Measuring Maturity and Effectiveness

KPIs, Measurements and Metrics

Chris Andes

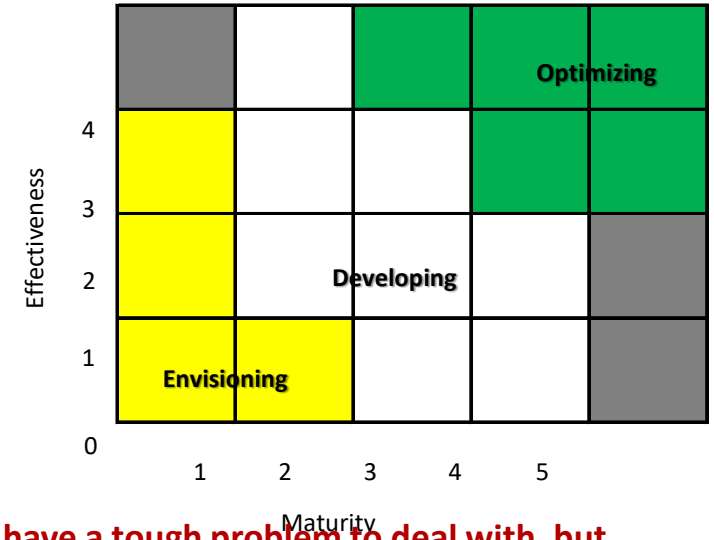
Why are We Here?

At the end of this presentation/Practical Application you'll understand the importance and use of metrics, measurements and KPIs; which will enable you to:

- Track the effectiveness and maturity of your application or service
- Demonstrate value
- Identify opportunities

Why Metrics are Important

- **Measure effectiveness**
- **Monitor maturity**
- **Demonstrate value**



"The Measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year"

- Sec of State John Foster Dulles

Definitions

Measurement: Point in time data

Metric: Data over time (trending)

KPI: Performance metrics that show progress towards a goal

Qualitative or Quantitative?

How they typically fail

- Lack of leadership support
- Too much information, too soon
- Wrong information
- Inaccurate, misleading or incomplete information
- *What is the story you are trying to tell*

Key components of metrics

- Measure performance using baselines and trends
- Monitor progress towards a stated goal
- Help metric owner communicate value
- Facilitate the use of data for decision making
- Be closely aligned with business objectives
- Aligned to service definitions

