Make Metrics Matter

Jessica Ireland, Senior Practice Manager – Security, Risk & Compliance
Info-Tech Research Group

First up…

A little about me

- Senior Practice Manager, at Info-Tech Research Group
  - IT-research firm
  - Security practice focuses on strategy-based research and technology product reviews
  - Also opportunities for on-site work with our clients – workshops, consulting
  - Our HQ: London, ON., also offices in Toronto and Las Vegas
- Contemporary dancer for over 20 years

- Which leads me to my next point…

Time to show us what you've got

- Security and IT professionals – the spotlight is on YOU now (more than ever before).
- So as you take centre stage…
  - **Are you Chris Christie?**
  - **Are you Michelle Obama?**
  - **Are you Will Smith?**

Takes 3 steps

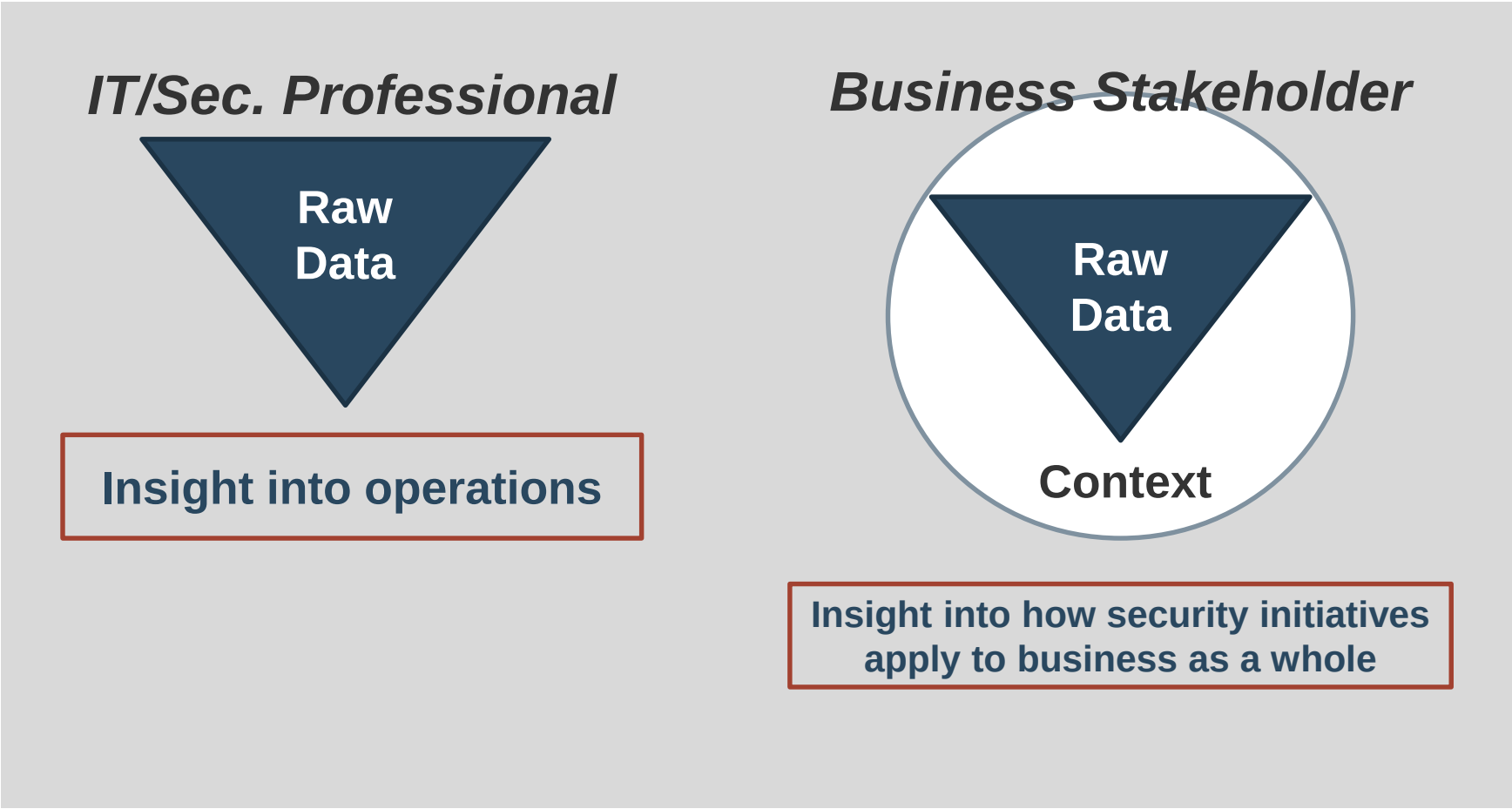
1. **Forget the formulas.**
   - You will sometimes see recommendations for metrics with fancy formulas. Give yourself some credit. You likely know what you should be measuring, keep it simple.

