Metrics that Matter

Help Management with Decision Making and Improve Security Posture of the Organization.

SANAZ SADOUGHI

INTERNATIONAL MONETARY FUND

Metricon X Summit – March, 2019

Disclaimer

The views expressed herein are those of the speaker and should not be attributed to the IMF, its Executive Board, or its Management.

Who We Are and Why Do We Care?

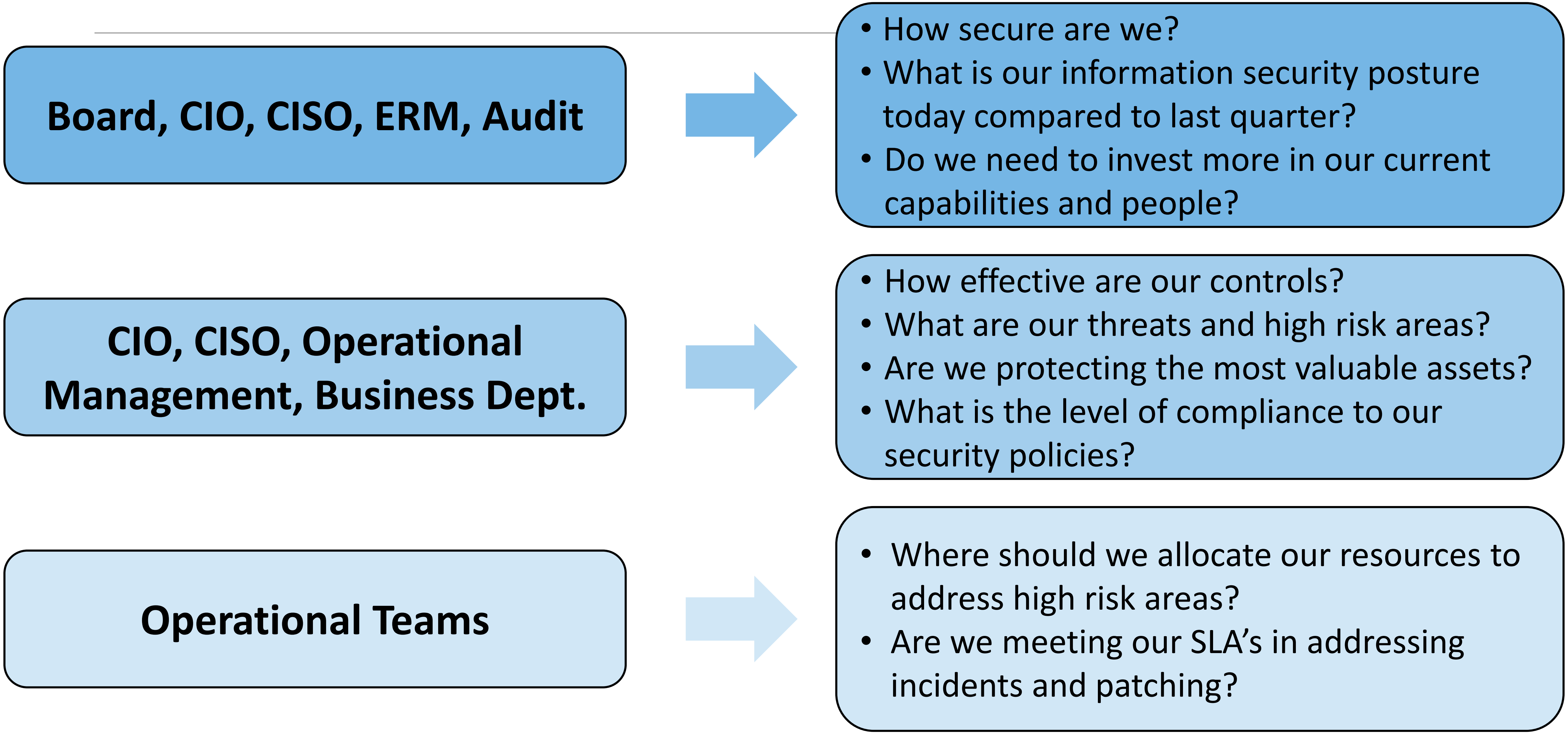
189 member countries

Lending

Capacity Development

Surveillance

Uneasy Questions



Board, CIO, CISO, ERM, Audit

- How secure are we?
- What is our information security posture today compared to last quarter?
- Do we need to invest more in our current capabilities and people?

CIO, CISO, Operational Management, Business Dept.

- How effective are our controls?
- What are our threats and high risk areas?
- Are we protecting the most valuable assets?
- What is the level of compliance to our security policies?

Operational Teams

- Where should we allocate our resources to address high risk areas?
- Are we meeting our SLA’s in addressing incidents and patching?