Designed for the Audience

Strategic Objectives

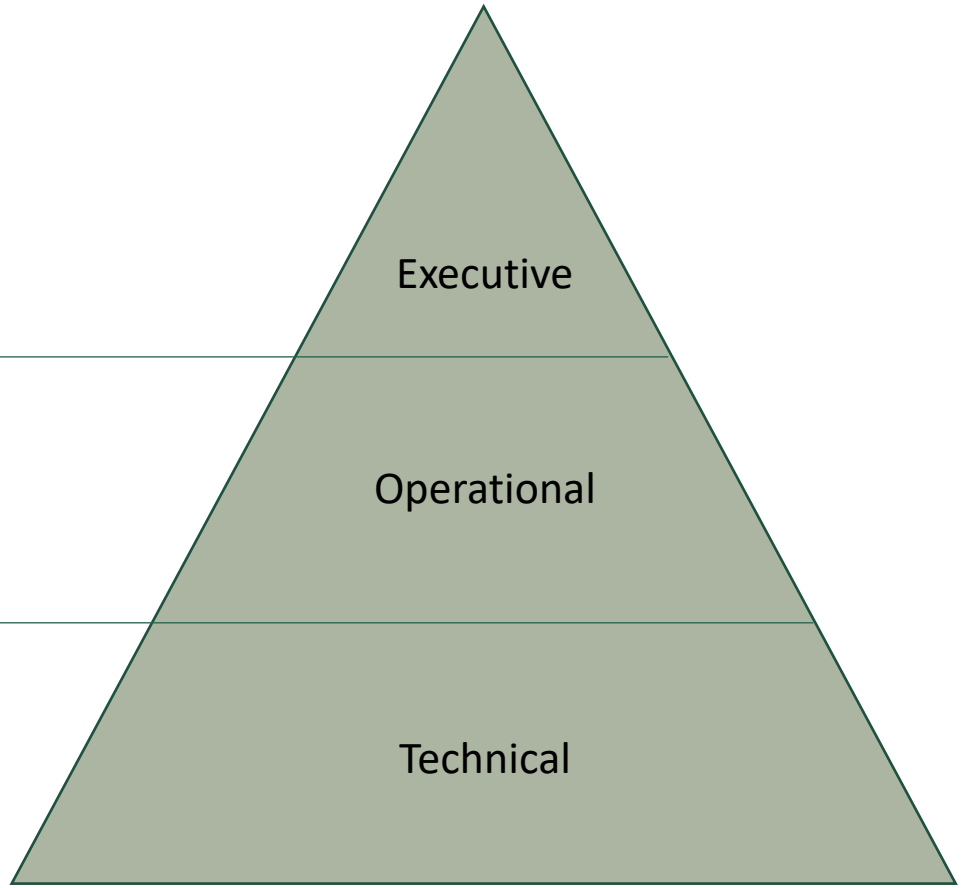
KPIs

Analysis and Trends

Metrics

Data

Measurements



Designed for the Audience

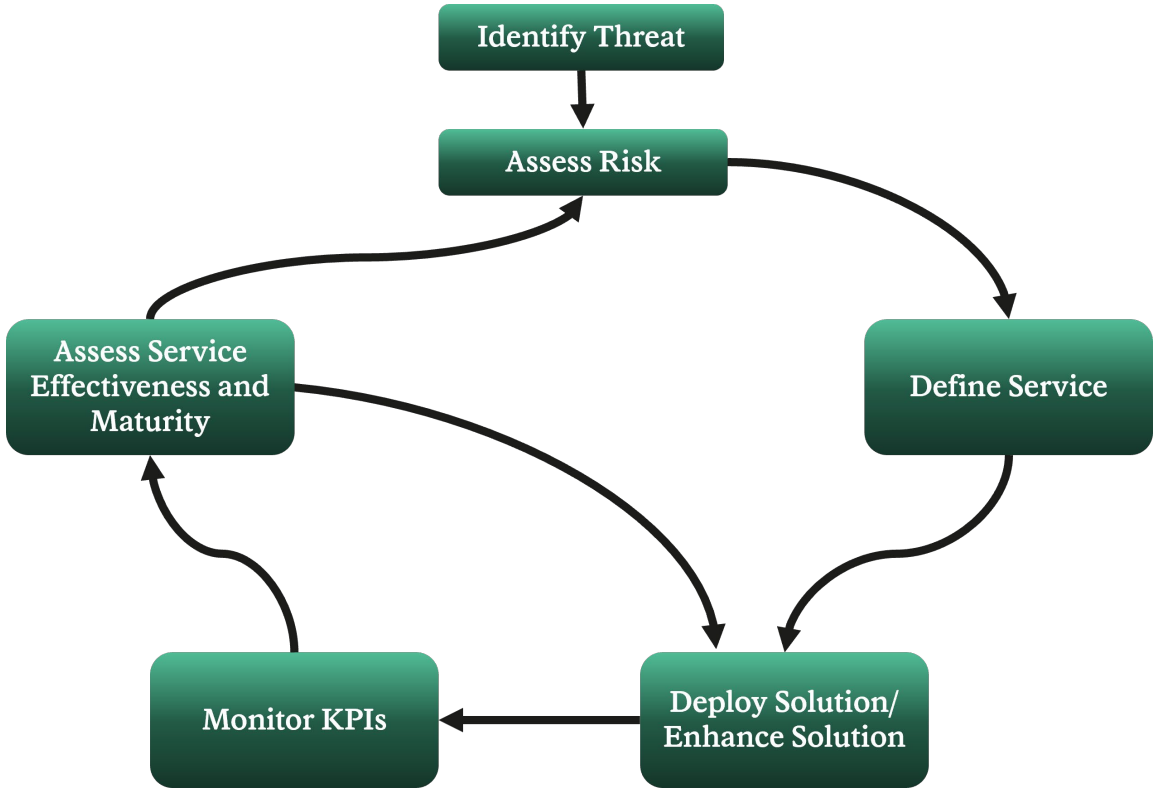
Example:

- **Service** – Vulnerability Management
- **Goal** – Identify vulnerabilities in servers and workstations

Technical	Operational	Executive
1. List of vulnerabilities on xx Server 2. List of hosts w/o Tenable Agent 3. List of servers with vulnerable Log4J version	1. By department, % of servers with critical or high vulnerabilities 2. By department, trend of 'aging' vulnerabilities 30+ days old	1. Current Maturity/Effectiveness of of VM Program: 3.5/2.75 (Optimizing Phase)

