Collecting and Sharing Security Metrics – the End of "Security by Obscurity"

a.k.a Communicating Security Performance to Non-Security Professionals

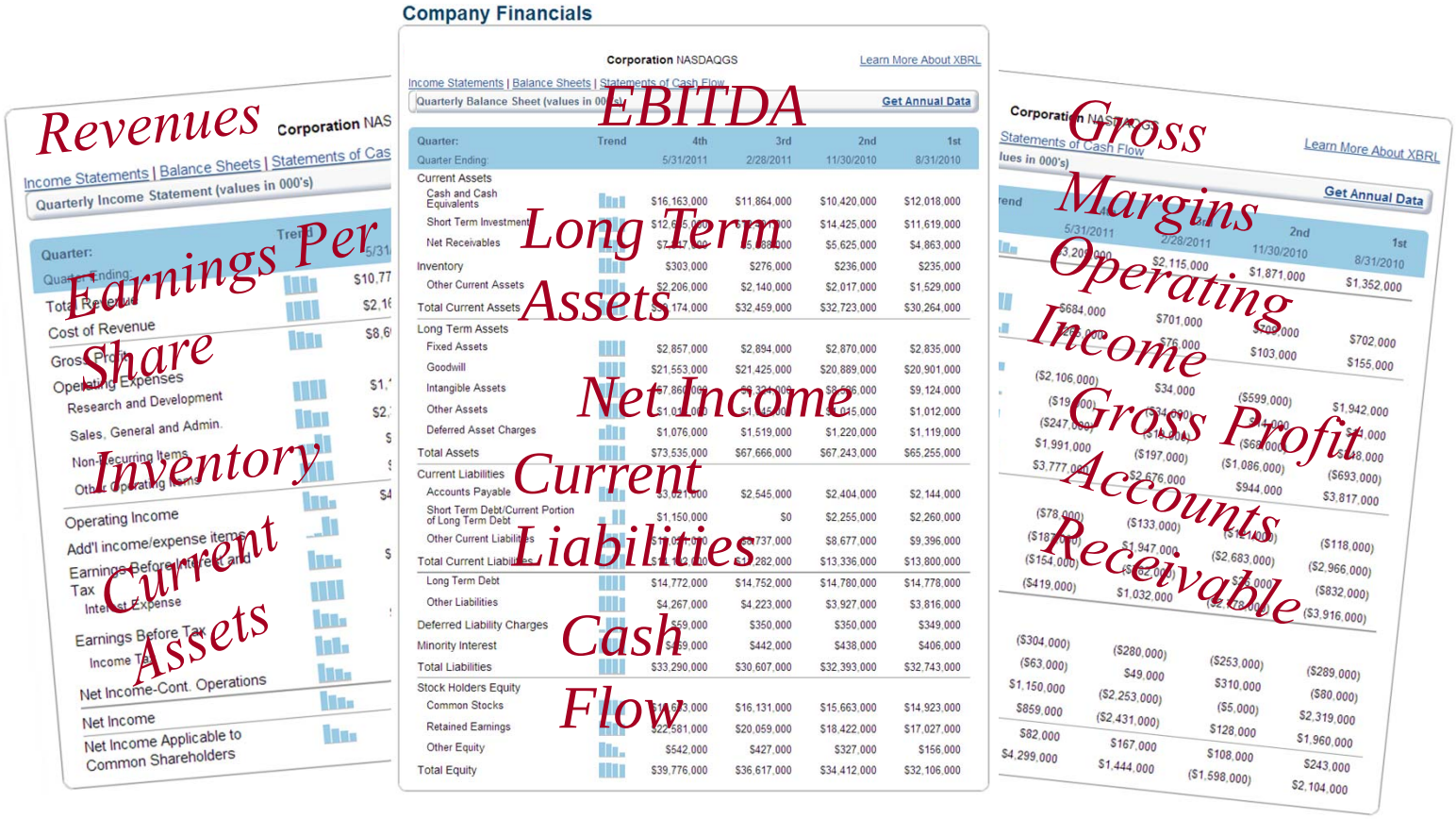
Jim Acquaviva
nCircle

Session ID: SPO2-204
Session Classification: Intermediate

RSA CONFERENCE 2012

The Quarterly Ritual

The Quarterly Ritual



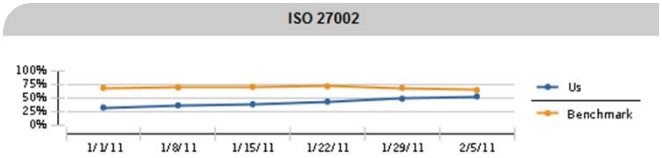
The CSO needs what the CFO has….

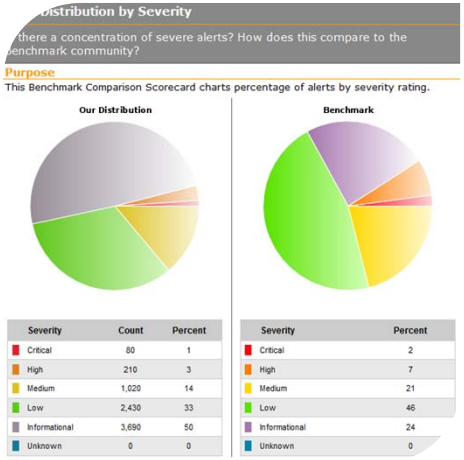
- **CISO's need metrics language to describe a company's security performance just like the CFO describes financial performance**
- Objective, fact-based reporting
- Consistent definitions
- Measured on a repeating schedule to show trends
