Technical Metrics Aren’t Enough: 10 Strategic Security Measures

SESSION ID: GRC-F01

Julia Allen
CERT® Program
Carnegie Mellon Software Engineering Institute
Pittsburgh, PA

Lisa Young
CERT® Program
Carnegie Mellon Software Engineering Institute
Pittsburgh, PA
Technical Metrics Aren’t Enough: 10 Strategic Security Measures

Learn how 10 strategic security measures, tied to business objectives, are more effective than tactical operational measures (systems patched, incidents reported) to determine your current security state and improve your security posture. Understand key questions to ask and ways to communicate with business leaders in their language using measures defined by the CERT® Resilience Management Model.

www.rsaconference.com/learn2014
Session Expectations

This session

- does not cover specific technical security measures
- does cover strategic security measures and their importance

Why you might want to stay for this session anyway - if you are interested in

- determining the current state of security in support of business objectives
- identifying risks and gaps in your current measurement processes
- selecting and implementing practices and controls tied to business objectives
- a description of candidate measures that will help you do these things
Key Takeaways

Determine which measures are most important: key questions to ask

Articulate 5 business objectives and 10 key measures that better
- illustrate your current state of security at a strategic/business level
- inform the selection of improvements

Put measures in place that stick

Communicate with business leaders in their language
Software Engineering Institute (SEI)

- Federally funded research and development center
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT – *Anticipating and solving our nation’s cybersecurity challenges*

- Largest technical program at the SEI
- Focused on internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response
CMU-SEI-CERT Cyber Risk Management Team

Engaged in applied research, education and training, putting improvements into practice, and enabling our federal, state, and commercial partners

In areas dealing with operational resilience, resilience management, operational risk management, and integration of cybersecurity, business continuity, disaster recovery, and IT operations

http://www.cert.org/resilience/
Topics

CERT Resilience Management Model (CERT-RMM) Overview
How Secure Am I?
Why Measure? What Should I Measure?
Measurement Defined
Key Measures
Getting Started
CERT-RMM Overview
Operational Resilience noun [ri-ˈzil-yəns]

- Power or ability to return to the original form, position, etc., after being bent, compressed, or stretched.
- Physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit.
- Ability to recover readily from illness, depression, adversity, or the like.
- Ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
- Ability to recover from or adjust easily to misfortune or change.
- Capability of a strained body to recover its size and shape after deformation.
- Ability of an ecosystem to return to its original state after being disturbed.
Operational Risk and Resilience

Security and business continuity are risk management processes.
For operational risk management to be effective, these activities must work toward the same goals.

Operational resilience emerges from effective operational risk management.

- Actions of people
- Systems and technology failures
- Failed internal processes
- External events
CERT-RMM

Framework for managing and improving operational resilience

“...an extensive superset of the things an organization could do to be more resilient.”
- CERT-RMM adopter

http://www.cert.org/resilience/
Organizational Context

Productive Activities

Service

People
protect sustain

Information
protect sustain

Technology
protect sustain

Facilities
protect sustain

CERT-RMM applies here

Operational Resilience Management System

Organization Mission
Service Mission
CERT-RMM: 26 process areas in 4 categories

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Operations Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM</td>
<td>Asset Definition and Management</td>
</tr>
<tr>
<td>CTRL</td>
<td>Controls Management</td>
</tr>
<tr>
<td>RRD</td>
<td>Resilience Requirements Development</td>
</tr>
<tr>
<td>RRM</td>
<td>Resilience Requirements Management</td>
</tr>
<tr>
<td>RTSE</td>
<td>Resilient Technical Solution</td>
</tr>
<tr>
<td>SC</td>
<td>Service Continuity</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enterprise Management</th>
<th>Process Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMM</td>
<td>MA</td>
</tr>
<tr>
<td>COMP</td>
<td>MON</td>
</tr>
<tr>
<td>EF</td>
<td>OPD</td>
</tr>
<tr>
<td>FRM</td>
<td>OPF</td>
</tr>
<tr>
<td>HRM</td>
<td></td>
</tr>
<tr>
<td>OTA</td>
<td></td>
</tr>
<tr>
<td>RISK</td>
<td></td>
</tr>
</tbody>
</table>


How Secure Am I?
How Secure Am I? - 1

When asked:
- How secure am I?
- Am I secure enough?
- How secure do I need to be?