How to Answer

Multiple systems of information

Data collections / cleansing

Lagging and leading indicators

Relevant

Manual processing

Manual analysis

Silo reporting

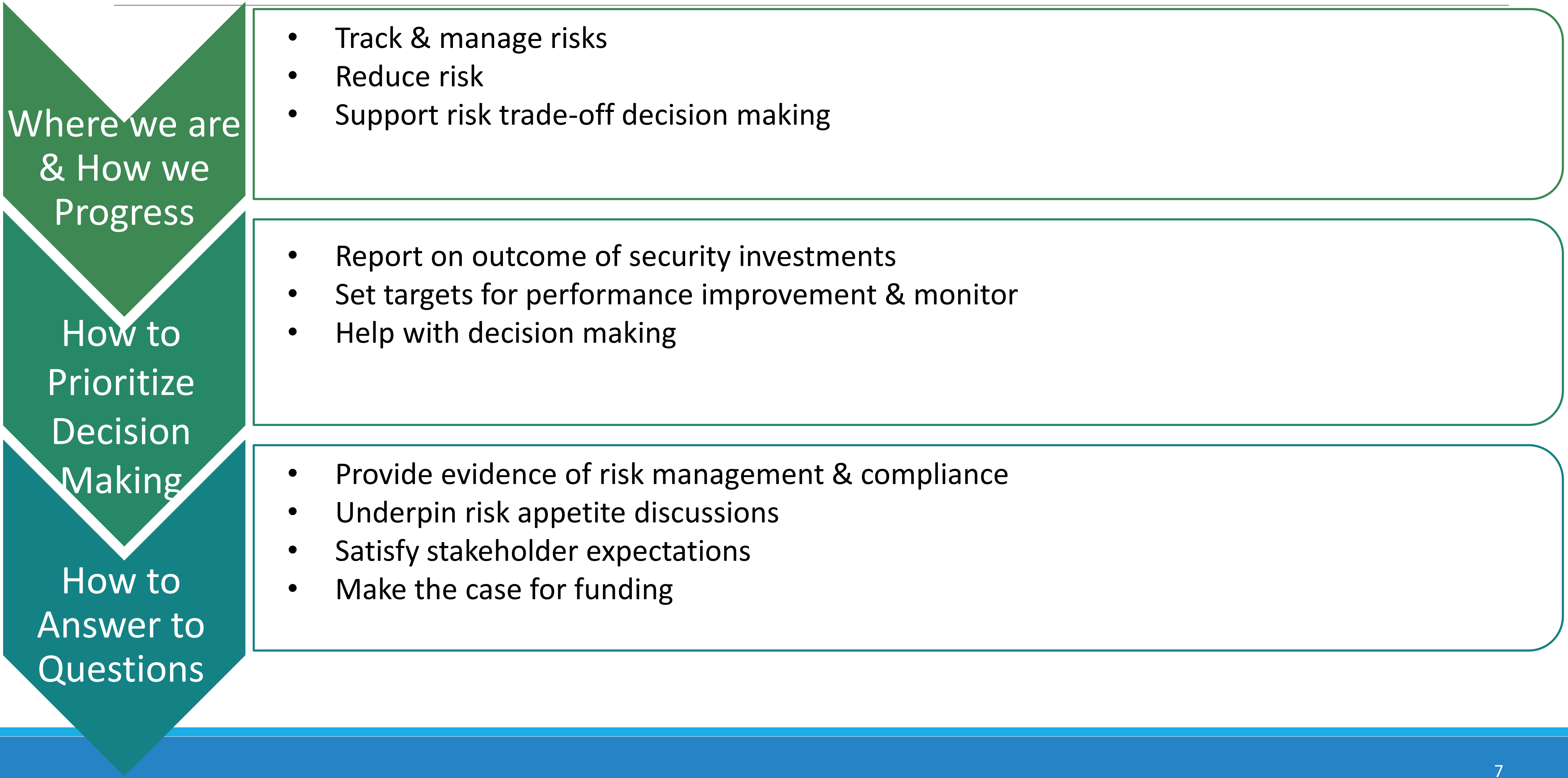
Impactful

Actionable

Different audiences

=

Our Goal



Where we are & How we Progress

- Track & manage risks
- Reduce risk
- Support risk trade-off decision making

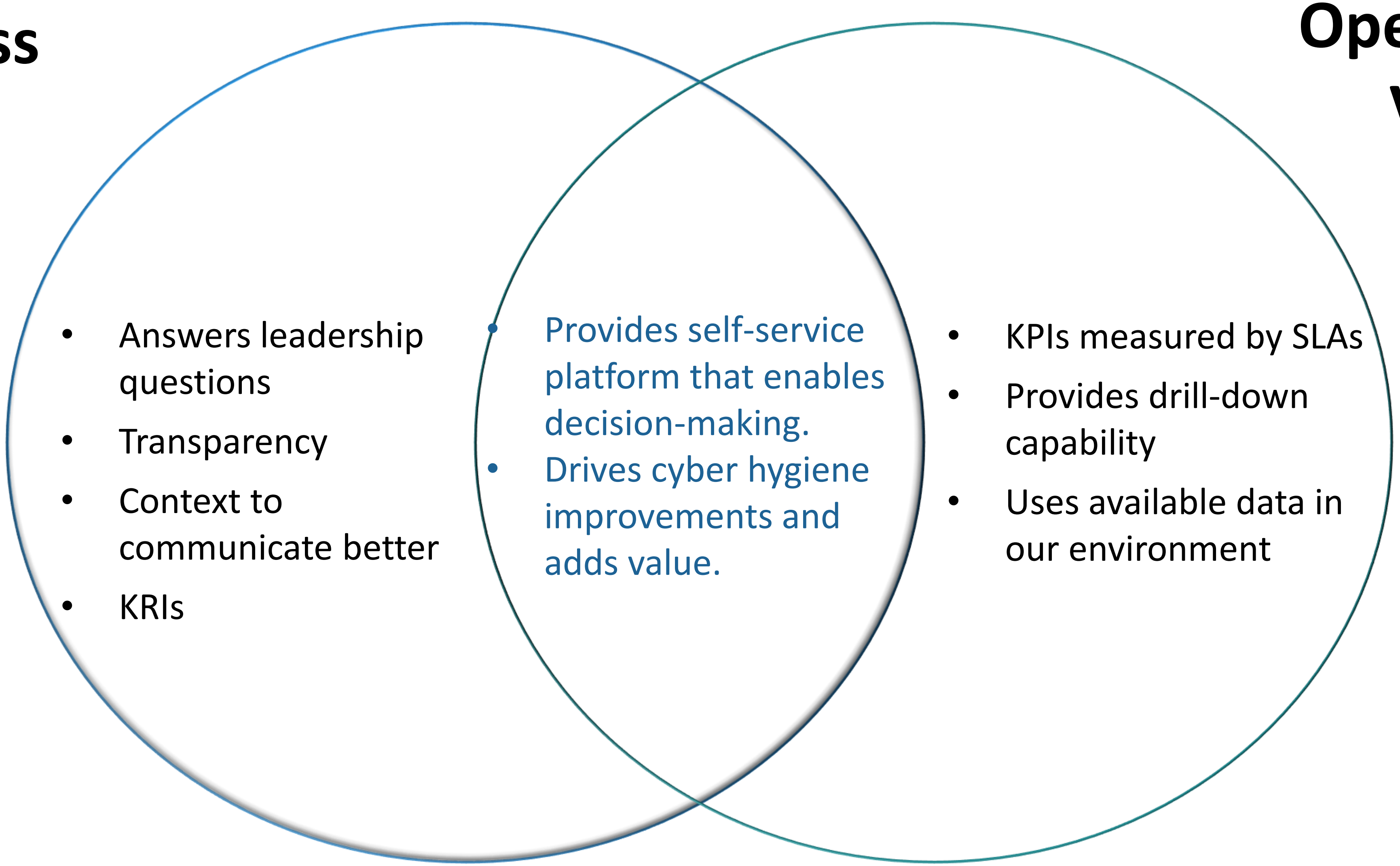
How to Prioritize Decision Making

- Report on outcome of security investments
- Set targets for performance improvement & monitor
- Help with decision making

