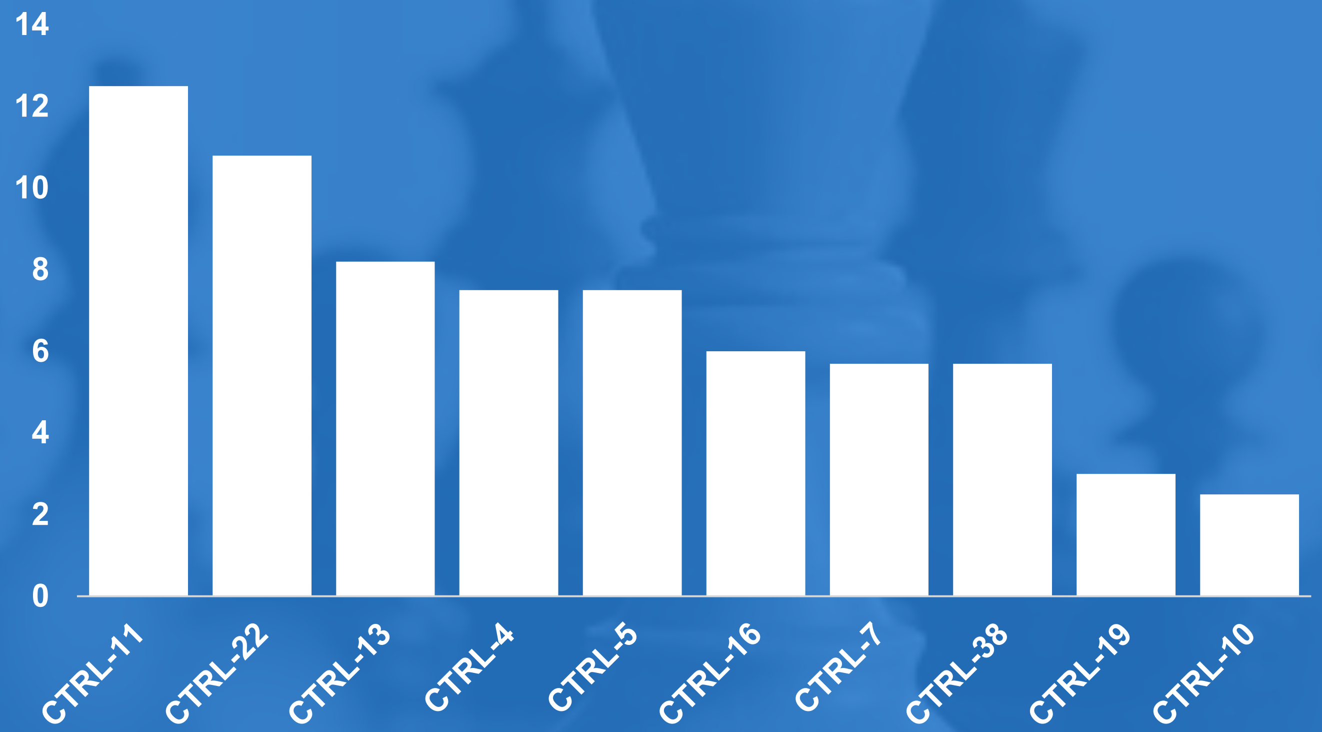
Controls-based Assessments

Risk Assessments

Benefit: Proportional Value of Controls

Can you rationalize how to allocate resources wisely?

Top 10 Controls and Values (ROSI)



Investment Questions:

- Where should I invest?
- Should I improve existing controls or build more?
- How much should I spend?
- Where can security innovation fit in?

Execution Questions:

- Did the PMO deliver what the investment was intended to yield?
- Did technology meet the marketing promise?

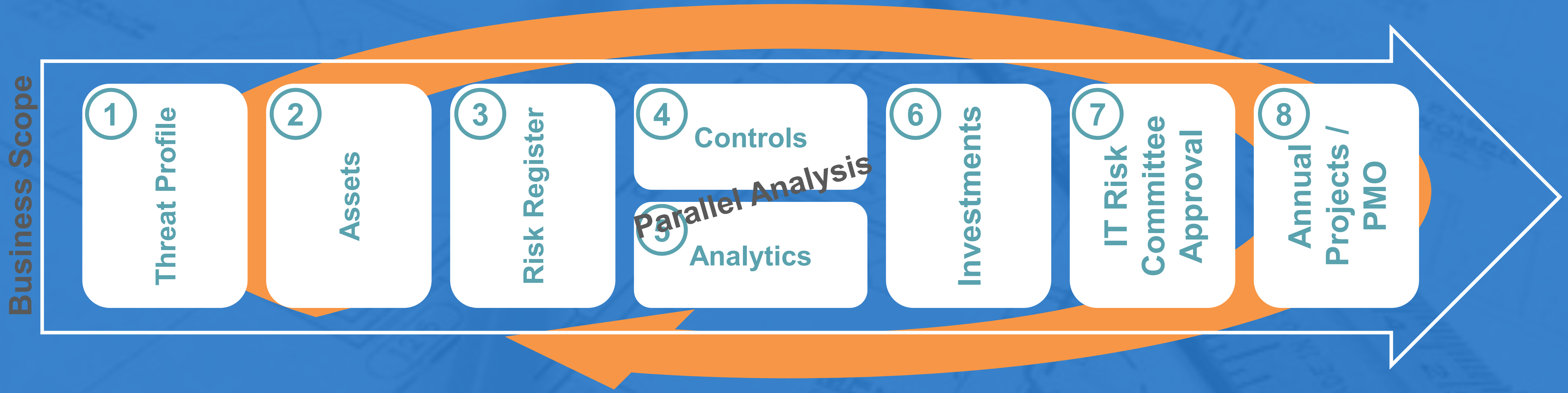
Operational Questions:

- Are any of my key controls decaying? KPI's
- What skills are needed?

OPENSKY A TÜV Rheinland Company

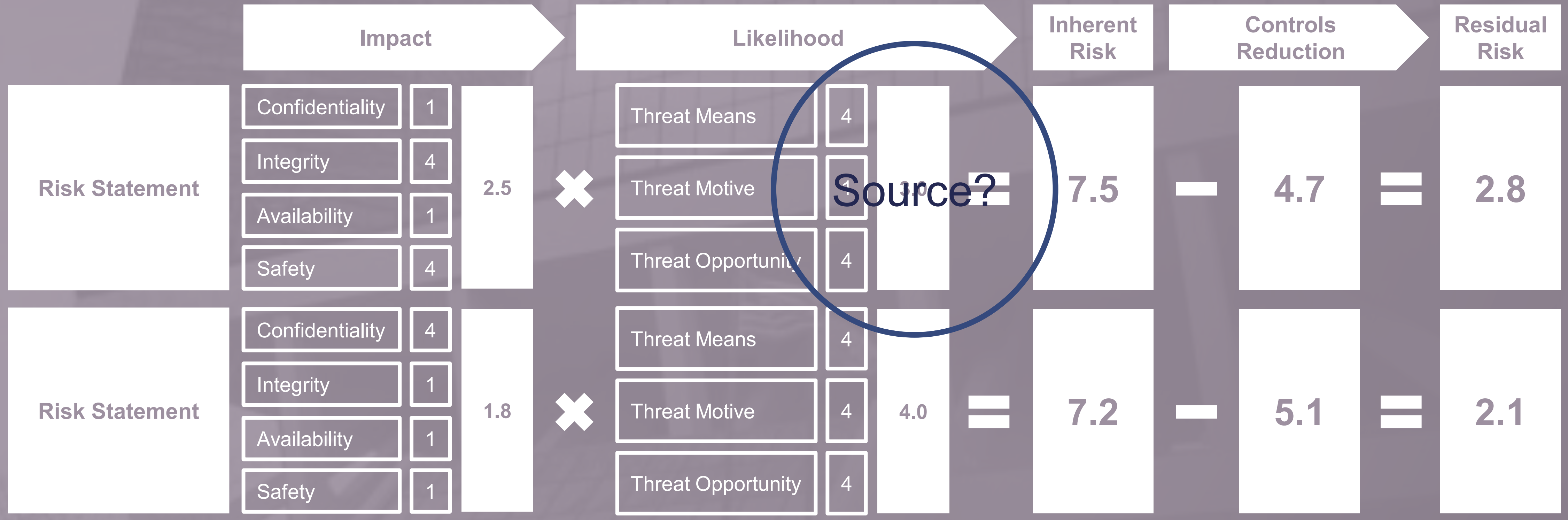
TÜVRheinland® Precisely Right.

Cyber-Risk Prioritization Methodology



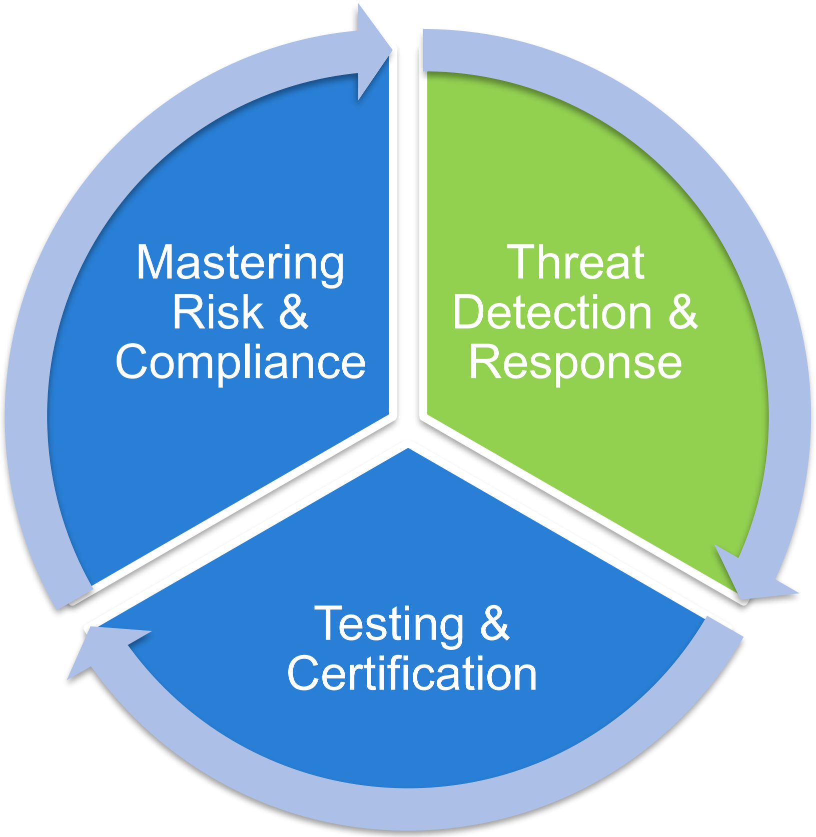
It starts with a business conversation which garners support and credibility in action

Mastering Risk – The new “Risk Register” is not control focused



	Impact				Likelihood				Inherent Risk		Controls Reduction		Residual Risk
Risk Statement	Confidentiality	1	2.5	✖	Threat Means	4	3.0	=	7.5	–	4.7	=	2.8
	Integrity	4			Threat Motive	1							
	Availability	1			Threat Opportunity	4							
	Safety	4											
Risk Statement	Confidentiality	4	1.8	✖	Threat Means	4	4.0	=	7.2	–	5.1	=	2.1
	Integrity	1			Threat Motive	4							
	Availability	1			Threat Opportunity	4							
	Safety	1											

Source?