What does this mean?
How Secure Am I? - 2

Depending on who’s asking the question, it can mean:

- Do I need to worry about security?
- If I get hacked, will it make the news? Will I end up in court? in jail?
- Do I meet compliance requirements?
- How secure am I compared to my competition?
- Do I need to spend more $$ on security? If so, on what?
- What am I getting for the $$ I’ve already spent?
Key Questions - 1

How secure is my IT infrastructure? My information? My facilities? My people? My supply chain?

- How secure do I need to be? How do I express this?
- What would change if I was more secure?

Have the investments I’ve made (controls, practices, technology, experts, etc.) made me more secure/secure enough? By how much? Compared to what? How do I know?
Key Questions - 2

What should I be measuring to determine if I am meeting my performance objectives for security?

- Do I know what these are? Do they reflect today’s realities?

What is the business value of being more secure?

- Of a specific security investment?
So What? Why Do You Care?

This is the most important question.

If I had this measure: (*)

- What decisions would it inform?
- What actions would I take based on it?
- What behaviors would it affect?
- What would improvement look like?
- What would its value be in comparison to other measures?

Why Measure? What Should I Measure?
Some typical technical measures

- % of assets (systems, devices) patched
  - min/mean/max time from patch release to patch implementation
- % of scanned assets not found in the CMDB
  - Goal: 100% of assets are inventoried in CMDB and reflect standard configurations
- % of devices/assets regularly scanned by antivirus software
- number of incidents reported/closed
  - number of incidents with a known solution (patch) that was not applied
- % of assets subject to ingress/egress filtering
Some typical strategic/business measures

- % of senior executives who have documented security objectives that are reviewed as part of the performance management review process
- % of security policies that are met (no violations; all exceptions approved)
- difference in planned vs. actual to perform security activities/actions/investments
  - schedule
  - resources
  - cost
- % of staff who have been assessed to determine if training has been effective commensurate with their job responsibilities
Why Measure?

Demonstrate that the security program has measurable business value

Speak to decision makers in their language

Answer key questions

Demonstrate that security objectives are (and continue to be) met

Justify new investments; improve

Help predict the future
What Should I Measure?

Determine business objectives and key questions

Define the information that is needed to answer the question

- What information do you currently have?
- What additional information do you need to collect?

Qualify and quantify the information in the form of measures

Analyze the measures and report out

Quantify the value of each measure (cost/benefit)

Refine and retire measures as you go
Who, What, Where, When, Why, How

**Who** is the measure for? Who are the stakeholders? Who collects the measurement data?

**What** is being measured?

**Where** is the data/information stored?

**When**/how frequently are the measures collected?

**Why** is the measure important (vs. others)? The most meaningful information is conveyed by reporting trends over time vs. point in time measures.

**How** is the data collected? How is the measure presented? How is the measure used?
Measurement Defined
Scope and Terminology

Measure vs. metric

- Measure (noun): the extent, dimensions, quantity, etc., of something, ascertained especially by comparison with a standard; any standard of comparison, estimation, or judgment

- Metric: pertaining to the meter or metric system; a non-negative real valued function; a system or standard of measurement; a criterion or set of criteria stated in quantifiable terms

For our efforts, metric = number; measure = number with analysis and meaning, in context. That said, our community often uses metric to mean both.
Technical vs. Process Measures
Process Measurement Types

Implementation
- Is this process/activity/practice being performed?

Effectiveness (a.k.a. outcome)
- How good is the work product or outcome of the process/activity/practice? Does it achieve the intended result?

Process performance
- Is the process performing as expected? Is it efficient? Can it be planned? Is it predictive? Is it in control?
Key Measures
Structure of the 10 Strategic Measures

Title: The context for the measure (a.k.a. business driver)

- business objectives
- high-value services and assets
- controls
- risks
- disruptive events

Two measures to aid in determining if each business driver is being met

Scenario example: The organization has decided to outsource selected security services and contract for such services using an SLA
Given Business Objectives (1 of 10)

Measure 1

Percentage of security activities(*) that do not directly (or indirectly) support one or more business objectives

Example

Outsource in-house security services
Transition/retire in-house services
Retrain/reassign staff

(*) An activity can be a project, task, performance objective, investment, etc. It represents some meaningful decomposition of the security program.
Given Business Objectives (2 of 10)

Measure 2

For each security activity, number of business objectives that require it to be satisfied (goal is = or > 1)

Example

SLA relationship with external security services provider
CIO/CSO objective
Given High-Value Services and Assets (3 of 10)

Measure 3

Percentage of high-value services that do not satisfy their security requirements(*) (should be zero)

- or measure a specific service of interest
- make sure criteria for selecting a specific service is defined