How to Answer to Questions

- Provide evidence of risk management & compliance
- Underpin risk appetite discussions
- Satisfy stakeholder expectations
- Make the case for funding

Our Proposed Vision



Business Value

- Answers leadership questions
- Transparency
- Context to communicate better
- KRIs

Operational Value

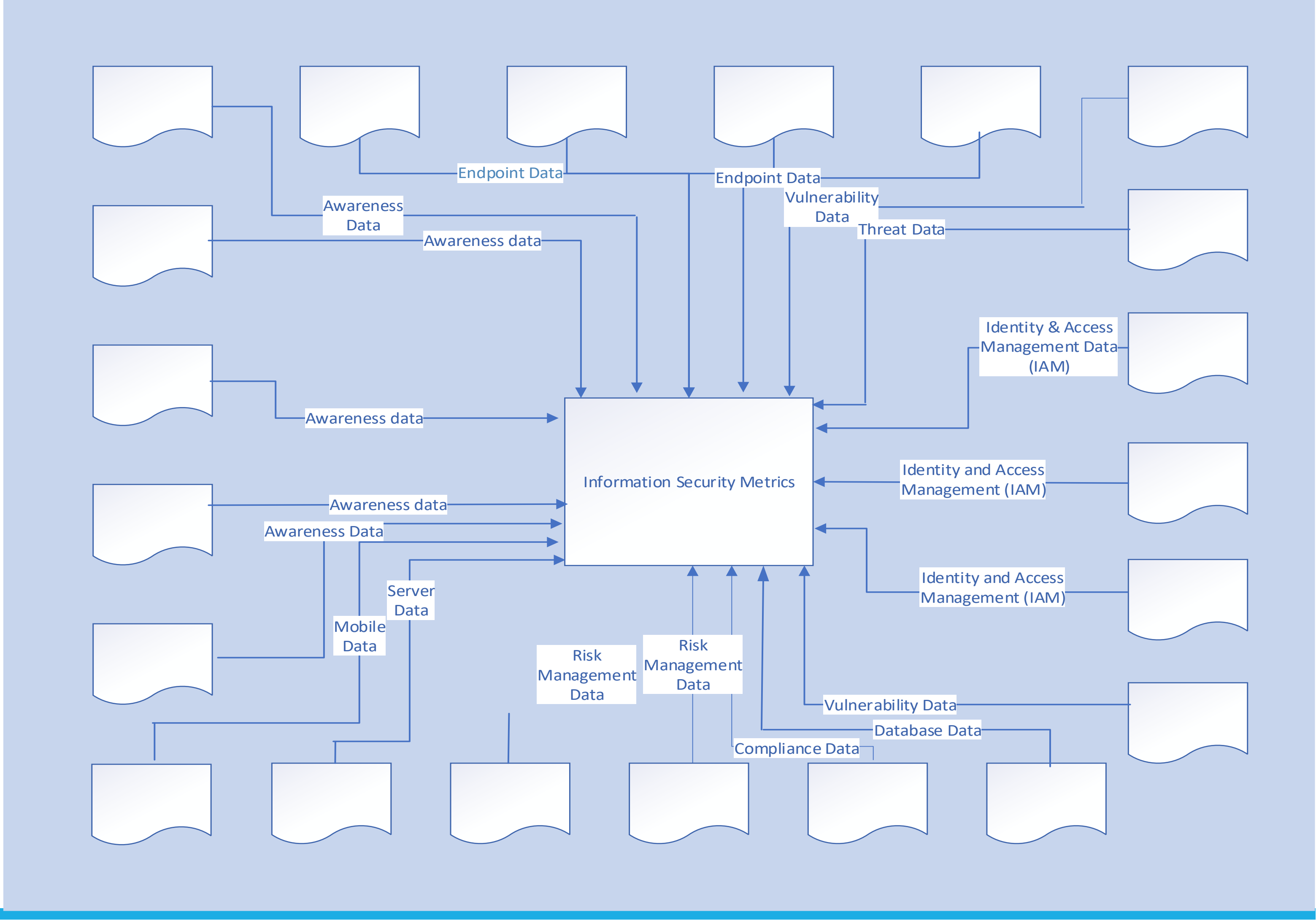
- KPIs measured by SLAs
- Provides drill-down capability
- Uses available data in our environment

- Provides self-service platform that enables decision-making.
- Drives cyber hygiene improvements and adds value.