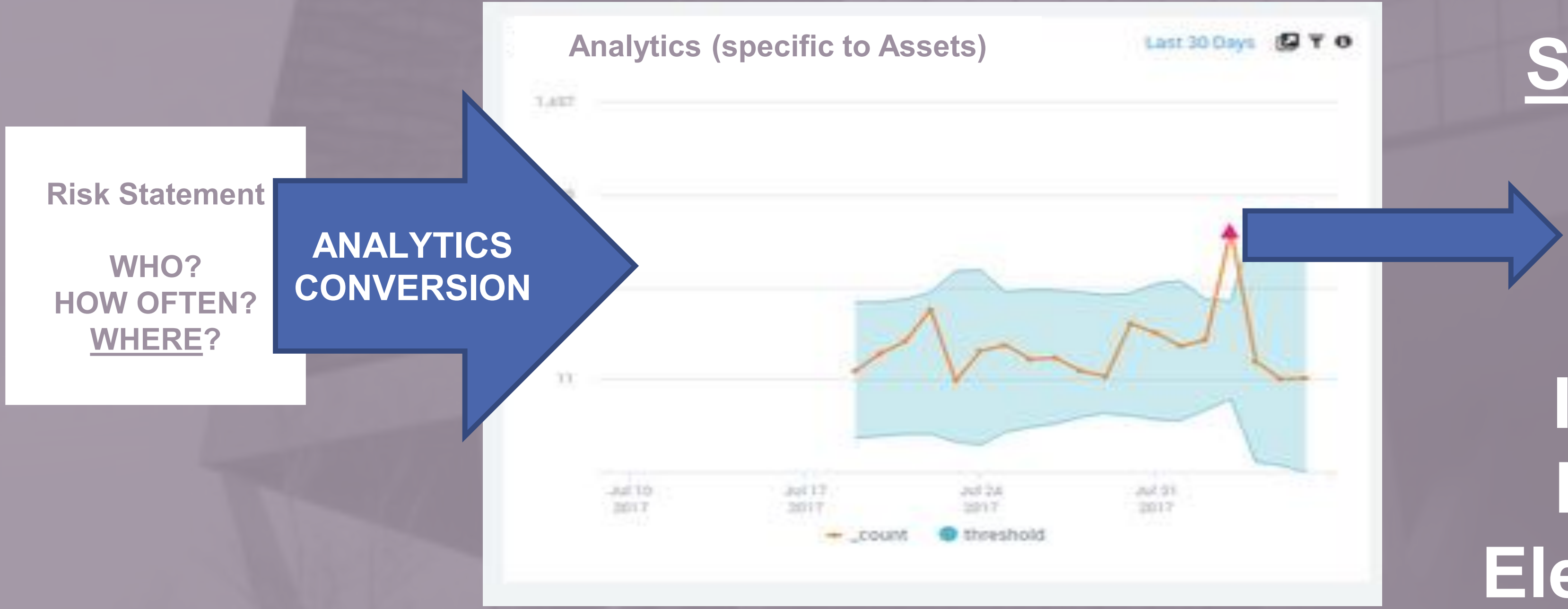


Step 2: Seek empirical data

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Enter Threat Intelligence:
Analytics and Machine Learning



Risk Statement

WHO?
HOW OFTEN?
<u>WHERE</u>?

ANALYTICS CONVERSION

Analytics (specific to Assets)

Sample from SumoLogic

<u>Specific Scenarios</u>

Spoofing

Tampering

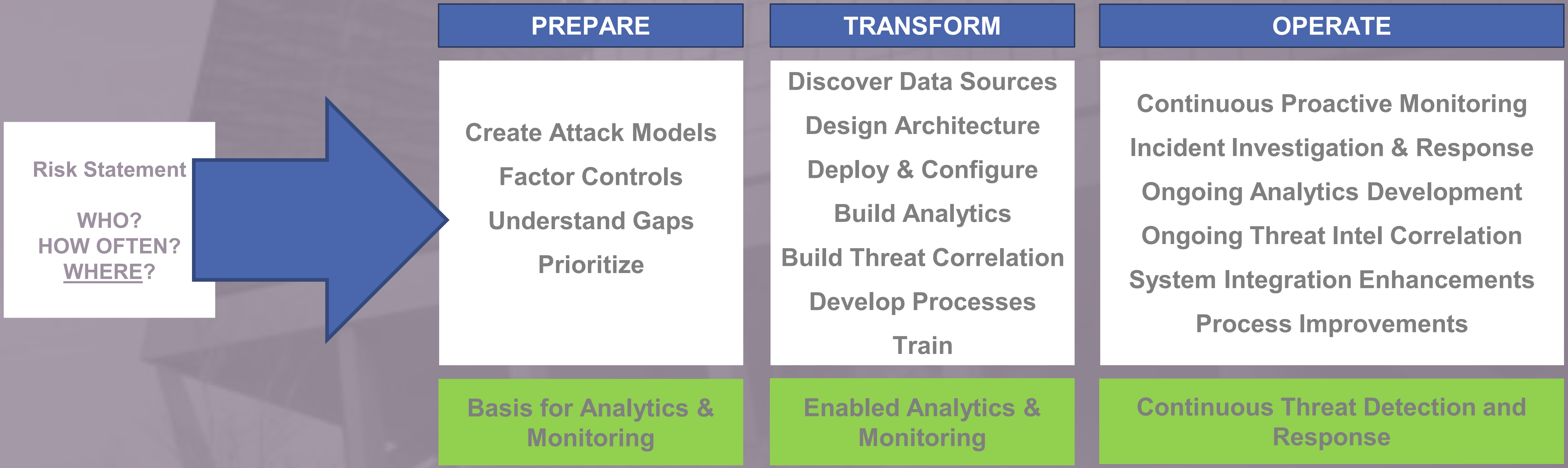
Repudiation

Information Loss

Denial of Service

Elevation of Privilege

Step by step conversion: Risk to Analytics



Risk Statement

WHO?
HOW OFTEN?
WHERE?