Example

SLA specifies security requirements and thresholds

- high-priority alerts from incident detection systems are resolved within xx minutes

Provider performance periodically reviewed to confirm compliance; corrective actions identified and addressed

(*) confidentiality, availability, integrity
Measure 4

Percentage of high-value assets\(^{(+)}\) that \textit{do not} satisfy their security requirements (should be zero)

- such as network infrastructure, a specific application, a database, a lead system administrator

Example

SLA specifies security requirements and thresholds
- Incident database: backups and ability to restore from backups

Provider performance periodically reviewed to confirm compliance; corrective actions identified and addressed

\(^{(+)}\) technology, information, facilities, people
Given Controls (5 of 10)

Measure 5
Percentage of high-value services with controls that are ineffective or inadequate (should be zero)

- unsatisfied control objectives
- unmet security requirements
- outstanding assessment/audit problems above threshold without remediation plans

Example
SLA specifies controls (policies, procedures, standards, guidelines, tools, practices, measures)
Provider performance periodically reviewed to confirm compliance; corrective actions taken and confirmed
Given Controls (6 of 10)

Measure 6

Percentage of high-value assets with controls that are ineffective or inadequate (should be zero)
- unsatisfied control objectives
- unmet security requirements
- outstanding assessment/audit problems above threshold without remediation plans

Example

SLA specifies controls (policies, procedures, standards, guidelines, tools, practices, measures)
Provider performance periodically reviewed to confirm compliance; corrective actions taken and confirmed
Given Risks (7 of 10)

Measure 7
Confidence factor that all risks that need to be identified have been identified

Example
Major sources of risk identified in SLA
Risk thresholds by service identified
Confidence factor expressed as plan vs. actual risks for all sources, displayed as a Kiviat diagram
Confidence in Risk Identification

- Organizations with defined risk parameters
  - 100%
  - 80%
  - 60%
  - 40%
  - 20%
  - 0%

- Lines of business with risk parameters inherited from organization
- Assets with associated services
- Services with associated assets
- Asset risks from all sources identified
- Service risks from all sources identified
- Plan
- Actual

- Confidence in Risk Identification: 39
Given Risks (8 of 10)

Measure 8
Percentage of risks with impact above threshold (should be zero)
- **without** mitigation plans (target = zero)
- that are effectively mitigated by their mitigation plans (target = 100%)
- that have been reviewed/actioned in the required timeframe (target = 100%)

Example
Provider risk periodically assessed to ensure risk impact is \( \leq 0 \); corrective actions taken and confirmed
Given a Disruptive Event (9 of 10)

(An incident, a break in service continuity, a man-made or natural disaster or crisis)

**Measure 9**
Probability of delivered service throughout a disruptive event

**Example**
SLA specifies service-specific availability and service levels during normal and disrupted operations
Provider performance periodically reviewed to confirm service levels; corrective actions taken and confirmed
Given a Disruptive Event (10 of 10)

**Measure 10**
For disrupted, high-value services with a service continuity plan, percentage of services that *did not* deliver service as intended throughout the disruptive event

**Example**
SLA specifies requirements for SC plans
Services with SC plans that do not maintain required service levels identified
Updates to provider and customer plans made, confirmed, tested
Top Ten Strategic Measures

1. Percentage of security “activities” that do not directly (or indirectly) support one or more organizational objectives
2. For each security “activity,” number of organizational objectives that require it to be satisfied (goal is = or > 1)
3. Percentage of high-value services that do not satisfy their allocated security requirements
4. Percentage of high-value assets that do not satisfy their allocated security requirements
5. Percentage of high-value services with controls that are ineffective or inadequate
6. Percentage of high-value assets with controls that are ineffective or inadequate
7. Confidence factor that all risks that need to be identified have been identified
8. Percentage of risks with impact above threshold
9. Probability of delivered service throughout a disruptive event
10. For disrupted, high-value services with a service continuity plan, percentage of services that did not deliver service as intended throughout the disruptive event
If These Don’t Work For You . . .

Identify the high-level objectives for your security program
Define measures that demonstrate the extent to which objectives are (or are not) being met
Make sure the measures you are currently reporting support one or more objectives
  - If they don’t, ask “why not?” and “so what?”
  - Measuring “security hygiene” is necessary but not sufficient
Measurement is expensive; collect and report measures that inform decisions and affect behavior
Getting Started
To Get Started

Identify sponsors and key stakeholders

Define security objectives and key questions

Determine information that informs these

- What information do you already have?
- What information do you need to collect?
- What is the value of collecting additional information?