2. **Just start somewhere.**
   - Analysis paralysis is a reality with metrics. You spend so much time worrying about having to come up with *something*, you can barely leave the starting line. Where do you begin? Where do you find the right data?

3. **Don’t do it all at once.**
   - You will set yourself up for failure if you decide to be Sally Overachiever. Don’t boil the ocean, put too many eggs in one basket, [insert idiom here]…

Metrics basics

Metrics are measurements that are compared to a baseline.



Differentiate terms used in the industry

Metrics and analytics both give visibility into your operations, but they have different uses, helping make data informational.

Metrics

Metrics are **tangible data points** extracted from hardware, software, and security devices.

- Typically in raw form and transformed into dashboards, plots, and graphs
- Can be compared and analyzed to other controls and over time
- Provide basic insights based on past data
- Provide an inside perspective

Management metrics demonstrate the effectiveness of controls and processes to justify spend and future security initiatives.

Analytics

Analytics are performed **on metrics** extracted from controls **to gain insights**.

- Used to answer strategic questions
- Used to anticipate future data or uncover root causes underlying metrics
- Provide an outside perspective
- Identify trends and correlations so that metrics can be understood and intelligent next steps can be chosen

When deciding which metrics to track, consider:

- What type of intelligence feeds do we have to derive performance? For example, do we have a SIEM solution?

Consider the different types of metrics

Aim to reach 100% for implementation metrics, then shift focus to effectiveness/efficiency and impact metrics.

Implementation Metrics	*For example:*
Purpose: Track the success of implementing information security programs, specific security controls, and security policies and procedures. ***Goal:*** Identify security controls in need of improvement and determine when an organization is mature enough to move towards measuring other metrics.	***Percentage of systems with approved system security plans.***

Effectiveness/Efficiency Metrics	
Purpose: Monitor the effectiveness (robustness) and efficiency (timeliness) of security processes and controls – if they're correctly implemented, operating as intended, and meeting requirements. ***Goal:*** Provide key information for decision makers: Were previous investments worthwhile? Where do we need increased protection?	***Percentage of OS vulnerabilities for which patches have been applied.***

Impact Metrics	
Purpose: Assess the impact of security on the organization's mission and goals. ***Goal:*** Gain organization-specific insight into the value of information security to the organization, allowing leadership to see the relationship between resources and security activities and events.	***Cost savings resulting from information security program.***

Forget the formula

One more time with feeling…

What REALLY makes a good metric?

- **Repeatable and consistent:** Maintain your integrity; ensure metrics are defensible.
- **Contextually-specific:** Provide clear, actionable information.
- **Relevant to business operations:** Ensure the metric satisfies a compelling business need.
- **Inexpensive to measure:** Don’t waste time / effort collecting and analyzing data if the outcome isn’t worthwhile for the business.
- **Yields quantifiable information:** Raw numbers or proportional measures allow the metrics to be objectively compared over time.

Identify which metrics should be measured

Ensure you're efficiently tracking metrics that matter to your organization.

 # Absolute Measures

% Relational Measures

Wondering which metrics to track?
Ask yourself, **"So What?"**

What makes a good metric?