PREPARE

Create Attack Models

Factor Controls

Understand Gaps

Prioritize

Basis for Analytics & Monitoring

TRANSFORM

Discover Data Sources

Design Architecture

Deploy & Configure

Build Analytics

Build Threat Correlation

Develop Processes

Train

Enabled Analytics & Monitoring

OPERATE

Continuous Proactive Monitoring

Incident Investigation & Response

Ongoing Analytics Development

Ongoing Threat Intel Correlation

System Integration Enhancements

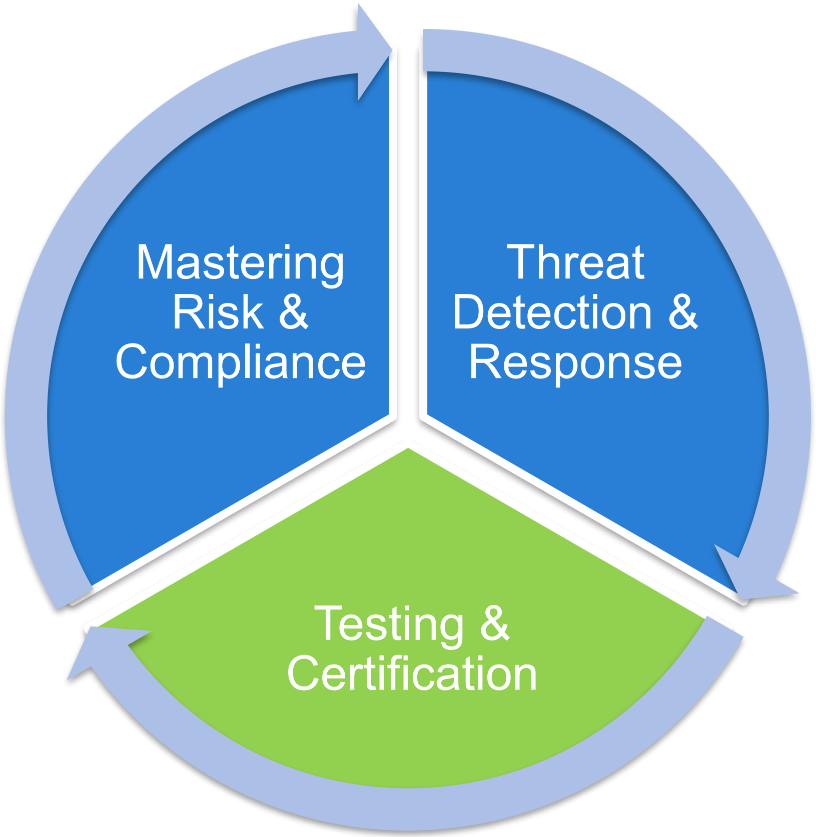
Process Improvements

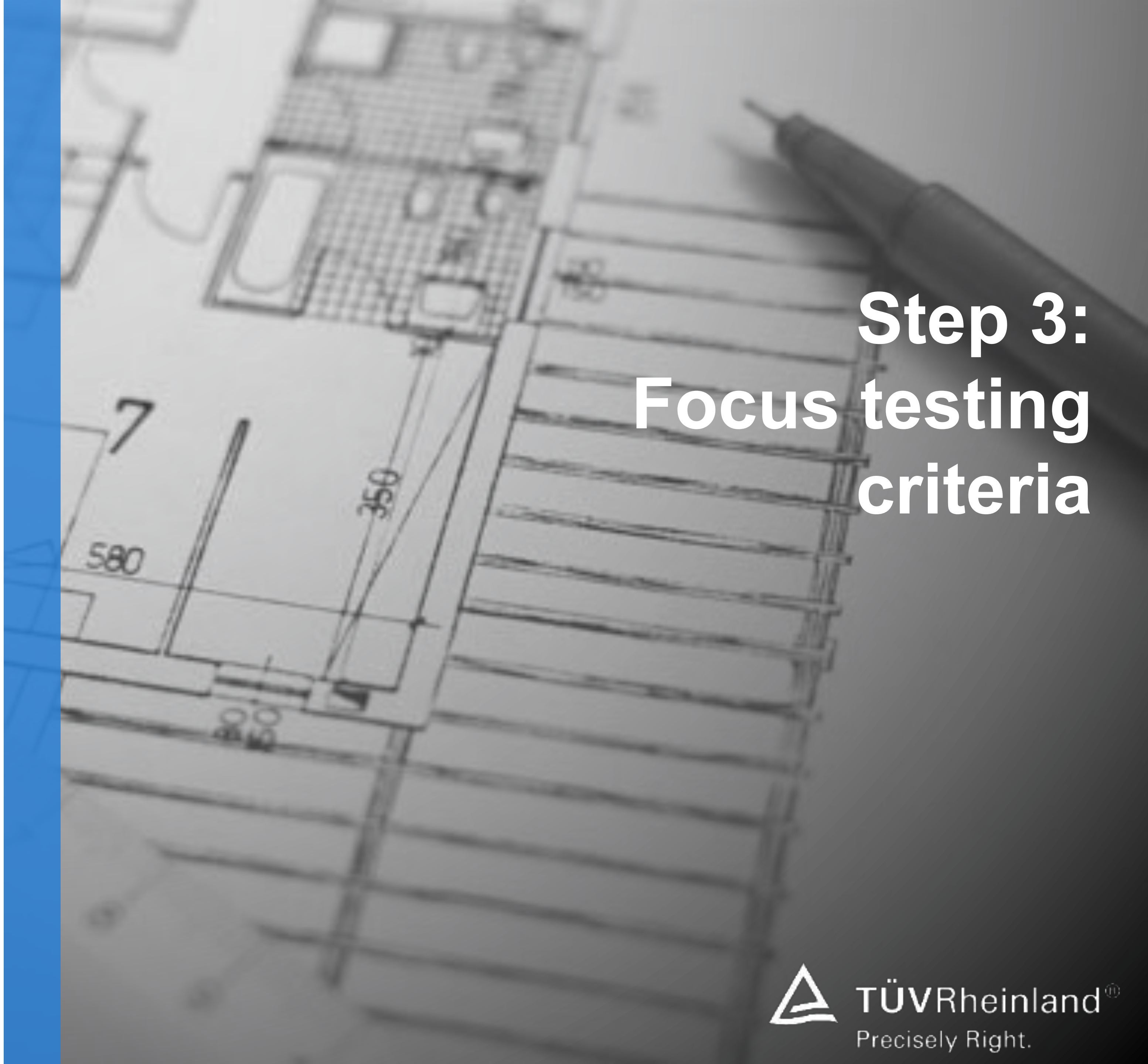
Continuous Threat Detection and Response

Analytics and Machine Learning Influence

Characteristics of optimal “Machine Learning” use

- Focus on specific behaviors driven from risk program
- Learn historic patterns of behaviors
- Anticipate future patterns using regression analysis
- Look at anomalies
- Leverage platform that provides clustering and baselining
- Practice statistical analysis to seek outliers



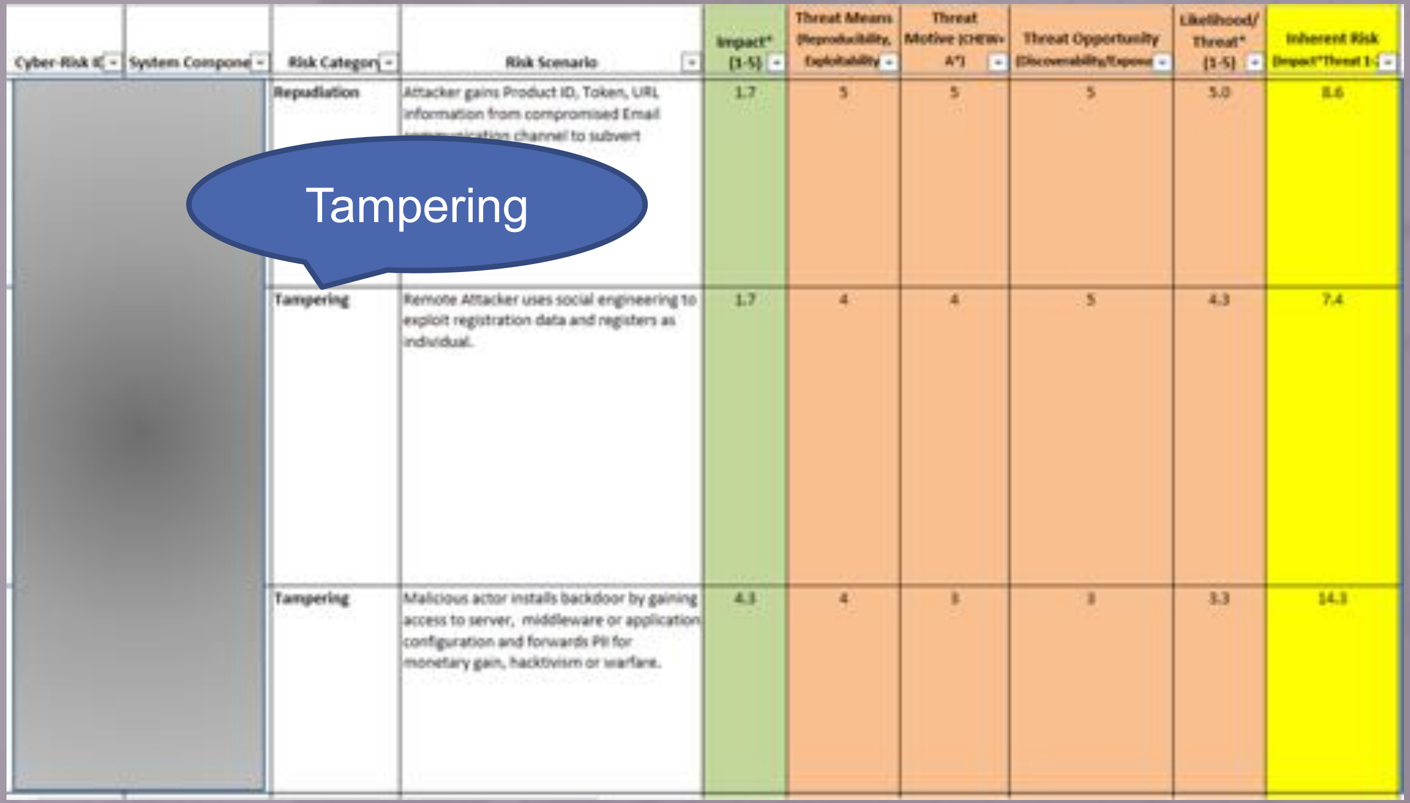


Step 3: Focus testing criteria

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Testing with Threat Modeling



Tampering

Cyber-Risk ID	System Compone	Risk Category	Risk Scenario	Impact* (1-5)	Threat Means (Reproducibility, Exploitability	Threat Motive (CHEW+ A*)	Threat Opportunity (Discoverability/Exposu	Likelihood/ Threat* (1-5)	Inherent Risk (Impact*Threat 1-
		Repudiation	Attacker gains Product ID, Token, URL information from compromised Email communication channel to subvert	1.7	5	5	5	5.0	8.6
		Tampering	Remote Attacker uses social engineering to exploit registration data and registers as individual.	1.7	4	4	5	4.3	7.4
		Tampering	Malicious actor installs backdoor by gaining access to server, middleware or application configuration and forwards PII for monetary gain, hacktivism or warfare.	4.3	4	3	3	3.3	14.3

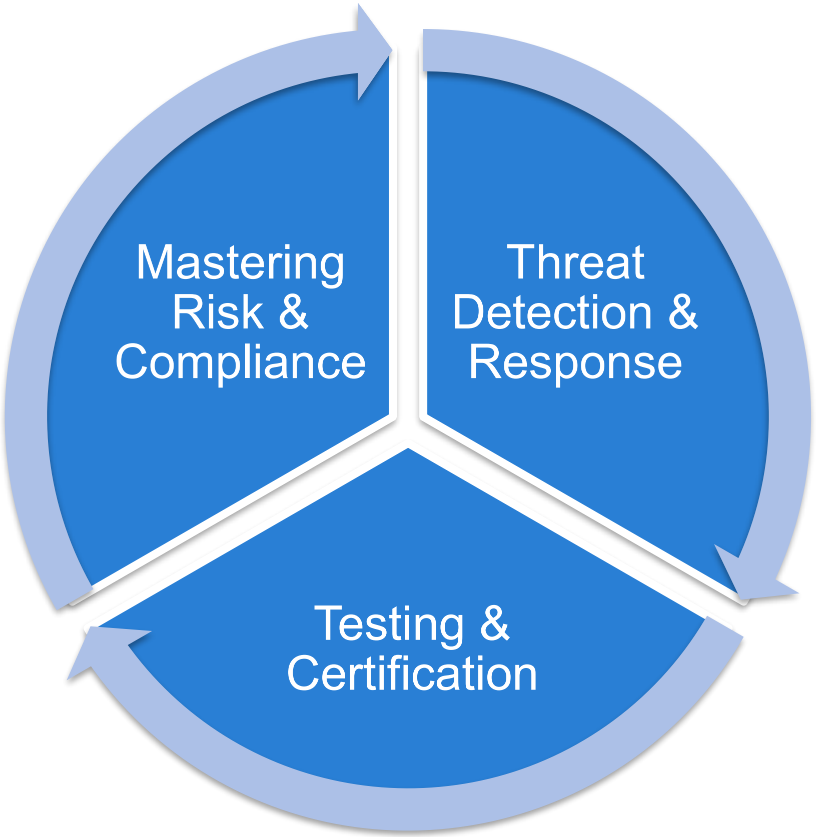
<u>When testing next release</u>:

- **Source Code Review Priorities**
- **Static & Dynamic Analysis results interpretation**
- **Penetration Testing – new impacts**

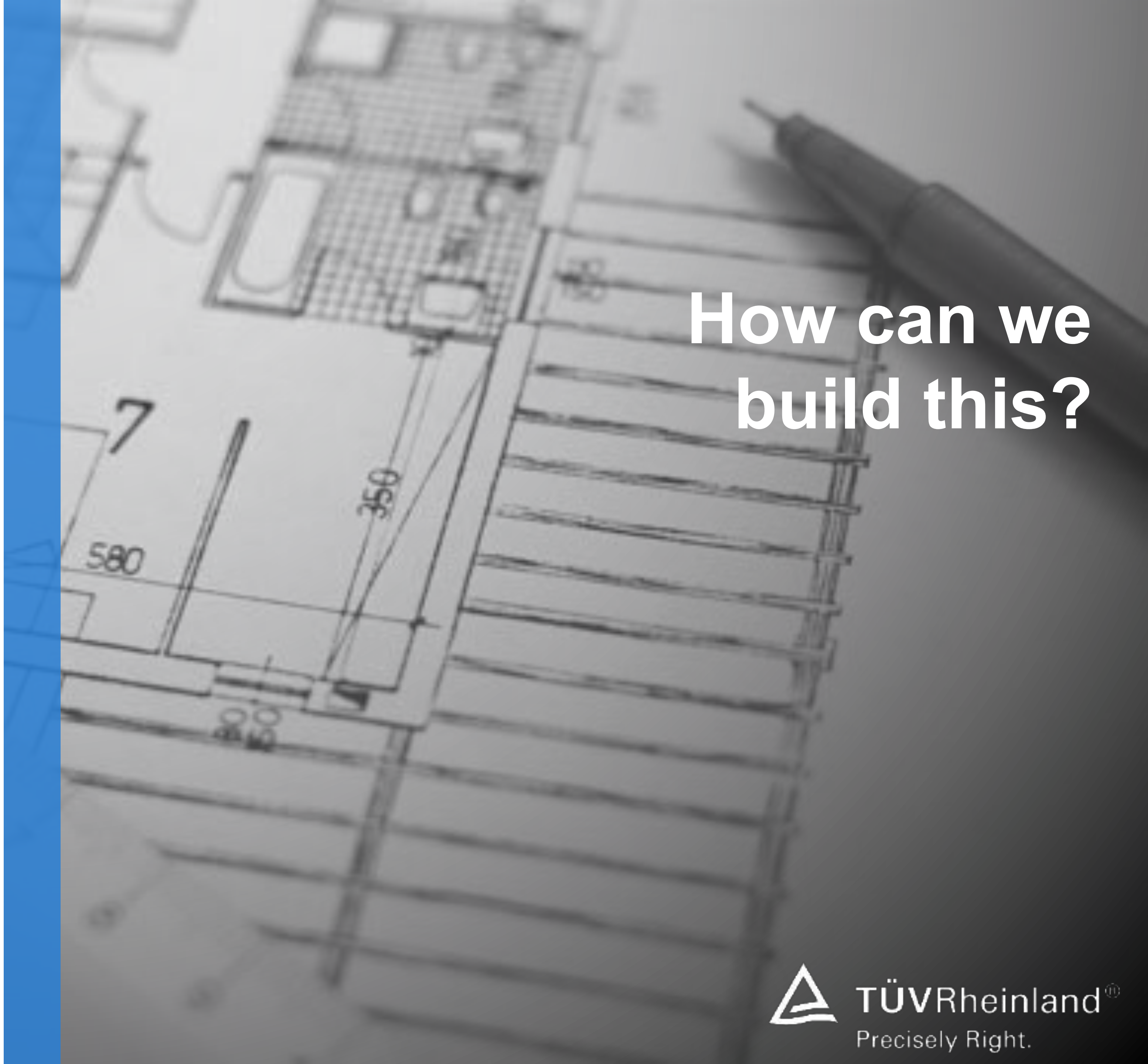
Testing with Threat Modeling

Characteristics of optimal "Threat Modeling" use

- Part of a broader build security in mentality - BSIMM
- Pragmatic Standards
  - When to trigger - Inherent risk filters
- Using attack categories for the art and science:
  - Lightweight, not too cumbersome, memorable
  - Boiling out bias through iterative encounters
- Tying results back into a GRC for action *or* monitoring



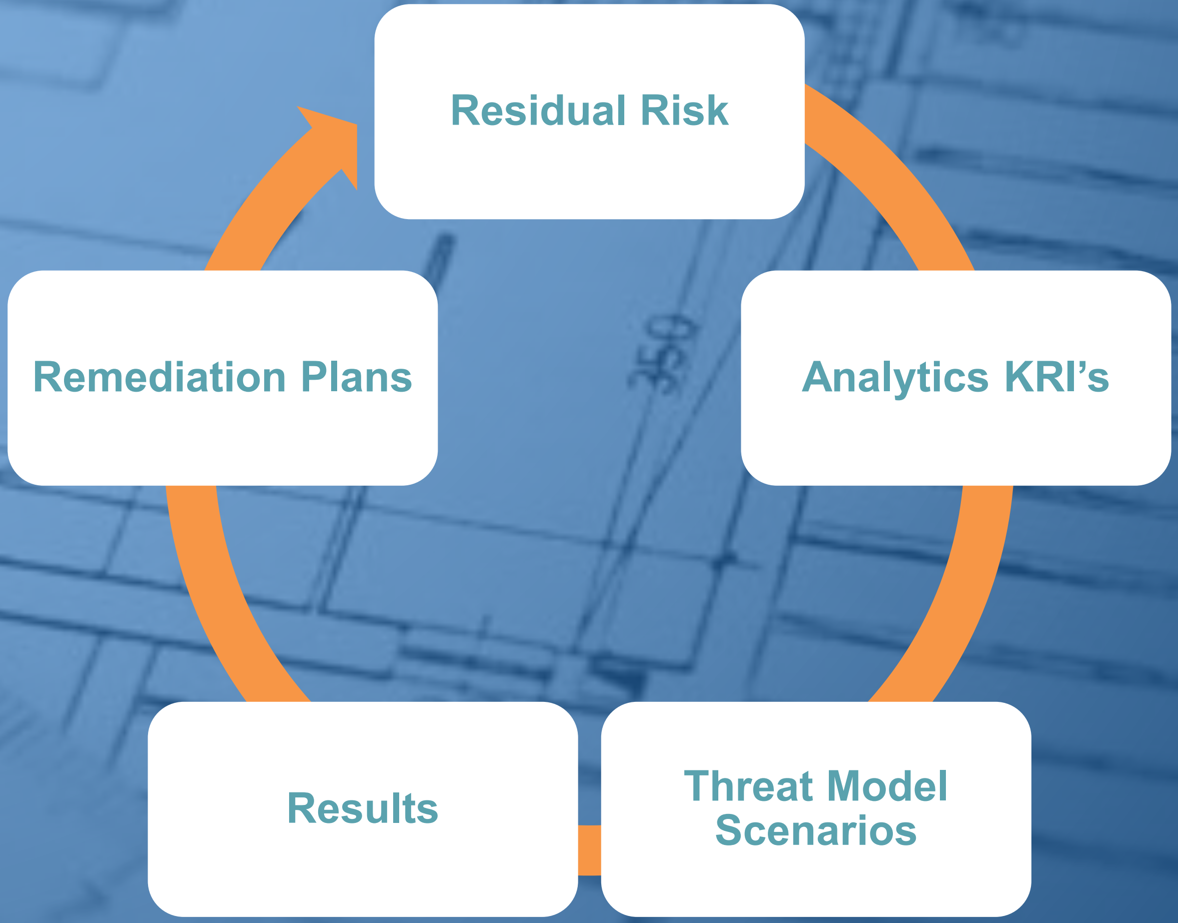
OPENSKY
A TÜV Rheinland Company



How can we build this?

TÜVRheinland®
Precisely Right.

Process View - Risk over Time



Residual Risk

Analytics KRI’s

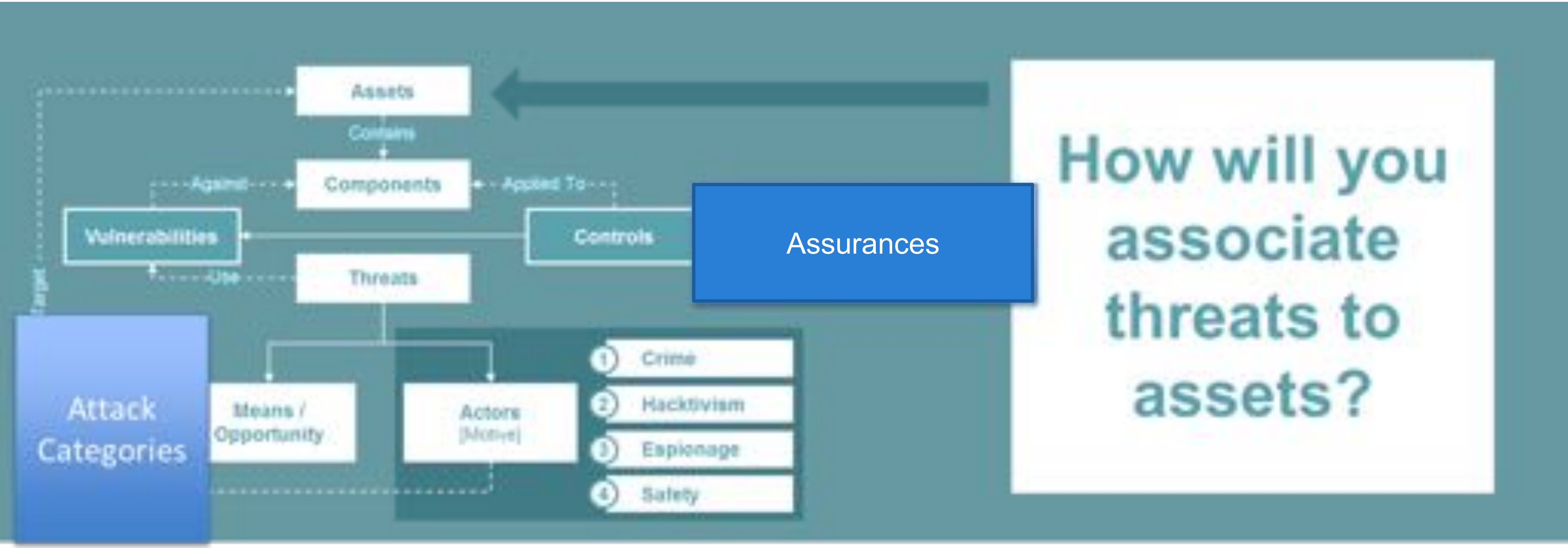
Threat Model Scenarios

Results

Remediation Plans

- Results show potential success in current, next versions
- Remediation plans tell timing
- Risks updated and further Analytics to monitor risks