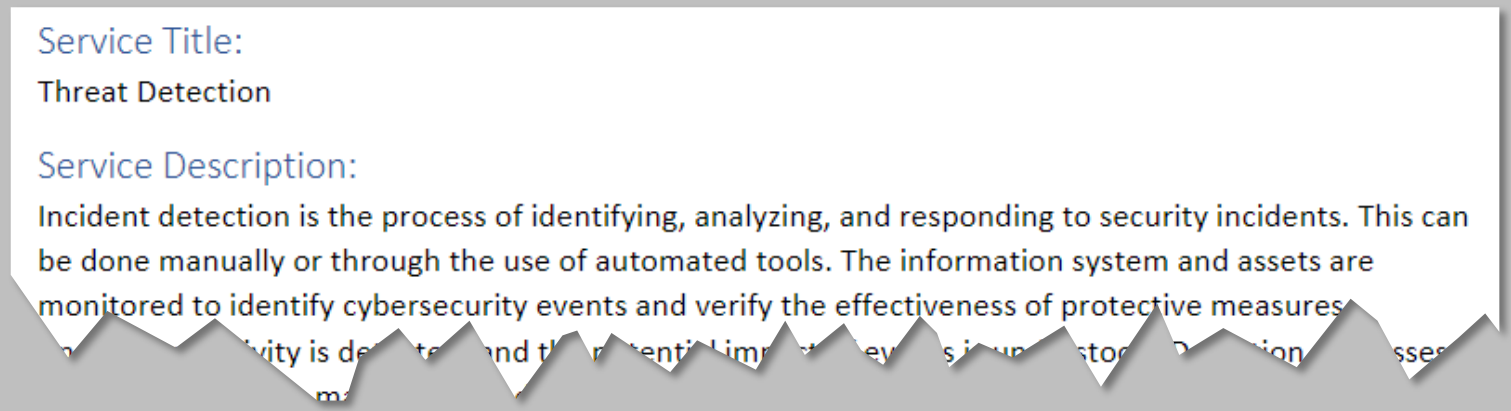
How to Create Metrics/Measurements

- Review your Service Description statement
- List goals/objectives of your service/application
- Brainstorm data points that support these goals
  - Use #s, %, qualitative language, etc.
- Ask yourself, what story does this data point tell?
- Ask yourself, who is the target audience for this data point?
- What is an appropriate cadence to collect/report this data
- Have a peer review
- Create a list of metrics/measurements and submit to Leadership Team for review.



Exercise

1. Review your service description


Service Title:

Threat Detection

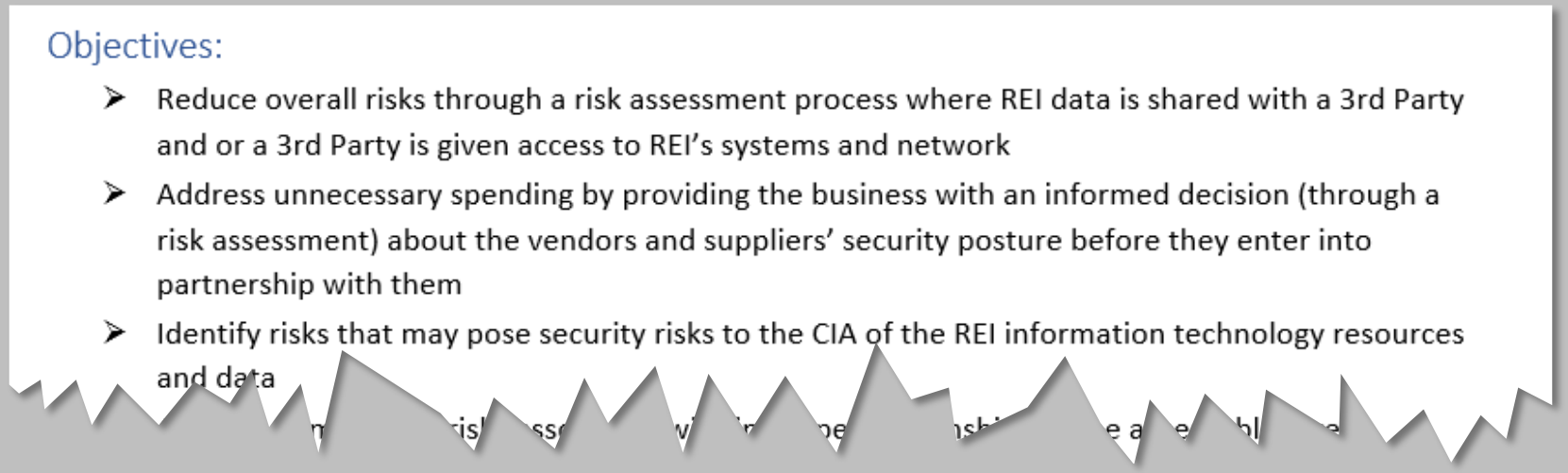
Service Description:

Incident detection is the process of identifying, analyzing, and responding to security incidents. This can be done manually or through the use of automated tools. The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures

- 5 Min -

Exercise

2. Create Service Objectives (2 or 3)



Objectives:

- Reduce overall risks through a risk assessment process where REI data is shared with a 3rd Party and or a 3rd Party is given access to REI's systems and network
- Address unnecessary spending by providing the business with an informed decision (through a risk assessment) about the vendors and suppliers' security posture before they enter into partnership with them
- Identify risks that may pose security risks to the CIA of the REI information technology resources and data

- 10 Min -

Exercise

3. Choose 1 or more objectives. Create a table and fill out:

Executive/Strategic Level	Operational Level	Tactical Level
1x KPI	2x Metrics	3x Measurements or Metrics

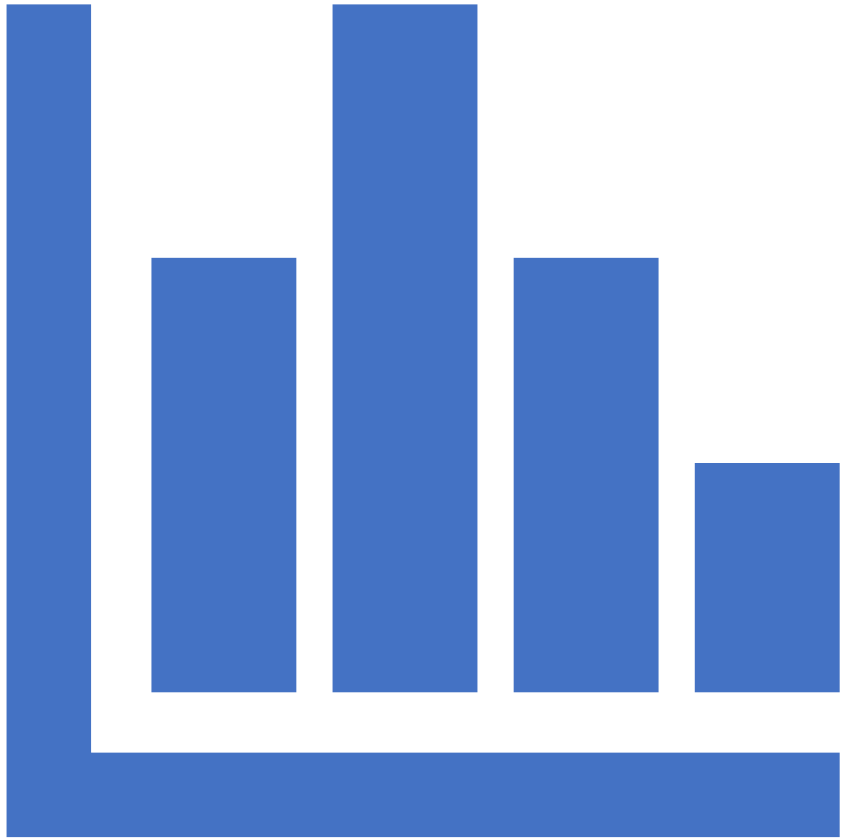
- 10 Min -

Round Table - Questions

- Read through of your Metrics/Measurements/KPIs

- Explain how they measure value

- Provide feedback to your peers



Next Steps

- Create Service Objectives by xx
- Create a list of Metrics/Measurements/KPIs for your services and applications (*save them in your service definitions*) by xx
- Peer review by xx
- Submit to Manager for review by xx

Complete by xx/xx/xx (30 days after class)

Questions

Appendix

Example Category of Metrics

- **Presence** – Binary indicator of whether a control is available *(do we have a vulnerability management program)*
- **Coverage** - % of assets or targets subject to a given control (*% or endpoints with Crowdstrike Installed)*
- **Utilization** – The extent to which specific features and capabilities of a control are being used (*% of available Saviynt features in use)*
- **Performance** – How well is the application/service doing what it is designed to (*Number of blocked phish emails*)
- **Efficiency -** How well does the application/service support business operations and increase efficiency (*Number of retail logins per day, tracked over time*)