- Demonstrated performance against goals
- And performance against peers

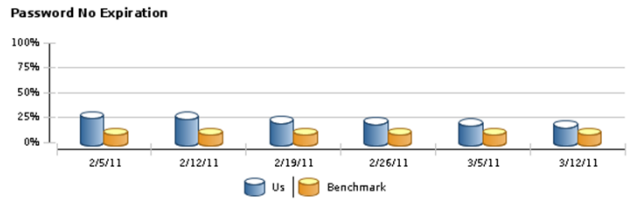
With a Security Performance Management Program, CISOs can demonstrate that

- There is a comprehensive approach to security that is…
  - Measured against specific goals & standards
  - In line with our risk tolerance
  - Aggregated by meaningful asset groupings
  - At least equal to or better than our own industry's investment & performance
  - Controls aligned with GRC objectives

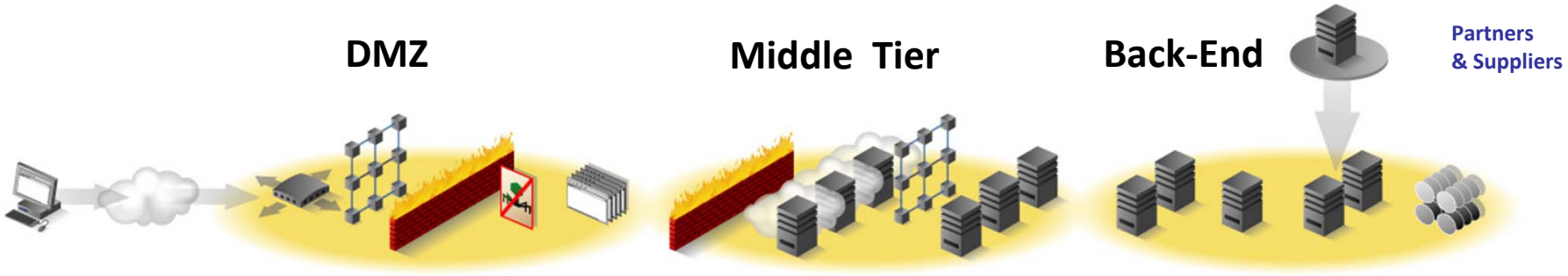
- Based on <u>actual data</u> on an ongoing basis that we can rely on to make decisions on:
  - Investment
  - Execution
  - Resource allocation