Define and vet a small number of key measures

Collect, analyze, report, refine

Put a measurement program in place
Set Up a Measurement Program

Define
- measurement objectives including audiences and key stakeholders
- measures (5-10 based on the measurement template)
- key roles to collect, analyze, and report these measures
- data collection and storage methods and tools
- analysis methods and procedures

Collect measurement data

Analyze measurement data

Store data and results in a secure manner

Report results

Start small
- data collection
- analysis procedures
- number of measures
- number of participating business units
# Measurement Template [refer to handout]

<table>
<thead>
<tr>
<th>Measure name/ID</th>
<th>Goal</th>
<th>Question(s)</th>
<th>Related processes &amp; procedures</th>
<th>Visual display</th>
<th>Data input(s) (data elements, data type)</th>
<th>Data collection (how, when, how often, by whom)</th>
<th>Data reporting (by, to whom, when, how often)</th>
<th>Data storage (where, how, access control)</th>
<th>Stakeholders (information owner(s), collector(s), customer(s))</th>
<th>Algorithm or formula</th>
<th>Interpretation or expected value(s)</th>
</tr>
</thead>
</table>


Questions
CERT-RMM Contacts

Rich Caralli  
rcaralli@cert.org

Nader Mehravari  
nmehravari@cert.org

Lisa Young  
lry@cert.org

Julia Allen  
jha@sei.cmu.edu

Richard Lynch  
Public Relations — All Media Inquiries  
public-relations@sei.cmu.edu

Pamela Curtis  
pdc@cert.org

Joe McLeod  
For info on working with us  
jmcleod@sei.cmu.edu

SEI Customer Relations  
customer-relations@sei.cmu.edu  
412-268-5800
Resources – 1 Resilience Measurement

SEI blog: Measures for Managing Operational Resilience [link]

CERT Podcast: Measuring Operational Resilience [link]

CERT-RMM Measurement & Analysis website: [link]


Resources – 2 CERT-RMM


CERT-RMM website: http://www.cert.org/resilience/rmm.html


## RSA 2014
### GRC-F01: Technical Metrics Aren’t Enough: 10 Strategic Security Measures
#### Security Measurement Template

<table>
<thead>
<tr>
<th>Measure Name/ID</th>
<th>Unique name or identifier for the measure. For example: <em>Number of Security Requirements</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Statement of security goal. Goal should be connected to overall organizational strategic goals and critical success factors, organizational security goals, service security goals, and/or asset security goals.</td>
</tr>
<tr>
<td>Question(s)</td>
<td>What question(s) is the measure intending to answer? For example: <em>How many incidents occurred last quarter?</em> The question should relate to the Goal.</td>
</tr>
<tr>
<td>Visual Display</td>
<td>Graphical depiction of the measure. For example: trend over time, percentages, cumulative results, Pareto analysis, frequency diagrams, etc.</td>
</tr>
<tr>
<td>Data Input(s)</td>
<td>Measure Name/ID and type (base or derived) of all input data elements used for this measure.</td>
</tr>
<tr>
<td>Data Collection</td>
<td>How the data will be collected (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Refer to forms or standards if needed.</td>
</tr>
<tr>
<td>Data Reporting</td>
<td>Identify the role that is responsible for reporting the measure. Identify for whom (role) the report is intended. This may be an individual role or an organizational unit.</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Identify where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>Who will use this measure? How? What are the roles? Asset owner, service owner, line of business manager, someone who heads up business continuity, steering group responsible for all aspects of security including security measurement. Consider stakeholders external to the organization.</td>
</tr>
<tr>
<td>Algorithm or Formula</td>
<td>Specify the algorithm or formula required to combine data elements to create input values for the measure. It may be very simple, such as input1/input2 or it may be much more complex. The relationship between the algorithm and the visual display should be explained as well.</td>
</tr>
<tr>
<td>Interpretation or Expected Value(s)</td>
<td>Describe what different values of the measure mean. Make it clear how the measure answers the Question(s) above. Provide any important cautions about how the measure could be misinterpreted and actions to take to avoid misinterpretation. Provide guidance on how to interpret the measure and also what not to do with the measure. If the measure has a target value or range for success (meeting the goal), include this here.</td>
</tr>
</tbody>
</table>
### Measure Example – Cost of Recurring Incidents with Known Solutions