- **Repeatable and consistent**
- **Contextually-specific**
- **Relevant to business operations**
- **Inexpensive to measure**
- **Yields quantifiable information**

If I had this measure:

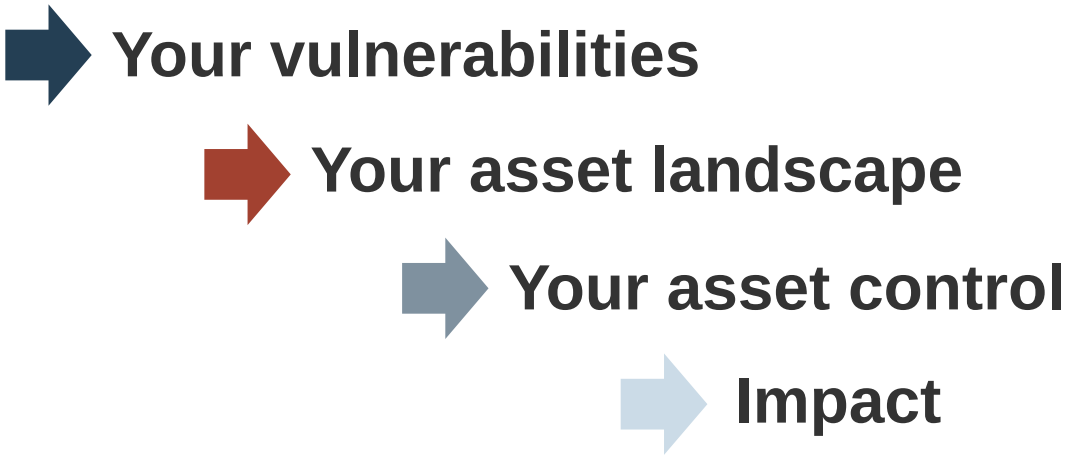
- Who would care?
- What decisions would it influence?
- What actions would it lead to?
- What behaviors would it affect?
- What would improvement look like?
- What would its value be in comparison to other measures?

Just start somewhere

Look before you leap

Like most security processes, knowing where your organization falls on the risk spectrum determines what metrics are most relevant.

- Before you embark on a metrics program and prioritize what to measure, understand the following:



Metrics should be informed by your risk tolerance

At a glance, identify your risk tolerance level

See how your organization fits into the criteria below. Descriptions and examples don't have to match your organization perfectly.