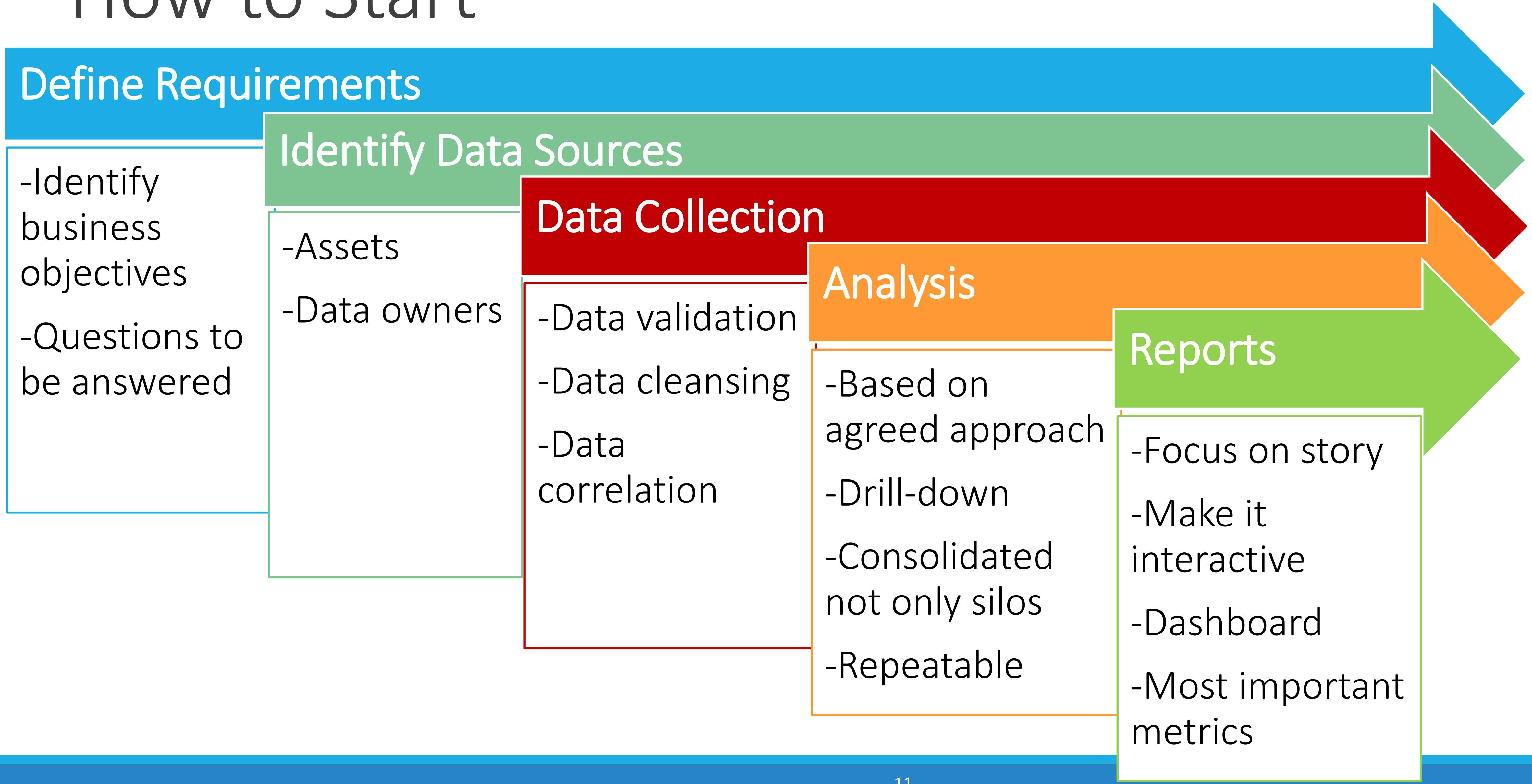
Overview of the Information Security Metrics Program (ISMP)

Where Are We Today

- Metrics on 7 domains
- Using 21 source systems
- Monthly reports
- CIO, CISO, Operational Teams, ERM, Audit



How to Start



Define Requirements

-Identify business objectives

-Questions to be answered

Identify Data Sources

-Assets

-Data owners

Data Collection

-Data validation

-Data cleansing

-Data correlation

Analysis

-Based on agreed approach

-Drill-down

-Consolidated not only silos

-Repeatable

Reports

-Focus on story

-Make it interactive

-Dashboard

-Most important metrics

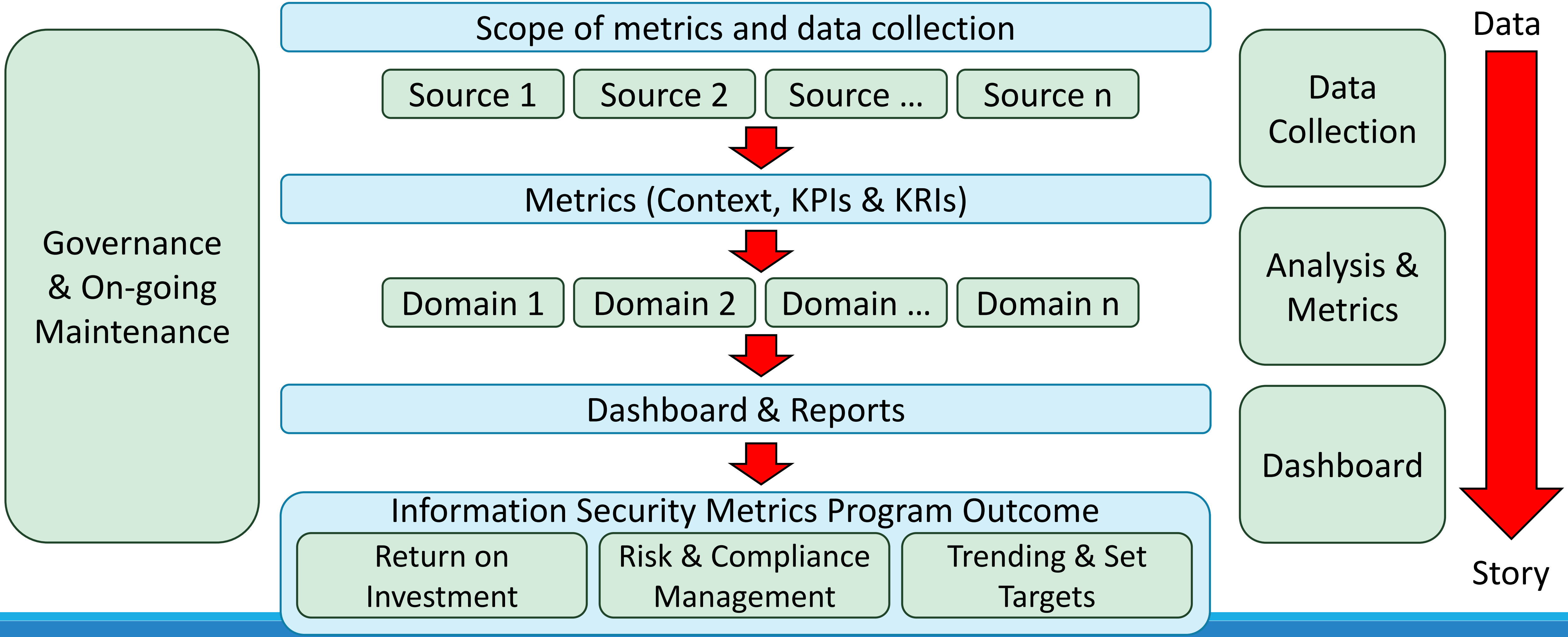
Objectives of the ISMP

The Implementation of an Information Security Metrics Program (ISMP) allows the organization to:

- Effectively communicate security posture
- Demonstrate the value of the security investment
- Drive performance improvement
- Help prioritize decision making
- Manage risk and compliance
- Provide quantitative measurements

The ISMP Framework

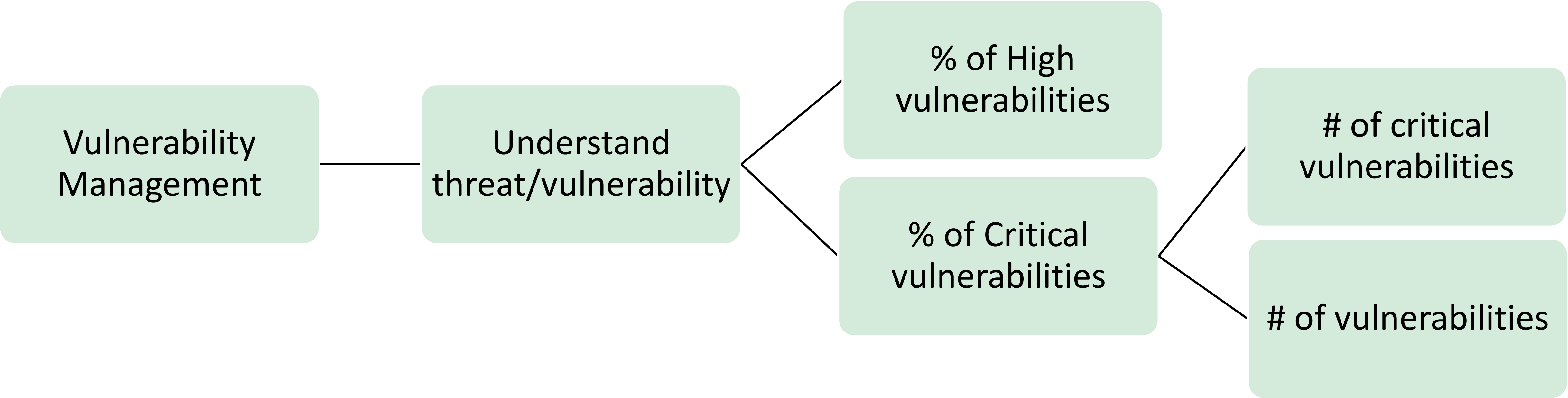
The stakeholder questions can be answered through an ISMP framework below:



Metrics Hierarchy

The metrics catalog has been designed based on the following hierarchy:

Domain → **Outcome** → **Metric** → **Raw Data**



Vulnerability Management

Understand threat/vulnerability

% of High vulnerabilities

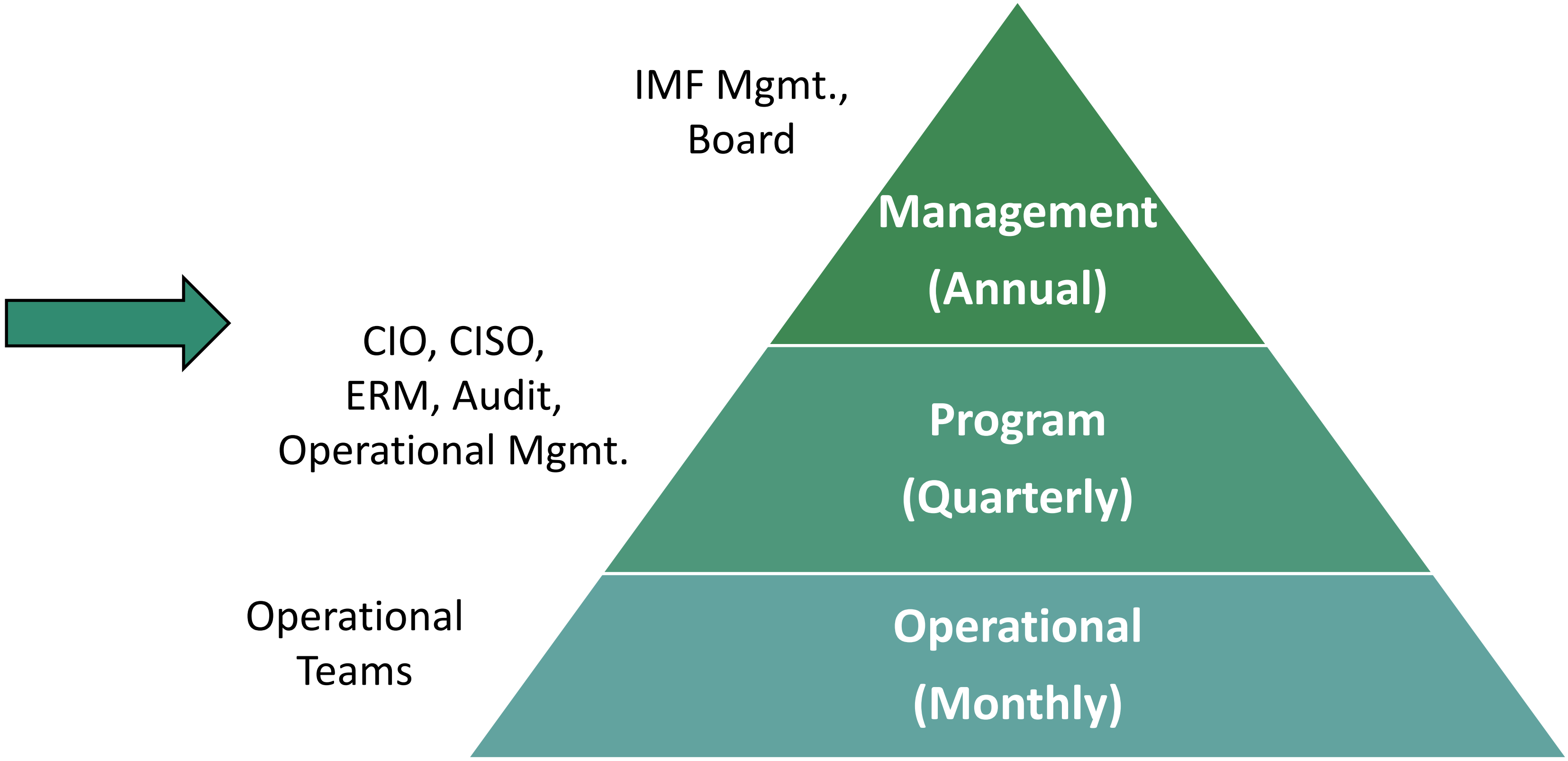
% of Critical vulnerabilities

# of critical vulnerabilities

# of vulnerabilities

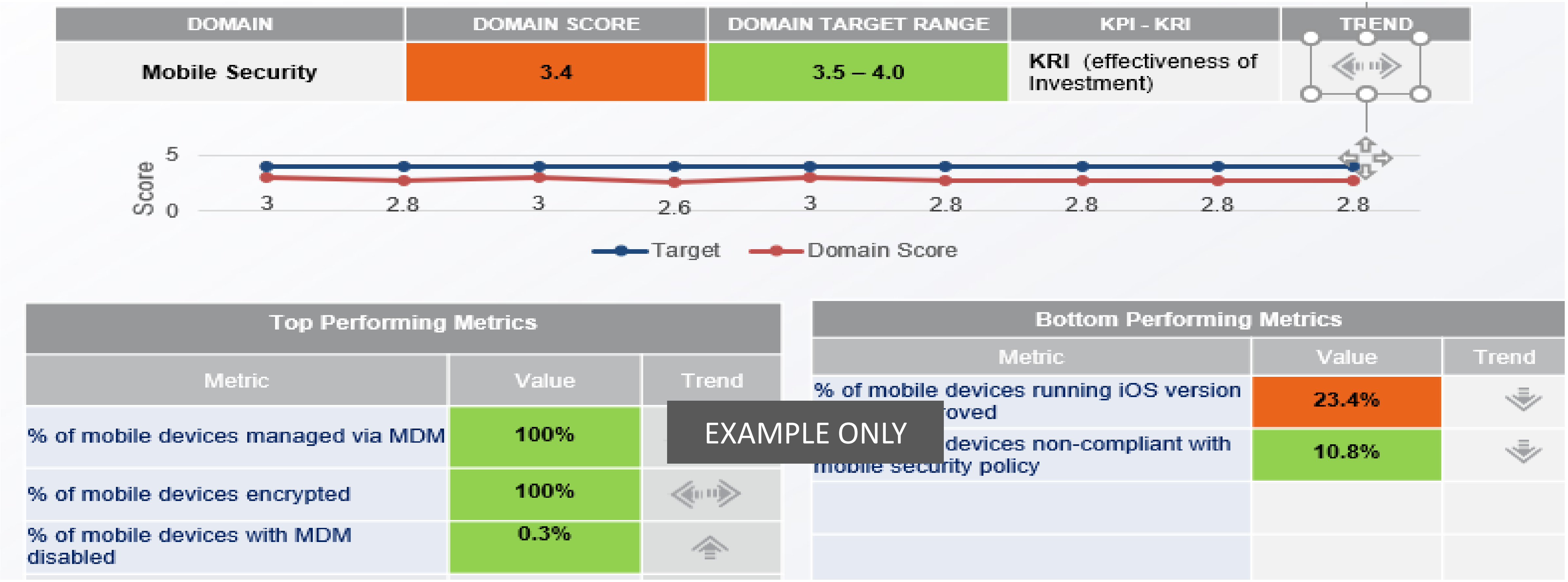
Domains & Reporting

Domains
1. Security Awareness
2. Vulnerability Management
3.Compliance Management
4. Risk Management
5. Identity & Access Management
6. Threat & Incident Management
7. Security Technologies



Program Level Dashboard

These reports will be reviewed on a monthly basis to take action.



DOMAIN	DOMAIN SCORE	DOMAIN TARGET RANGE	KPI - KRI	TREND
Mobile Security	3.4	3.5 – 4.0	KRI (effectiveness of Investment)	⇔

Top Performing Metrics		
Metric	Value	Trend
% of mobile devices managed via MDM	100%	[illegible]
% of mobile devices encrypted	100%	⇔
% of mobile devices with MDM disabled	0.3%	⇑