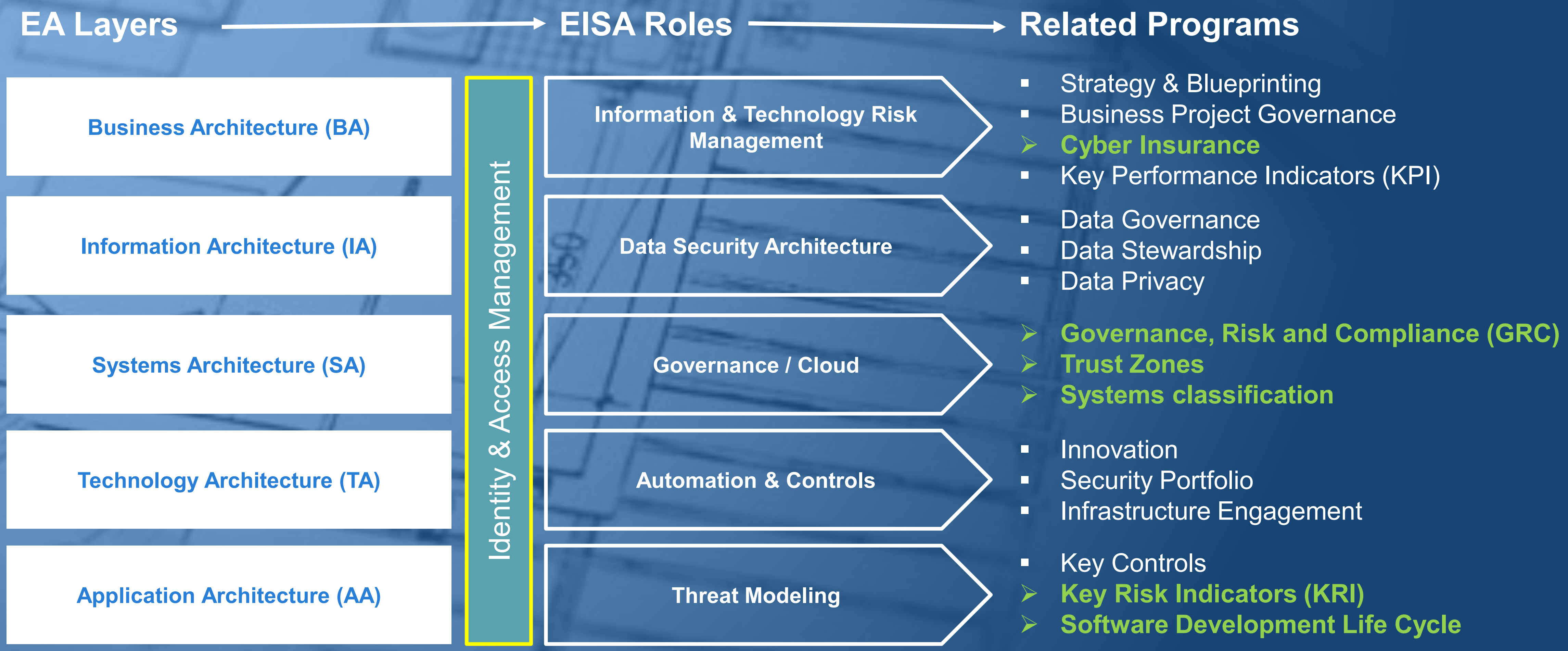
Information View – Decision Support



How will you associate threats to assets?

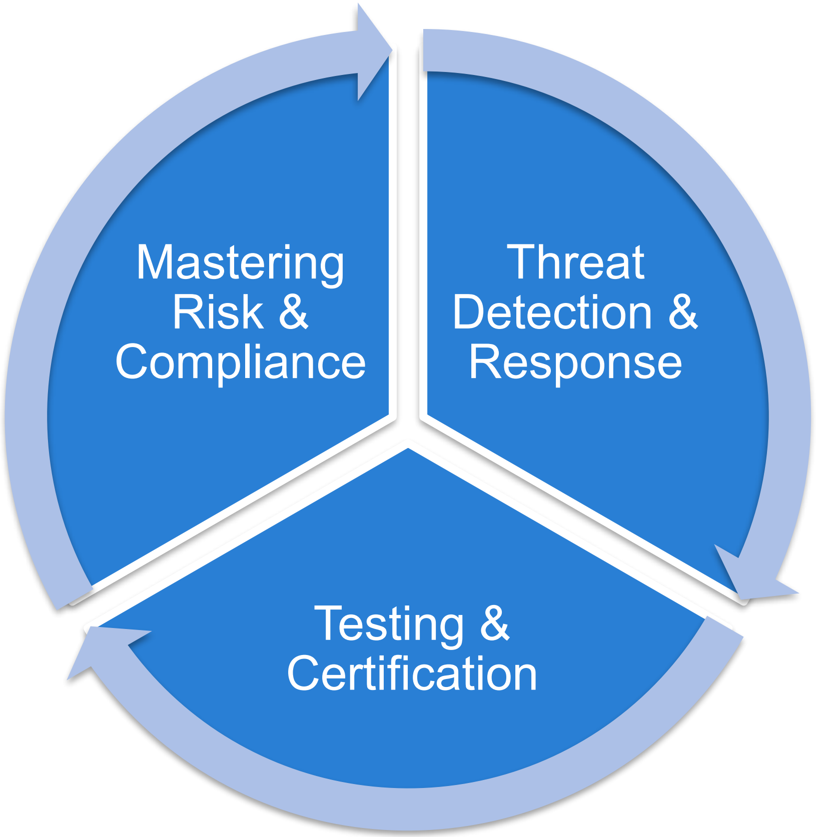
Key to Success

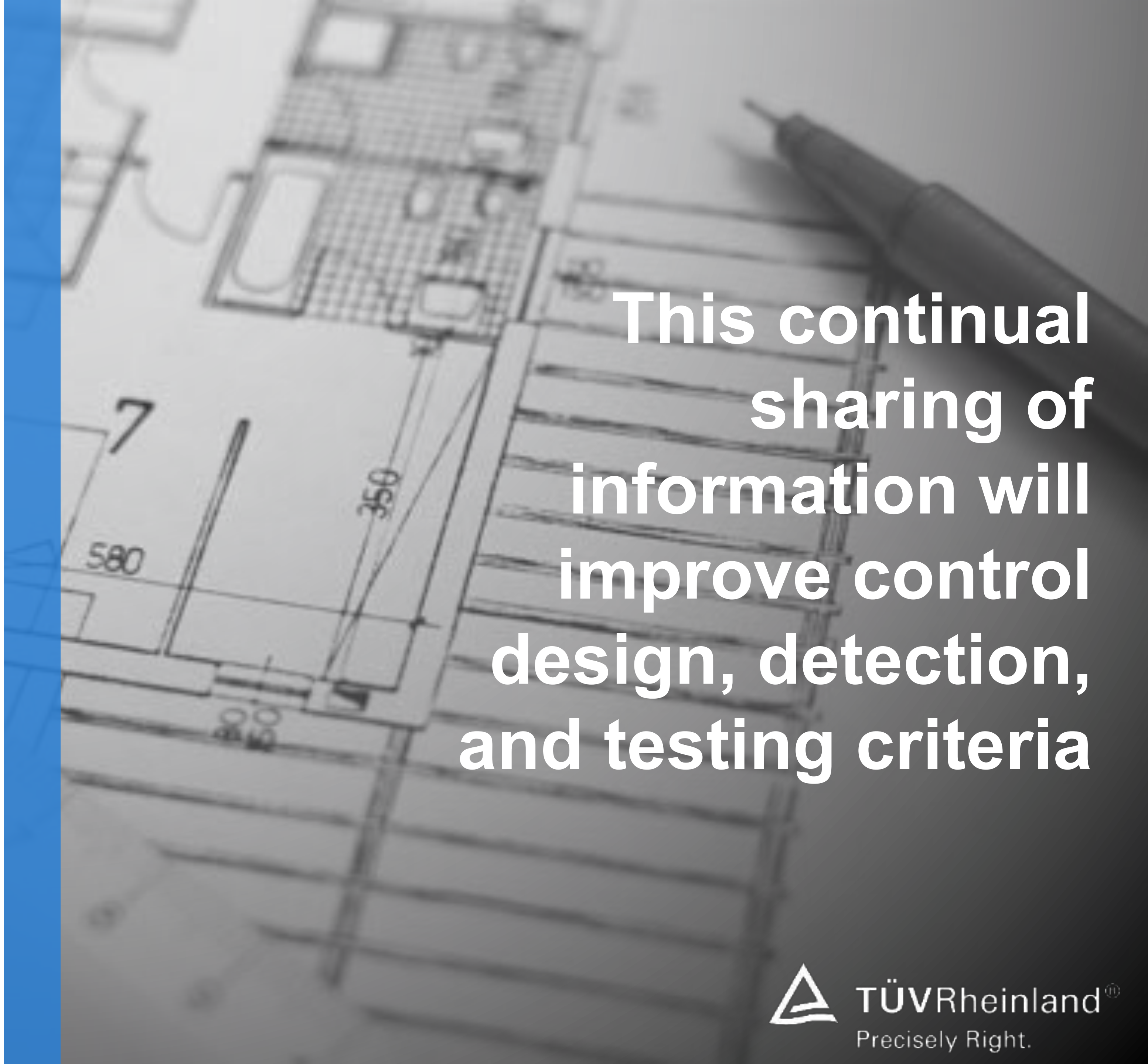
Enterprise Security Architecture



EA Layers → EISA Roles → Related Programs

EA Layers	EISA Roles	Related Programs
Business Architecture (BA)	Information & Technology Risk Management	▪ Strategy & Blueprinting ▪ Business Project Governance ➢ **Cyber Insurance** ▪ Key Performance Indicators (KPI)
Information Architecture (IA)	Data Security Architecture	▪ Data Governance ▪ Data Stewardship ▪ Data Privacy
Systems Architecture (SA)	Governance / Cloud	➢ **Governance, Risk and Compliance (GRC)** ➢ **Trust Zones** ➢ **Systems classification**
Technology Architecture (TA)	Automation & Controls	▪ Innovation ▪ Security Portfolio ▪ Infrastructure Engagement
Application Architecture (AA)	Threat Modeling	▪ Key Controls ➢ **Key Risk Indicators (KRI)** ➢ **Software Development Life Cycle**