<table>
<thead>
<tr>
<th>Measure Name/ID</th>
<th>Cost of recurring incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal</strong></td>
<td>In the face of realized risk, the security program ensures the continuity of essential operations of high-value services and associated assets.</td>
</tr>
<tr>
<td><strong>Question(s)</strong></td>
<td>How many incidents with impact greater than X and with known solutions have recurred during the last reporting period?</td>
</tr>
</tbody>
</table>

#### Visual display

![Cost of Recurring Incidents](image)

#### Data Input(s)

<table>
<thead>
<tr>
<th>Data Elements</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date of last</td>
<td>Base measure of type “schedule”</td>
</tr>
<tr>
<td>reporting period</td>
<td></td>
</tr>
<tr>
<td>End date of last</td>
<td>Base measure of type “schedule”</td>
</tr>
<tr>
<td>reporting period</td>
<td></td>
</tr>
<tr>
<td>Number of recurring</td>
<td>Base measure of type “count”</td>
</tr>
<tr>
<td>incidents during</td>
<td></td>
</tr>
<tr>
<td>the last reporting</td>
<td></td>
</tr>
<tr>
<td>period</td>
<td></td>
</tr>
<tr>
<td>Impact of each</td>
<td>Base measure of type “cost”</td>
</tr>
<tr>
<td>recurring incident</td>
<td></td>
</tr>
<tr>
<td>(cost or effort)</td>
<td></td>
</tr>
<tr>
<td>Impact threshold</td>
<td>Base measure of type “cost”</td>
</tr>
</tbody>
</table>

#### Data Collection

**How**

- Information about an incident is collected throughout the incident management process, on an event-driven basis, by the organization’s service desks.
- Information is reviewed either when the incident is closed or when the post-incident review is performed.
- Impact threshold is established by the Chief Information Security Officer (CISO) and is informed by risk management.

**When/How Often**

- Data is reported to CISO by Computer Security Incident Response Team (CSIRT).
- Data is reported once per reporting period.

#### Data Reporting

<table>
<thead>
<tr>
<th>What</th>
<th>How Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where</td>
<td></td>
</tr>
<tr>
<td>Data is stored in incident knowledgebase.</td>
<td></td>
</tr>
<tr>
<td>All incident report records contain cost information.</td>
<td></td>
</tr>
<tr>
<td>All incident report records contain recurrence information.</td>
<td></td>
</tr>
<tr>
<td>Everyone has read access to the incident report database.</td>
<td></td>
</tr>
<tr>
<td>Only CSIRT has write access to the incident report database.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Information Owner(s)</th>
<th>Information Customer(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CISO is the owner of the incident knowledgebase.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The CISO establishes the impact threshold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The CISO and senior management are the customers for this information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• The Incident Owner is responsible for maintaining and presenting all information related to an incident.
• The staff responsible for managing incidents validates the measures and may be called upon to act on the results.

Algorithm or Formula

Each incident record in the incident knowledgebase must contain the following information:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Occurrence</td>
<td>Date</td>
</tr>
<tr>
<td>Cost</td>
<td>Effort Hours or Currency</td>
</tr>
<tr>
<td>Occurred before</td>
<td>Boolean</td>
</tr>
</tbody>
</table>

Other information needed:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of Reporting Period</td>
<td>Date</td>
</tr>
<tr>
<td>End of Reporting Period</td>
<td>Date</td>
</tr>
<tr>
<td>Impact threshold</td>
<td>Effort Hours or Currency</td>
</tr>
</tbody>
</table>

Algorithm steps to create frequency histogram
1. Create cost bins for the frequency histogram. All costs greater than the established impact threshold should be counted in the last bin.
2. For all incidents in the incident knowledgebase where (“Start of Report Period” < “Date of Occurrence” <= “End of Reporting Period”) and (“Occurred before” is True)
   a. Get “cost” of incident.
   b. Increment frequency of the bin the cost falls into.
   c. Increment cumulative percentage of items in bins.

Example input data:

<table>
<thead>
<tr>
<th>Incident Number</th>
<th>Incident Cost (in thousands of dollars)</th>
<th>Incident Occurred Before?</th>
<th>Impact Threshold (in thousands of dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>87</td>
<td>Yes</td>
<td>80</td>
</tr>
<tr>
<td>2</td>
<td>23</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>27</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>45</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>45</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>62</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>52</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>20</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>29</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>43</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>44</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>92</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>66</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>74</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>61</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Example output data:

<table>
<thead>
<tr>
<th>Cost</th>
<th>Frequency</th>
<th>Cumulative %</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 20 K</td>
<td>2</td>
<td>18.18%</td>
</tr>
<tr>
<td>&lt;= 40 K</td>
<td>1</td>
<td>27.27%</td>
</tr>
<tr>
<td>&lt;= 60 K</td>
<td>3</td>
<td>54.55%</td>
</tr>
<tr>
<td>&lt;= 80 K</td>
<td>3</td>
<td>81.82%</td>
</tr>
<tr>
<td>More than threshold</td>
<td>2</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

Plot Frequency and Cumulative % on the Y-axis, and Cost bins on the X-axis.