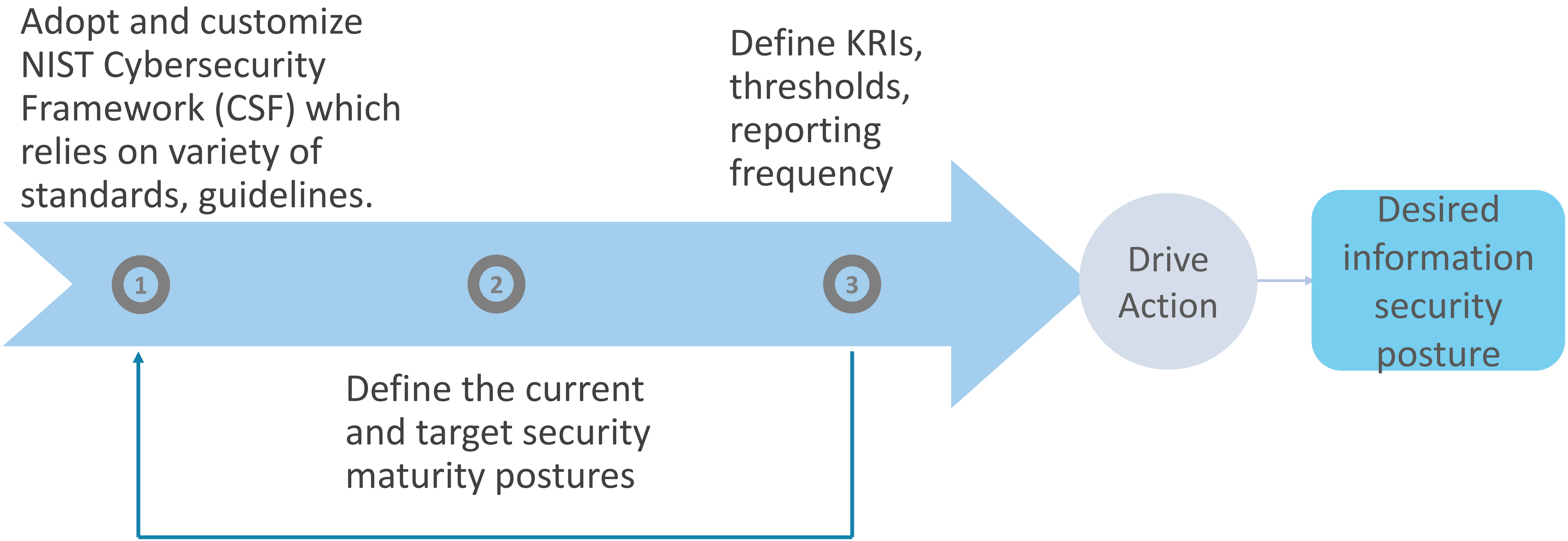
Bottom Performing Metrics		
Metric	Value	Trend
% of mobile devices running iOS version [illegible]oved	23.4%	⇓
[illegible] devices non-compliant with mobile security policy	10.8%	⇓

EXAMPLE ONLY

Revised Metrics & KRIs

Tailored to audience and Agreed on what's important -
Iterative testing of what works

Measure Security Posture Using NIST CSF



Adopt and customize NIST Cybersecurity Framework (CSF) which relies on variety of standards, guidelines.

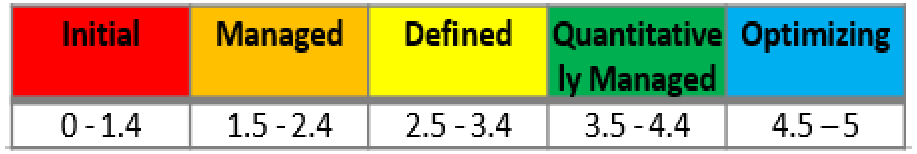
Define KRIs, thresholds, reporting frequency

Define the current and target security maturity postures

Detect

Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Function	Domain/Category	Maturity
Detect (DE)	Anomalies and Events	2.9
	Security Continuous Monitoring	2.3
	Detection Processes	2.2



Initial	Managed	Defined	Quantitatively Managed	Optimizing
0 - 1.4	1.5 - 2.4	2.5 - 3.4	3.5 - 4.4	4.5 – 5

Domain	Metric	Low	Medium	High	Critical	KRI Score
Vulnerability Management (Detection Processes)	% of critical vulnerabilities on **most-exposed** infrastructure	< 5%	< 10%	< 20%	>= 20%	4
	% of critical vulnerabilities on **internal** infrastructure	< 25%	< 50%	< 75%	>= 75%	3

Risk Statement

Vulnerabilities in the assets can be exploited & led into information disclosure, financial loss, etc.

Proposed Actions

Remediate critical vulnerabilities

EXAMPLE ONLY

Crown Jewels

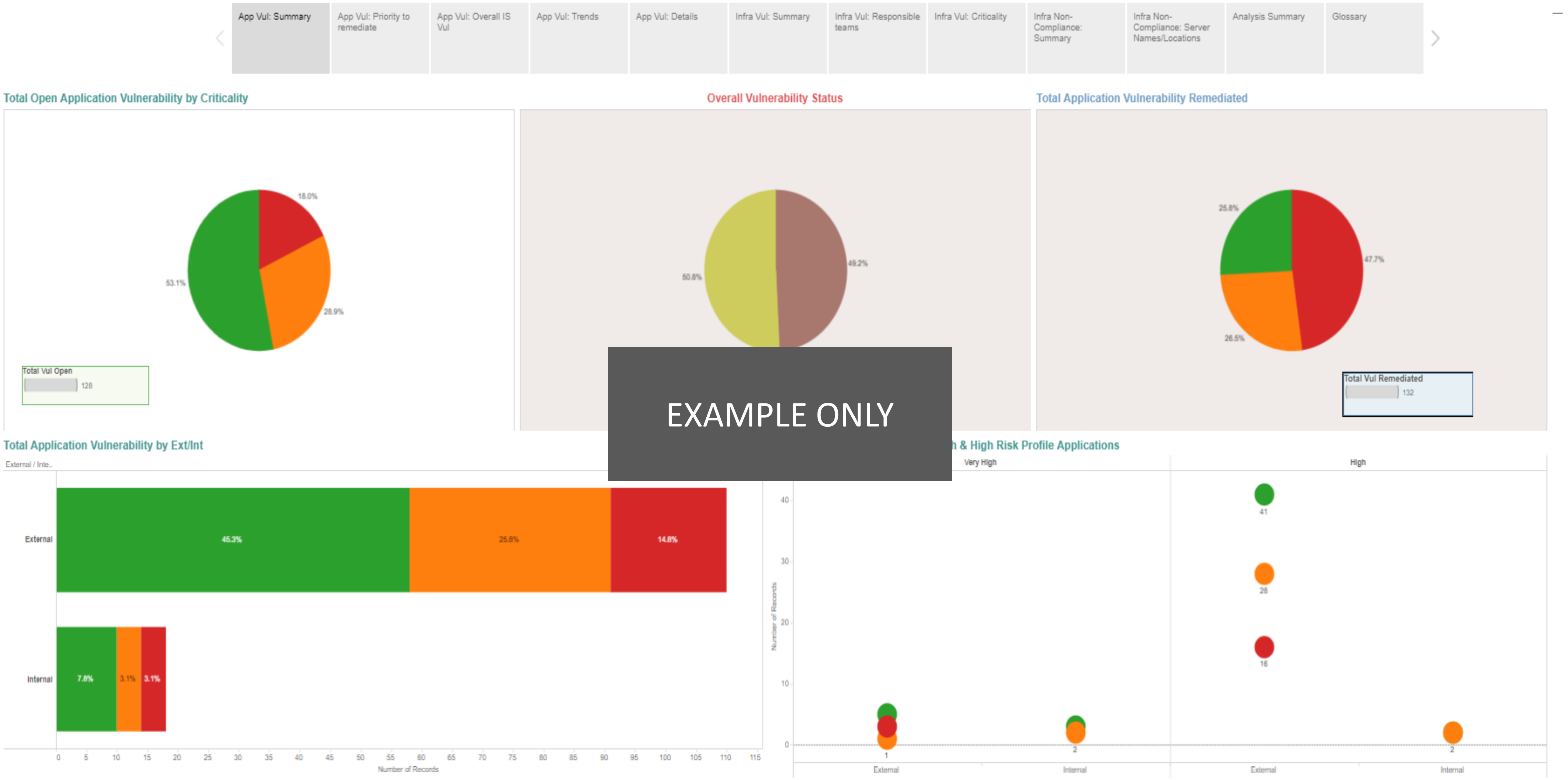
Create metrics dashboards for Crown jewels