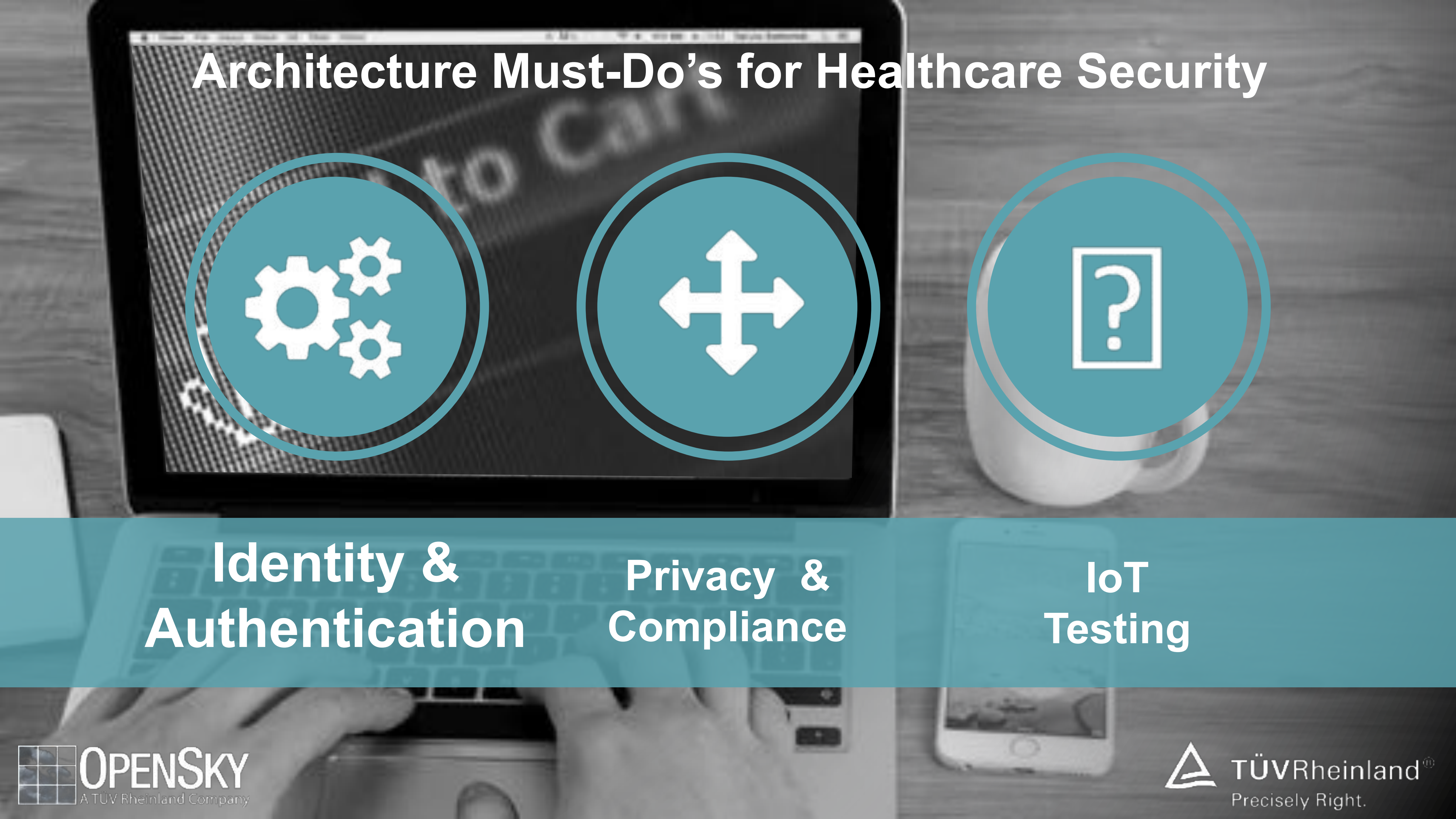


This continual sharing of information will improve control design, detection, and testing criteria

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Architecture Must-Do’s for Healthcare Security



Identity & Authentication

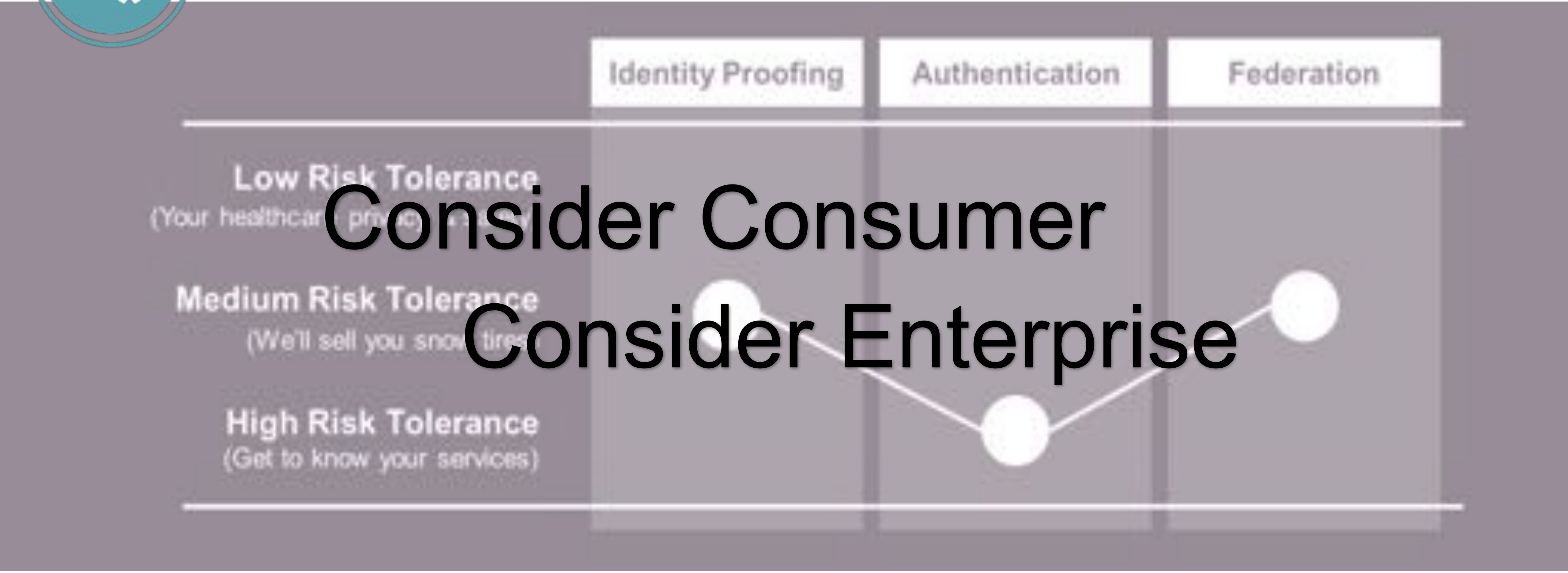
Privacy & Compliance

IoT Testing

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Healthcare Identity & Authentication



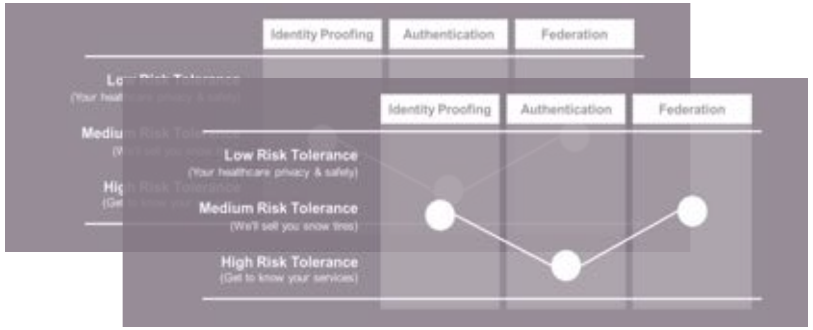
Consider Consumer

Consider Enterprise

Healthcare Identity & Authentication

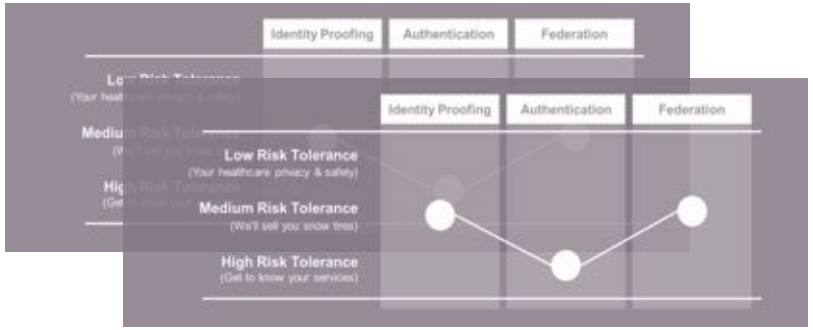
Enterprise IAM – time to centralize, clean and strengthen

- New perimeter for modern day organizations using cloud
- Controlling IaaS, PaaS, SaaS
- Privileged use – elevation of privilege findings
- M&A benefit and other collaboration enablement
- Heterogenous system integration
- Access Control for Analytics file systems
- Trust Zones for Analytics
- Policy decision and enforcement point
- Provisioning AND De-provisioning in the expanded enterprise
- Mobile *gotchas*



Healthcare Identity & Authentication

Consumer/Patient IAM – time for scale, consent and shared identities



- Modern day platforms
- NH-ISAC working group on Identity
  - SAFE BioPharma
- NSTIC working group on Healthcare
- MIFA – emphasis on linking to fraud
- EP3.org – potential governance of “Privacy Enhancing Networks”
- GPII.info – it’s like NPI but for patients and more resilient!
- FIDO – strong authentication without the pain
- UMA – User Managed Access and Consent
- FHIR – Secure API for exchanging Electronic health records.
- CHIME – Investments in interoperability

Healthcare Identity & Authentication

What happens when a source of identity itself becomes breached?