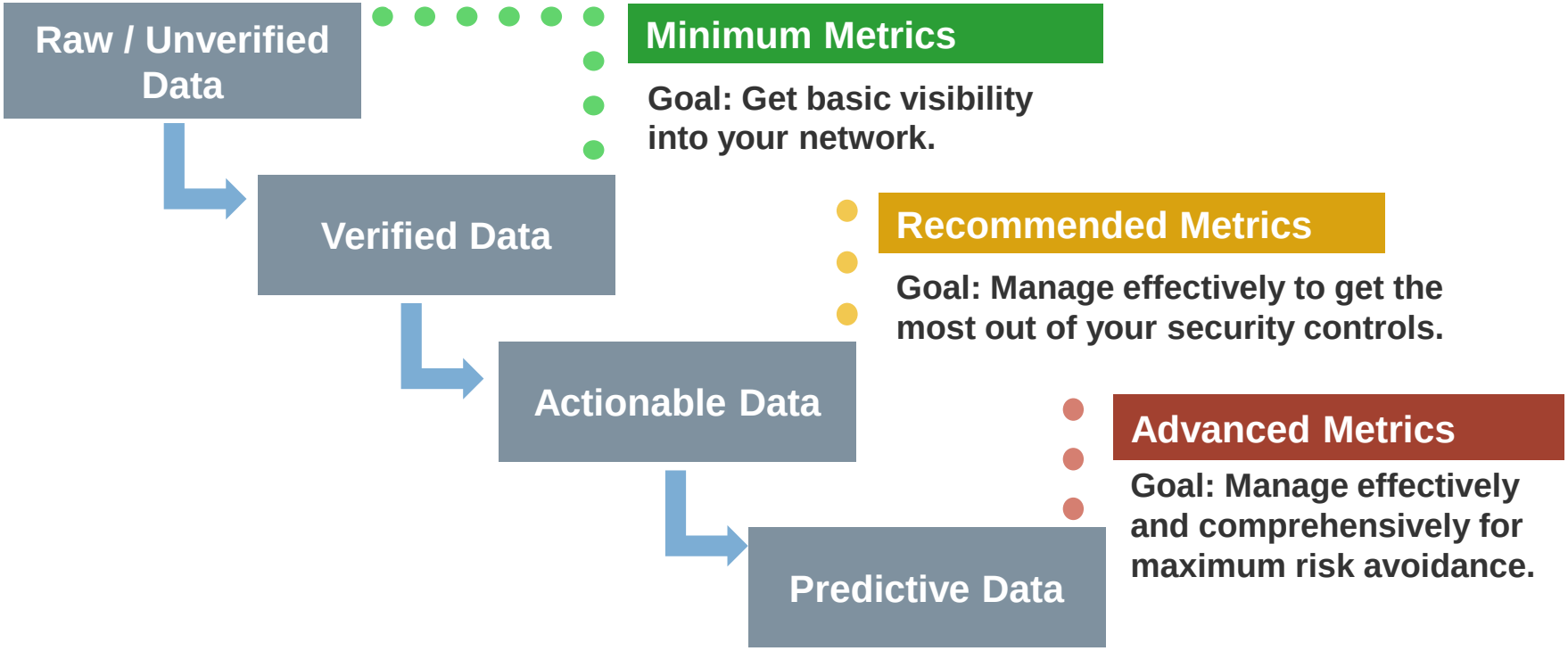
High Tolerance

Moderate Tolerance

Low Tolerance

Step-by-step

Iterative metrics programs allow organizations to focus on identifying what they need to measure as a baseline, and then recognize where there are opportunities to grow.



Don’t do it all at once

High Tolerance: where to start

- Can accept more risk in their processes.
- You may not be more comfortable with risk, but it may mean you are unable to afford the right technologies or stakeholders invest more in business than in security.
- You may also have less sensitive data.

Start with the **minimum**:
Get basic visibility into your network.

High-tolerance metrics example

Category	Example Metrics
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity)

Before you get too overwhelmed, know that if you're just starting, focus on the BASICS. Don't complicate things or you'll set yourself up for failure.

Just know your numbers first.

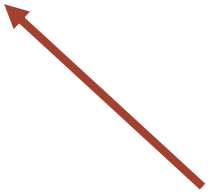
Medium Tolerance: where to start

- You may have some compliance requirements, but could face restrictions on how comprehensive your security strategy can be due to budgetary limitations or lack of skilled resources.

Your metrics should be at the recommended level:
Manage metrics effectively to get the most out of your security controls

Medium Tolerance: where to start

Category	Example Metrics
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity), mean time to recovery, percentage of recurring incidents, incident rate (by type of incident/severity of)



Expand on the numbers and get more specific, add more CONTEXT.

Low Tolerance: where to start

- Your organization likely has sensitive data to protect and/or you must adhere to multiple compliance requirements.

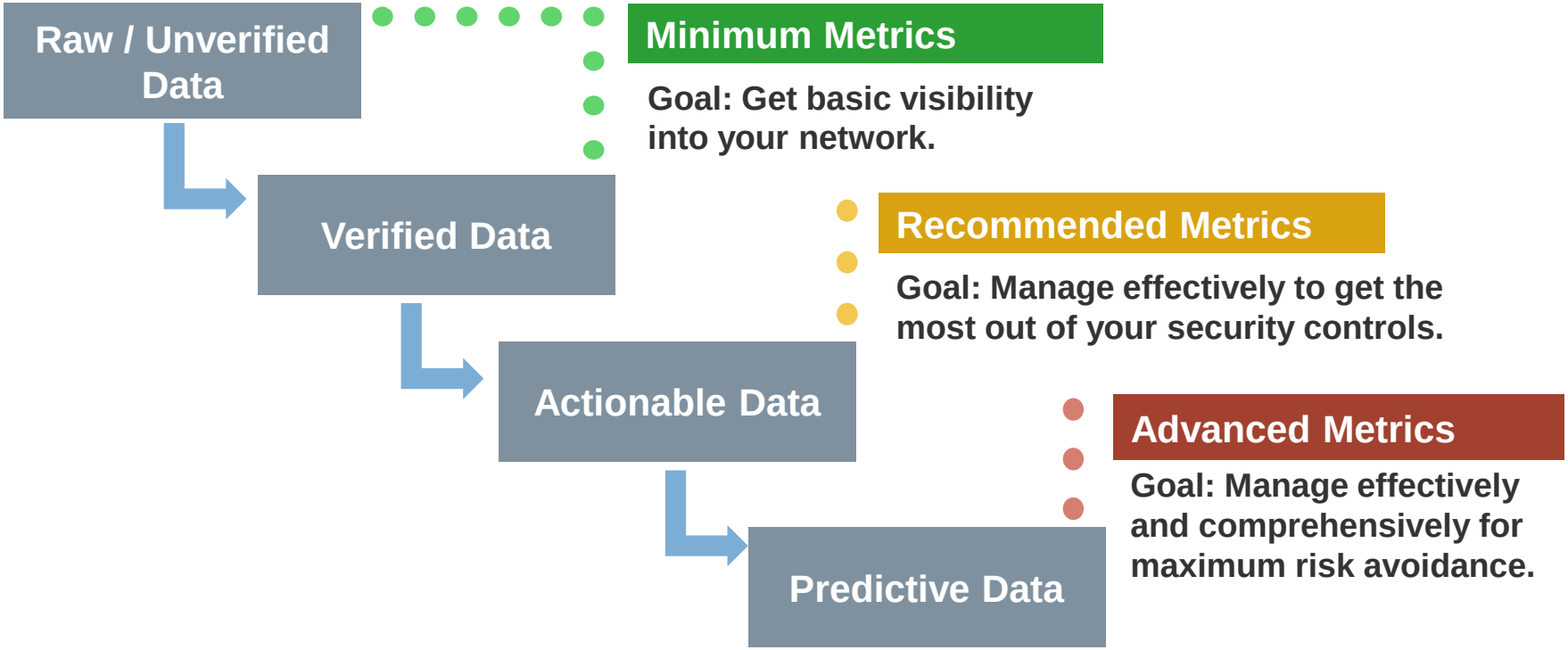
Time to look at advanced metrics: Manage metrics effectively and comprehensively for maximum risk avoidance.