Measuring Security is a Top CISO Priority but it is Challenging

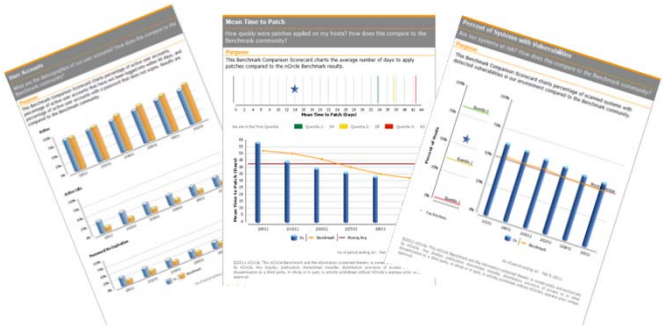


IAM	Firewall	Antivirus	Web Filtering	IDS/IPS	System Mgt	Patch	Audit & Compliance	SEIM	Vulnerability Management
MS AD	Checkpoint	Symantec	Web Sense	McAfee	HP	WSUS	nCircle	ArchSight	IP360
Tivoli	Juniper	McAfee	Barracuda	Source Fire	IBM Tivoli	SCCM	RSA	enVison	Qualys
CA	Cisco	Trend Micro	Surf Control		CA	PatchLink	Agiliance	Intellitatics	R7
Oracle	Symantec	Sophos			BMC Remedy				Foundstone

- Heterogeneous and dispersed silo's of vital IT information
- Variety of contributors and application sources each doing it differently
- Need to fuse together silo's and map results to a business context
- Challenging to reliably and consistently calculate
- Exacting to communicate effectively to wide variety of audiences

Well Constructed Security Metrics & Scorecards

- Align security initiatives with business objectives
- Deliver trusted, timely, and actionable decision making information
- Identify and communicate concentration of risks
- Affirm the existence and effectiveness of security controls
- Continuously monitor controls
- Enable and evidence management oversight; communicate performance and evaluate corrective actions