EQUIFAX

Digital Enterprises strive to provide meaningful consumer products and services with convenient channels including social, mobile, email and web.

Your approach for consumer identity management needs to be robust and diversified to overcome this broad reaching privacy loss and maintain consumer confidence. Risk-based approaches that also leverage privacy techniques need to define your identity assurance standards and technology selection.

Solutions and strategy need to be focused on three evolving areas of innovation:

- Sector based Trust frameworks and ecosystems which can transfer risk appropriately
- Privacy enhancing networks which can abstract and triangulate sources of proofing
- “Virtual in-person proofing” capabilities, which are no longer an oxymoron
- Resilient private identifiers

Healthcare Identity & Authentication

A special note on block chain potential

Blockchain is a “distributed ledger” technology instead of a hierarchical relationship.
It can create trust and maintain privacy at thee same time. There is great debate on how it can help with shared identities. While not a silver bullet, it should be thought of as a transactional model for B2B and B2B2C. Governance of entities and APIs is required – this is not a new endeavor. Some serious considerations:

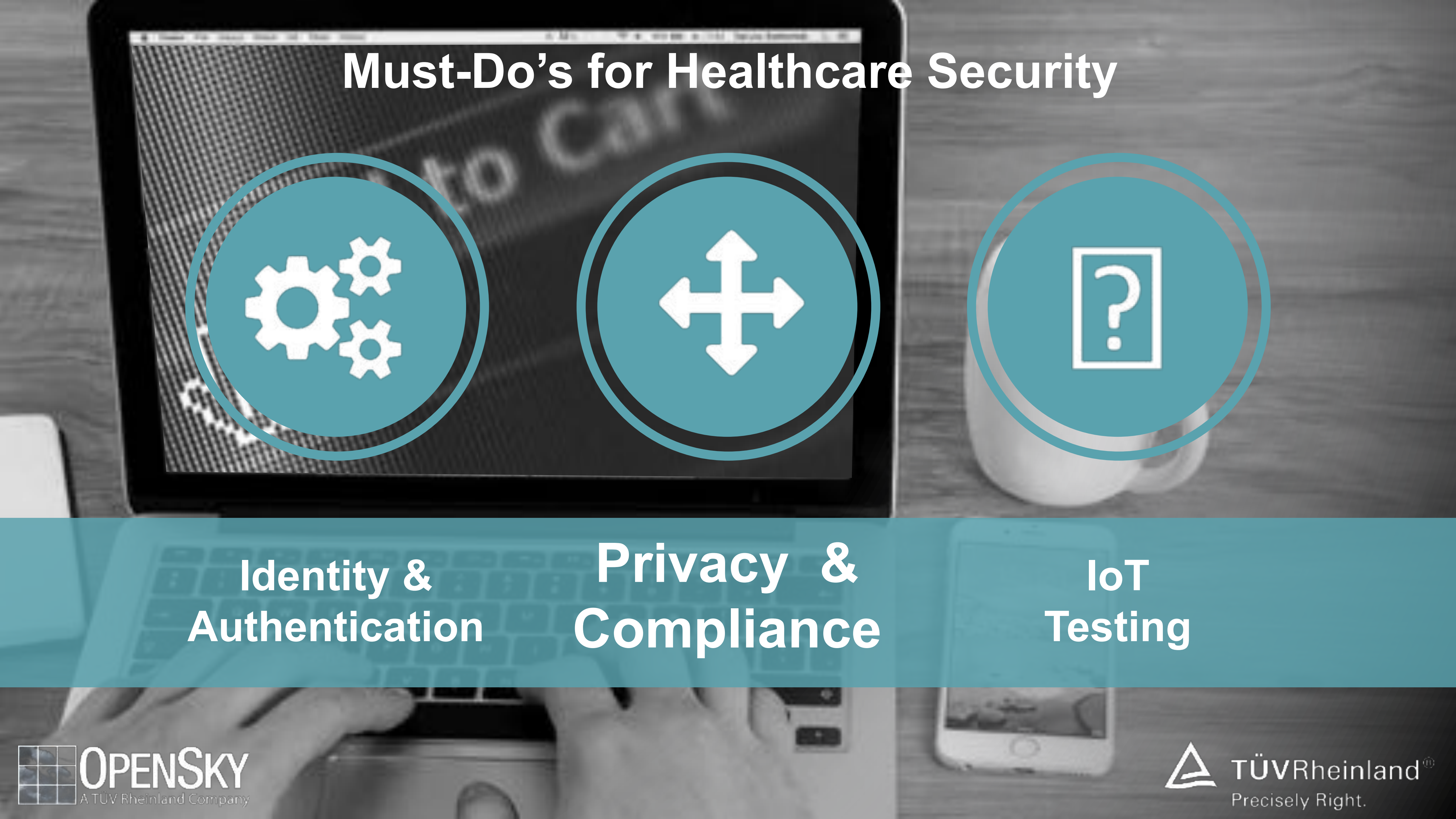
Pharma Supply Chain

- Real-time visibility to the entire product path both up or down the supply chain.
- Immutable track of the movement and state of drugs from its origin to the end consumer.
- Prevention of counterfeit drugs by validating its proof of existence in the chain.
- Avoidance of prescription drug abuse.

Clinical Trials Data

- Traceable and Transparent record of Patients consent that can never be repudiated.
- Privacy and anonymity in data sharing that drives more consumers to the platform.
- Immutable chaining of clinical trial steps for provenance of methodology followed.
- Voluminous data held in secured locks protecting it from any kind of data manipulation.

Must-Do’s for Healthcare Security



Identity & Authentication

Privacy & Compliance

IoT Testing

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Healthcare Privacy & Compliance

Innovation in Consumer centered solutions (supports GDPR)

- Advanced Encryption and Key Management
- De-Identification: Virtual identifiers, Tokenization
- Consumer managed Access and Consent
- Privacy Enhancing Networks (Blockchain can fit here)

Global compliance / GRC

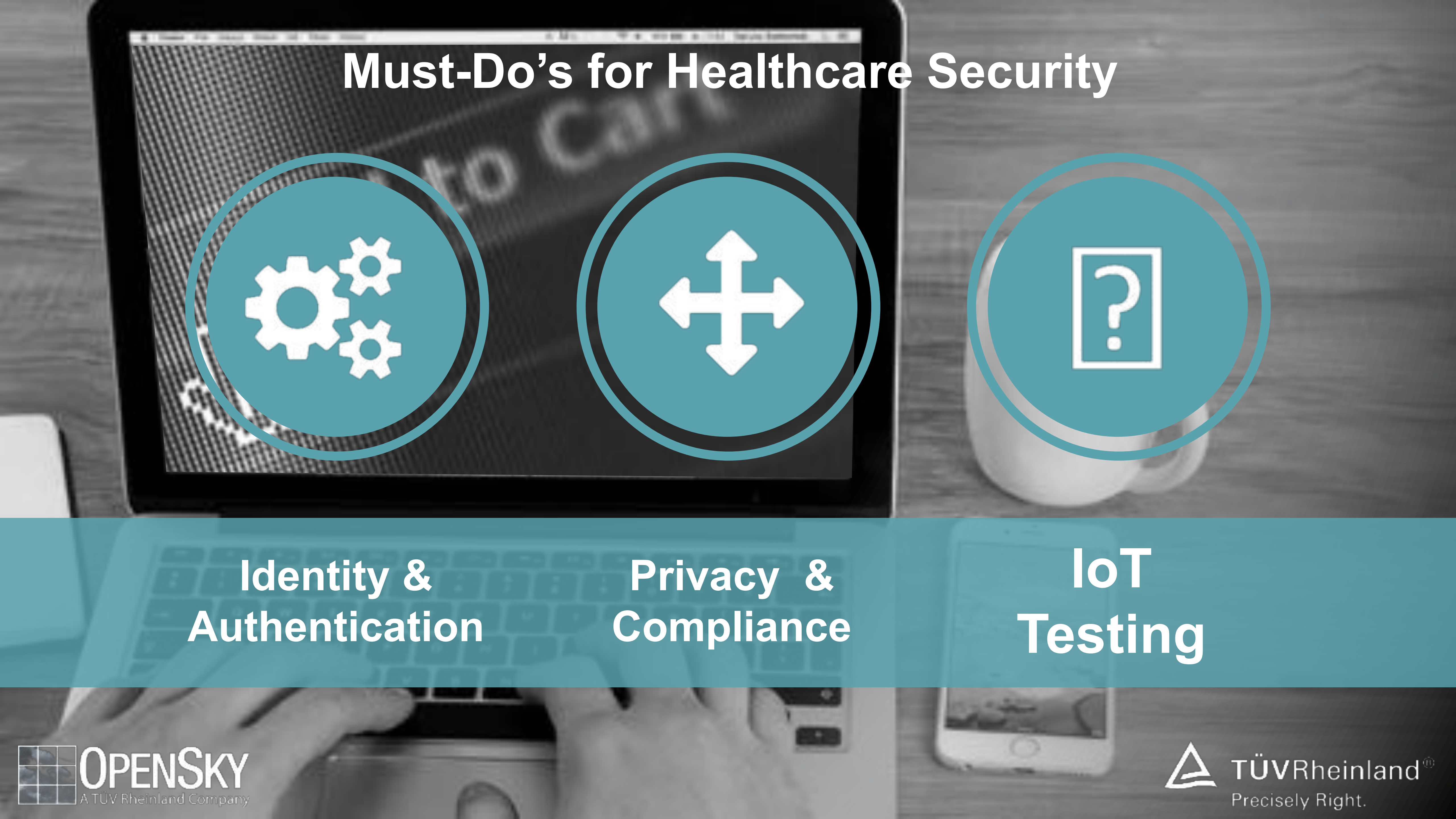
- Policy Management Hierarchy
- Authoritative source mappings (prove once comply many)
- Compliance Auditing / Assurance (audit or even better KPIs)
- GDPR Certifications including IoT ecosystems

Healthcare Privacy & Compliance

Data Governance – the key to empowered Business control of Cloud

- Coordinated Charters between CDO, IT and Security (Data Governance Institute)
- Data Discovery / Master Data Management
- Data Accuracy Retention and erasure
- Data Loss Prevention (including cloud)
- Cloud Governance
- Data Labeling & Classification - Watch for layered data!