Low Tolerance: where to start

Category	Example Metrics
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity), mean time to recovery, percentage of recurring incidents, incident rate (by type of incident/severity of), incident to attack/threat ratio (by type)

It comes down to a maturing the metric(s)

Grow on basic numbers, add context, get specific, classify instead of generalize (severity of incidents rather than incidents as a whole), get creative.



Prioritize

Be realistic about what's on your plate – you won't be able to track everything right away. Openly discuss the metrics that matter most.

Consider the following factors when prioritizing your metrics:

- Affordability
- Alignment with business objectives
- Ease of data collection
- Ease of data management
- Availability of tracking tools

Gettin' grid-y with it

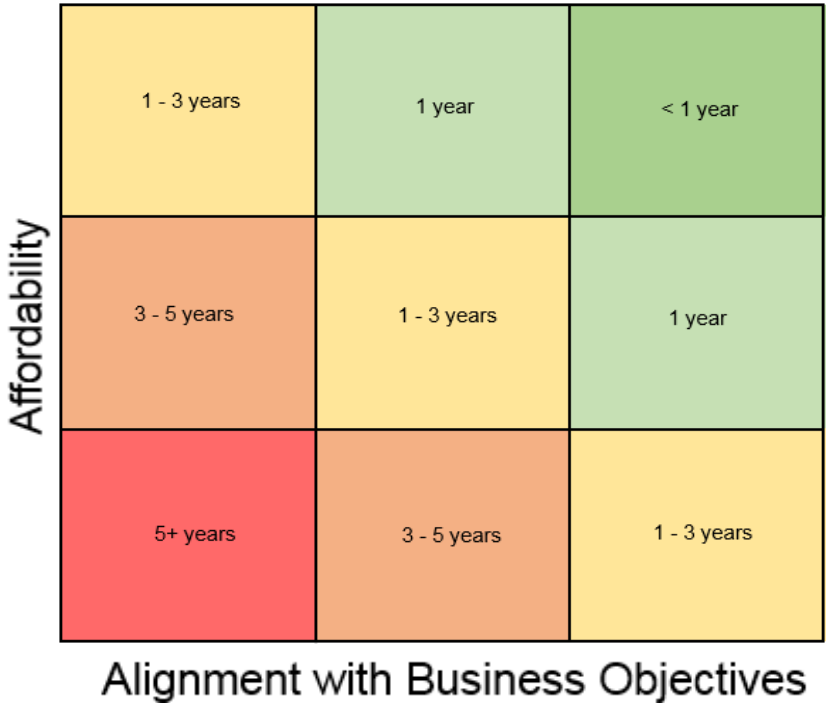
1. Create a grid (such as the example below) of Affordability vs. Alignment with Business Objectives (or other relevant factors) on a whiteboard or table top.