**Interpretation or Expected Value(s)**

All recurring incidents that cost more than the established organization threshold should be referred to the *(business process that handles this).* Any incident in the bin labeled *above threshold* is cause for concern. The heights of the bins represent the number of recurring incidents whose costs fall in that bin. Therefore, the higher the height of the last bin, the greater the concern.
## Measure Example – Confidence in Risk Identification

<table>
<thead>
<tr>
<th>Measure Name/ID</th>
<th>Confidence in risk identification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal</strong></td>
<td>The security program manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services.</td>
</tr>
<tr>
<td><strong>Question(s)</strong></td>
<td>Have risks from all sources been identified?</td>
</tr>
</tbody>
</table>

### Visual display

![Confidence in Risk Identification Diagram](image-url)

### Data Input(s)

<table>
<thead>
<tr>
<th>Data Elements</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of organizational units in enterprise</td>
<td>No data type: this is an attribute of the enterprise.</td>
</tr>
<tr>
<td>List of lines of business per organization</td>
<td>No data type: this is an attribute of the organization.</td>
</tr>
<tr>
<td>List of high-value assets</td>
<td>N/A</td>
</tr>
<tr>
<td>List of high-value services</td>
<td>N/A</td>
</tr>
<tr>
<td>List of risk sources</td>
<td>N/A</td>
</tr>
<tr>
<td>Start date of last reporting period</td>
<td>Base measure of type &quot;schedule&quot;</td>
</tr>
<tr>
<td>End date of last reporting period</td>
<td>Base measure of type &quot;schedule&quot;</td>
</tr>
</tbody>
</table>

### Data Collection

- List of organizations is collected from the enterprise organization chart.
- List of lines of business per organization is collected from each organization’s organization chart.
- List of high-value services is collected from the service repository.
- List of high-value assets is collected from the asset database.
- List of risk sources is predefined as failed internal processes, inadvertent or deliberate actions of people, problems with systems and technology, and external events.
- Data is collected by the security measurement group, once per reporting period.

### Data Reporting

- Data is reported by the security measurement group to the CISO once per reporting period. The confidence factor report is generated by a report generation tool.
**Data Storage**  
**Where**  
**How**  
**Access Control**  
The confidence factor reports are archived on the CISO SharePoint website by the security measurement. Only this group has write access to the site. The CISO staff has read access.

**Stakeholders**  
**Information Owner(s)**  
**Information Collector(s)**  
**Information Customer(s)**  
- The information in the asset database is owned by the CISO.  
- The information in the service repository is owned by the CISO.  
- Organizational charts and lines of business charts are owned by HR.  
- The CISO is the primary customer for this report.

**Algorithm or Formula**  
3. Determine the percent of organizations with defined risk parameters (Percent_Orgs).  
4. For each organization, identify lines of business. Determine the percent of lines of business with defined risk parameters inherited from parent organization (Percent_LOBs).  
5. From the service repository, determine the percentage of services where risks have been identified from all four sources (Percent_Services).  
6. From the asset database, determine the percentage of assets where risks have been identified from all four sources (Percent_Assets).  
7. From the asset database and service repository, determine the percent of assets used by at least one service (Asset_Usage_By_Services), and the percent of services where all associated assets are in the asset database (Service_Usage_Of_Assets).  
Confidence = Percent_Orgs * Percent_LOBs * Percent_Services * Percent_Assets * Asset_Usage_By_Services * Service_Usage_Of_Assets

**Interpretation or Expected Value(s)**  
The goal is for the plan and actual axis on the radar plot to be as close as possible, to indicate the actual confidence level is close to the planned confidence level. Overall confidence factor can be determined by multiplying the actual percentage of each axis. A confidence factor of 100% means that all organizations in the enterprise have established risk parameters, that all lines of business in each organization have derived their own risk parameters from their parent organization, that risks from all sources have been identified for all services in the service repository, that risks from all sources have been identified for all assets in the asset database, that all services use assets defined in asset database, and that all assets in the asset database are used by at least one service. If there are other factors that should contribute to this measure, they can be easily added.