Must-Do's for Healthcare Security



Identity & Authentication

Privacy & Compliance

IoT Testing

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Healthcare IoT Testing - Consumer

Risk Factors

Dependence

Impact

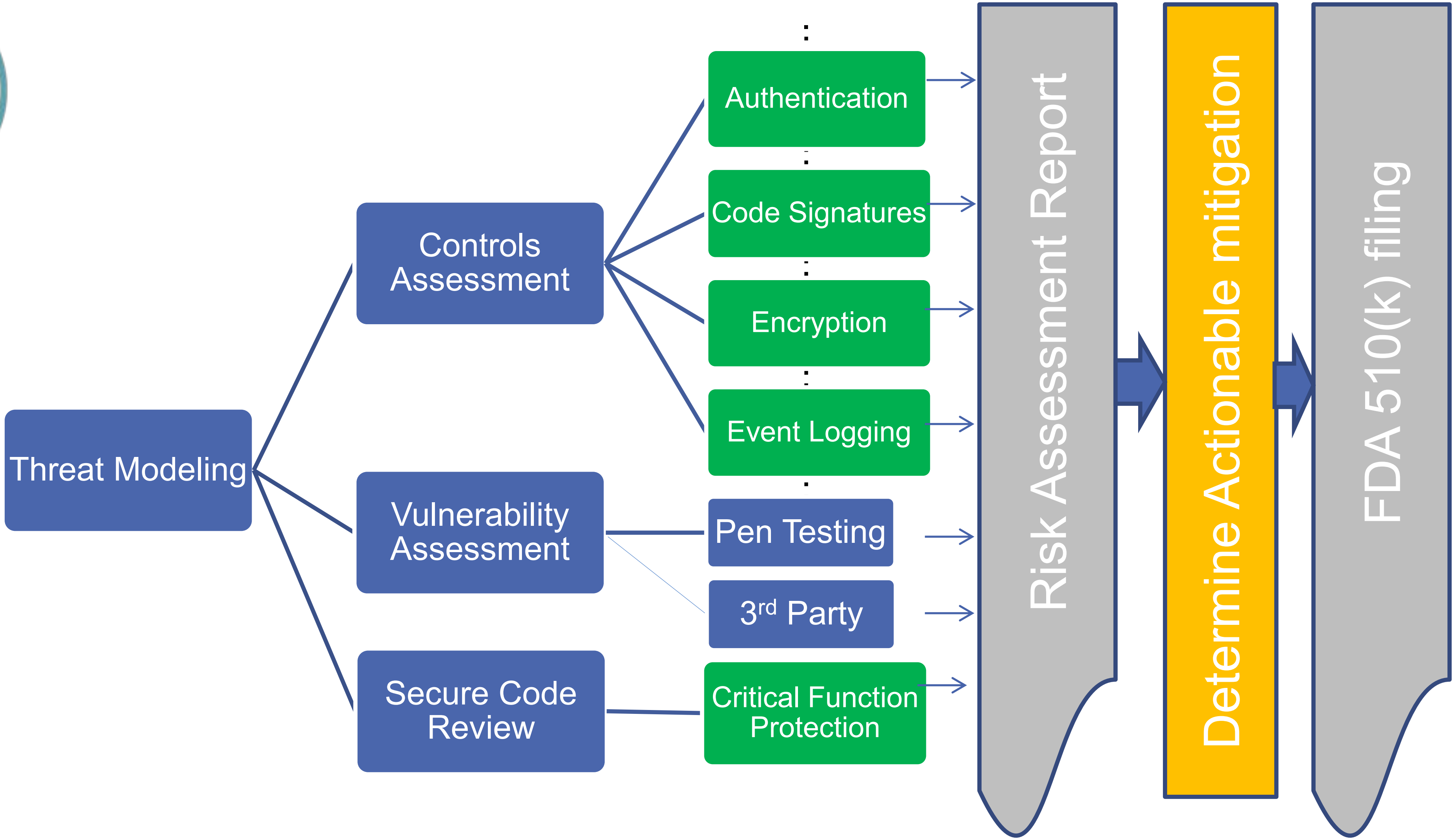
Complexity

Ecosystem

IoT is defined by the Consumer Technology Association across 26 marketplaces:

- Education
- eCommerce
- Family
- Fitness
- Gaming
- Health
- Kids
- Sports
- Vehicles
- …many more

Healthcare IoT Testing – FDA Guidelines Pre-Market



Threat Modeling

Controls Assessment

Authentication

Code Signatures

Encryption

Event Logging

Vulnerability Assessment

Pen Testing

3rd Party

Secure Code Review

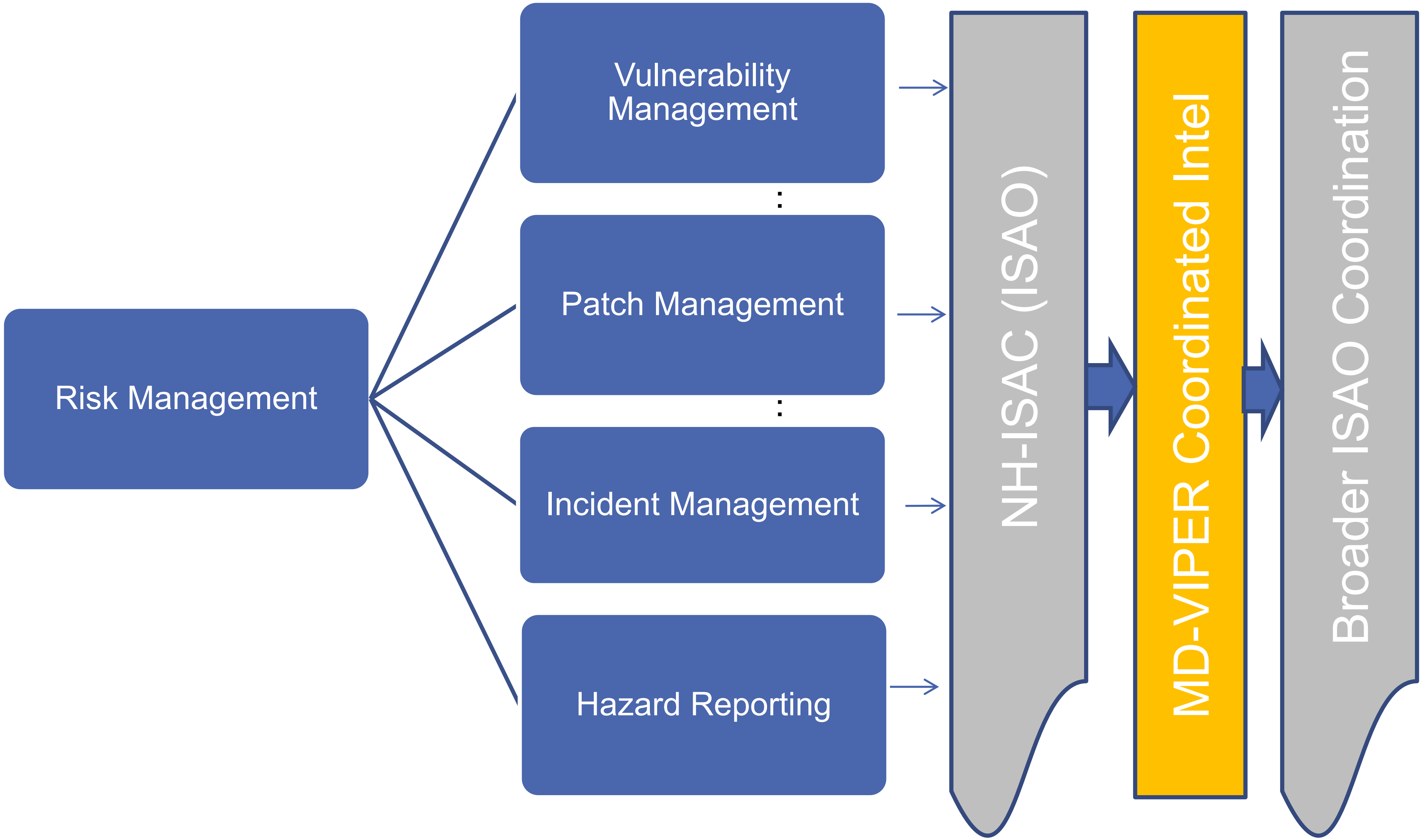
Critical Function Protection

Risk Assessment Report

Determine Actionable mitigation

FDA 510(k) filing

Healthcare IoT Testing – FDA Guidelines Post Market



Healthcare IoT Testing – frameworks

Privacy +

- GDPR
- HIPAA
- FIPPS

Security +

- Controls (NIST CSF, NIST 800-53)
- Threats (STRIDE, OCTAVE, STIX)
- Risk (OCEG, FAIR, ISO 31000)
- Program (ISO 27000, COBIT 5)

Safety

- ISO 14971
- IEC 62443, 60601-1
- DTSec (Diabetes Technology Society – closed loop systems)

The ransomware challenge

Preventative + Detective + Response

Preventative

- Trust Zones
- Consolidated IAM
- ActiveDirectory hygiene
- PIM/PAM
- Configuration Mgt.

Detective

- Egress monitoring
- Analytics
- Threat Intelligence

Response

- High grade isolated backup / recovery (with test plan)
- Incident Response drills
- Relationship with local Authorities

Take Home Message

Get a grip on priorities based on threats

- Master Risk
- Leverage Security Analytics
- Tie to testing criteria
- Response / Recovery

Emphasize capabilities that enable Healthcare 2.0

- Identity
- Privacy
- Safe Analytics
- IoT trustworthiness

Key Takeaway

- Expect solutions - Charter Security Architecture
- Demand Risk management decision support
- Get involved with an ISAO (NH-ISAC et al)

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.