2. Assign each square an estimated start date to begin tracking metrics. The upper-right will represent metrics with high affordability and low alignment with business objectives, so assign it a sooner time frame (e.g. this year, next quarter, etc.).

3. Write each metric listed you've established on a sticky note.

4. With team members, discuss an appropriate timeline for each metric and place it on the grid. Make sure you can justify each placement.

5. Analyze the resulting grid.



Breaking down the data

Leverage various tools and approaches to collect data, aiming to efficiently track metrics to meet organizational needs.

Collect raw data of technical metrics from the following tools:

- Application security scanners
- Anti-malware software
- Anti-spam software
- Asset management programs
- Databases
- Firewalls
- GRC software
- IDPS software
- Managed software services
- Media sanitizers
- Mobile data protection software
- Network access control solutions
- Operating systems
- Secure web gateways
- SIEM software
- Unified threat management solutions
- Web application firewalls
- Website statistics

Use qualitative data carefully.

- "Soft" answers in surveys can provide valuable insight regarding the opinions, confidence, and perceived effectiveness of security controls and strategies.
- However, these metrics are subjective and suffer from biases and inconsistent interpretations among users.
- Use these metrics to *support* objective *hard* facts and glean perspectives, but be wary of fallacies in the data.

Establish data ownership early.

- Ensure consistency and accountability through assigning owners to each metric. Each owner will be responsible for tracking and reporting a subset of metrics.
- Keep it manageable. No one should have more than 5-10 metrics under their ownership, depending on their role.

As always, relate the metrics back to management's priorities. Make sure the data being collected is given proper context and answers relevant questions to reach the business's goals and keep the organization secure.

Make data useful

Reporting raw metrics on their own doesn't necessarily contribute to the overall security strategy – analyze the data to make the metrics valuable.

Provide context

Data needs an explanation to be useful.

Metric + **Context** = **Valuable insight**

Other tips:

Cleanse your data	Make data accurate	Identify missing information	Correlate your data

Track based on your maturity (remember part 2?)

Don’t go overboard – use tracking and analysis tools proportional to your organizational maturity for the most efficient use of resources.

Low Metrics Maturity

Don’t waste resources investing in overcomplicated tools.

- Leverage simple spreadsheets (e.g. Excel) to compile and aggregate high-level data.
- Use built-in features to present the data in a variety of methods – don’t present all the information using the same graph type.

Medium Metrics Maturity

Don’t waste resources manually visualizing data that you’re already collecting.

- Leverage analytics software solutions to compile data from various existing databases and automatically generate professional-quality graphs and charts.
- For example, Tableau and Domo offer solutions to connect data, see relationships, and present to management.

DOMO tableau

High Metrics Maturity

Don’t waste resources manually collecting, analyzing, and reporting data.

- Leverage software tools such as GRC and SIEM solutions to automatically and dynamically collect and manage security data from your network.
- More refined than business analytics software, these solutions will assist with compliance requirements and give specific security visibility.
- These tools include sophisticated, customizable dashboards to streamline your reporting process.

To close…

Keep it simple, take it slow and add context

Thank you!

Appendix

At a glance, identify your risk tolerance level

See how your organization fits into the criteria below. Descriptions and examples don't have to match your organization perfectly.

High Tolerance

- Most likely your organization does not operate within the following areas. Examples:
  - Finance
  - Health care
  - Telecom
  - Government
  - Research
  - Education
- You have no compliance requirements.
- You do not store sensitive data.
- Customers do not expect you to implement and maintain strong security controls.
- Innovation and revenue generation come before security, so your risk posture is higher.
- Organization does not have remote locations.

Moderate Tolerance

- Most likely your organization operates within the following areas. Examples:
  - Research
  - Education
- You have some compliance requirements (e.g. HIPAA, PCI, CJIS, NCIC, PIPEDA).
- You have a moderate amount of sensitive data, and you are required to retain records.
- Customers need strong security controls for data that you store, transactions, and activities.
- Due to the sensitive data, information security is more visible to senior management.
- Organization has some remote locations.

Low Tolerance

- Your organization operates within the following areas. Examples:
  - Finance
  - Government
  - Health care
  - Telecom
- You have multiple compliance requirements and house sensitive data, such as medical records.
- Customers require and expect your organization to have and maintain strong security controls.
- Information security is highly visible to senior management and public investors.
- Organization has multiple remote locations.