- Identify the sensitive information assets
- Identify the most critical infrastructure and applications

Prioritize vulnerability assessment and remediation

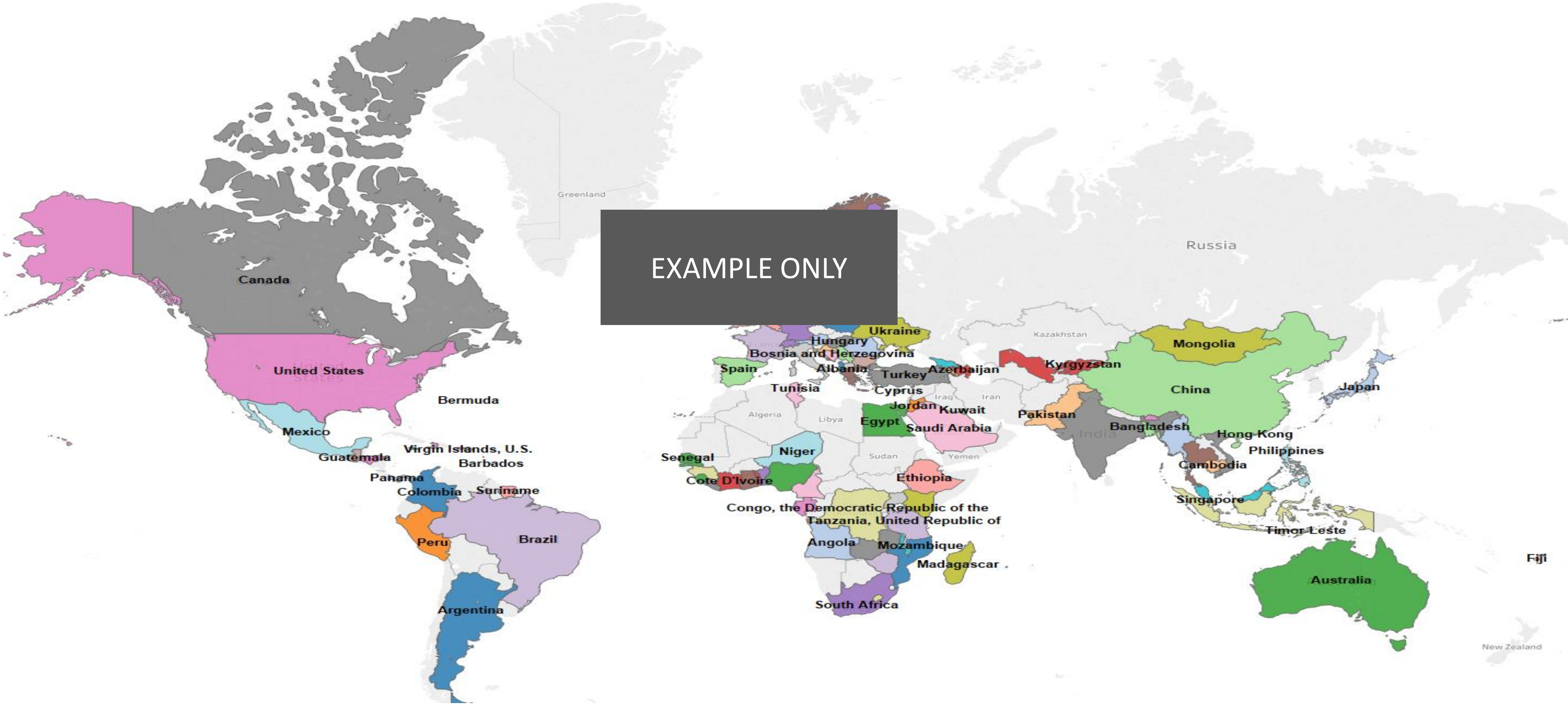
Prioritize compliance assessment and remediation

Demo of Metrics & Dashboards



EXAMPLE ONLY

Demo of User Behavior Analysis



EXAMPLE ONLY

IMF Next Steps

- Automation and reduce overhead
- Focus more on context and analysis
- Stakeholder iterative input to refine KRI’s
- Align to NIST CSF (quantitative and qualitative) measures
- Report on actions taken and impact

Next Steps – How you to Apply

Next Month:

- Identify your organizations’ key questions
- Define your requirements and what resonates with your audience

In the first 3 Months:

- List your data sources
- Define potential metrics to start with

Within 6 Months:

- Create sample reports
- Identify quick wins

Thank You!

Sanaz Sadoughi

sskhosroshahi@imf.org

International Monetary Fund