2.1 Prioritize the recommended metrics

Be realistic about what's on your plate – you won't be able to track everything right away. Openly discuss the metrics that matter most.

Consider the following factors when prioritizing your metrics:

Affordability	Consider both the up-front cost of the tracking tool, as well as the cost of collecting, managing, and analyzing the data of each metric. Include estimates for the time and effort required for the tracking and reporting of the metric.
Alignment with business objectives	Factor in how transformational the insights of each metric are to reaching corporate goals, fitting the needs of the metrics program, and keeping the organization secure.
Ease of data collection	A metric is only worth tracking if the time and effort required to do so does not outweigh the actionable results it can lead to. Trade-offs of time and effort for an insightful metric are to be expected, but don't waste business time.
Ease of data management	Personnel is required to manage each metric, so the availability of expertise is a limiting factor in the number and type of metrics that can be tracked. Spend your resources wisely – if you assign an individual too many metrics to manage, other areas of work will be compromised.
Availability of tracking tools	Available resources to track the metrics may be a bottleneck in the metrics program. Make sure that you have the necessary tools before committing to tracking a particular metric.

High-tolerance metrics examples

Category	Example Metrics
Compliance & Audit	Volume of audit obligations (total # including internal and external audits/assessments, etc.)
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity)
Security Awareness & Training	Number of end users who have received appropriate training
Budget & Cost	None…for now

Before you get too overwhelmed, know that if you're just starting, focus on the BASICS. Don't complicate things or you'll set yourself up for failure.

Just know your numbers first.

Medium Tolerance: where to start

Category	Example Metrics
Compliance & Audit	Volume of audit obligations (total # including internal and external audits/assessments, etc.), number of & severity of infractions in audit reports, reviews, assessments, etc., mean time to resolve findings
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity), mean time to recovery, percentage of recurring incidents, incident rate (by type of incident/severity of)
Security Awareness & Training	Number of end users who have received appropriate training, security awareness level (e.g. test score information, random sampling, etc.)
Budget & Cost	None…for now, annual cost of information security controls, incident response costs

Low Tolerance: where to start

Category	Example Metrics
Compliance & Audit	Volume of audit obligations (total # including internal and external audits/assessments, etc.), number of & severity of infractions in audit reports, reviews, assessments, etc., mean time to resolve findings, mean time to resolve infractions (by severity)
Security Incidents & Threats	Number of incidents reported , number of information security incidents (different severity), number of information security threats (different severity), mean time to recovery, percentage of recurring incidents, incident rate (by type of incident/severity of), incident to attack/threat ratio (by type)
Security Awareness & Training	Number of end users who have received appropriate training, security awareness level (e.g. test score information, random sampling, etc.)
Budget & Cost	None…for now, annual cost of information security controls, information security budget as % of IT budget, incident response costs (by type of incident)

2.5 Make data useful for decision making, improving performance, and assigning accountability

Reporting raw metrics on their own doesn't necessarily contribute to the overall security strategy – analyze the data to make the metrics valuable.

Provide context — **Data needs an explanation to be useful.**

Metric:
Data indicating a reduction of overall security incidents in one year

+

Context:
- ✓ How big is the reduction compared to last year?
- ✓ Is this high or low if we were to benchmark against other organizations in our market space?
- ✓ What contributed to this reduction?
- ✓ Has anything suffered as a result of the reduced incidents? (e.g. Are there user concerns that security is too rigid, affecting user experiences?)

=

Valuable insight supporting future decisions, improving performance, and assigning accountability.

Cleanse your data	Make data accurate	Identify missing information	Correlate your data
Not all data will be relevant to your overall program. Regularly cleansing collected data by getting rid of duplicates and data that could skew results is essential to ensuring data is accurate, complete, and consistent.	Eliminate (or call out) false positives/negatives that skew results to suggest inaccurate conclusions. Many technical solutions, such as vulnerability scanners, result in less than 100% accuracy. Tune your systems up or down to fit your needs.	Incomplete datasets can reject insightful conclusions. Look for gaps in tracking logs and anomalies in the data. If you suspect missing information, speak with individuals responsible for inputting data as human error is a common cause.	Raw data generated from multiple systems can be correlated into a single metric to report. Data on its own may not draw any conclusion, but analyzing it relative to other information may lead to actionable results. Use spreadsheets or GRC solutions for analysis.