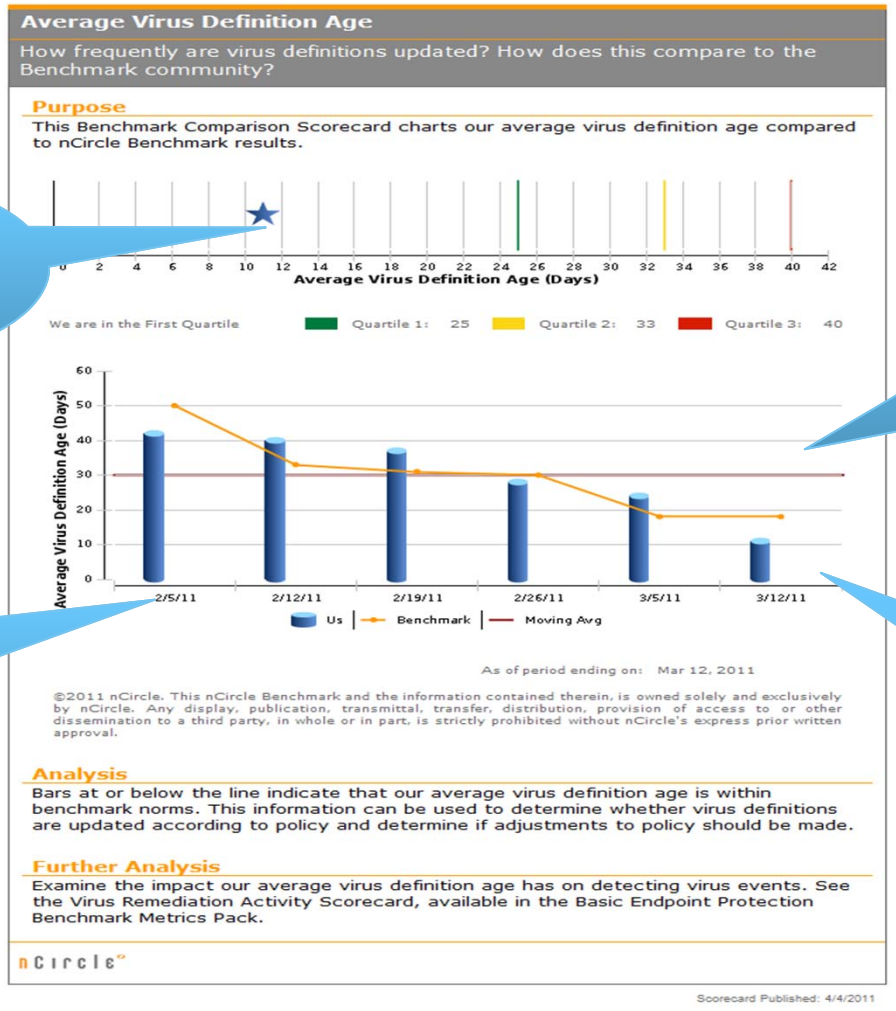
Valuable Peer Benchmarks

Benchmark Performance Quadrants

Participant Results

Benchmark Performance Standard

Weekly Performance Benchmark



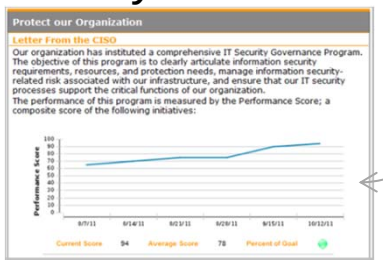
Communicate Security and Compliance Posture: Metrics & Scorecards Roll-ups and Drill-in's

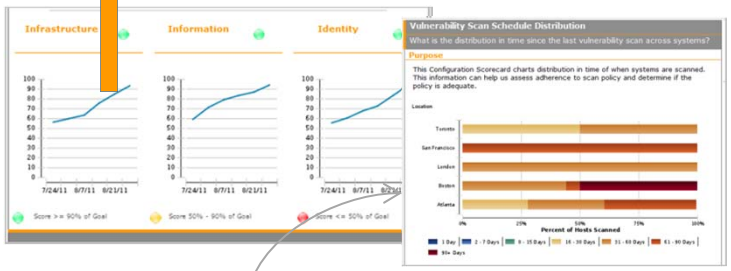
Overview by Initiatives and by Divisions

Overviews of Initiatives and Profiles of Users and Assets are rolled-up to the executive level

Metric results are weighted and aggregated to provide control, policy, and initiative key indicators

Roll-up View

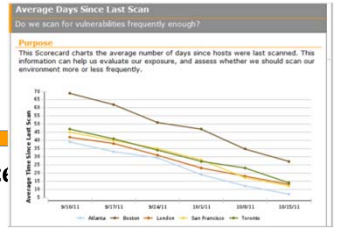




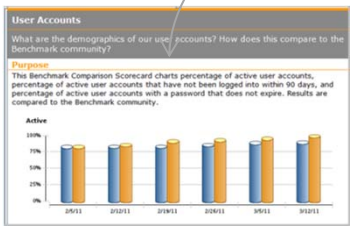
Initiative and Security Process Scorecards

Roll-up View

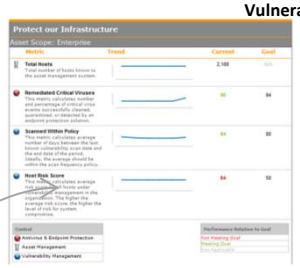
Key Performance Indicators



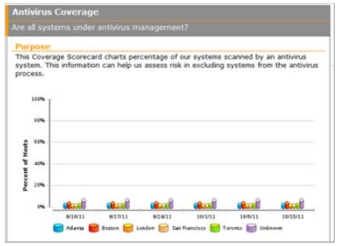
Vulnerability Management



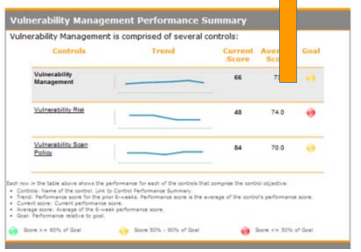
Identity & Access Management



Patching Activity



Antivirus and Endpoint Protection



Configuration Auditing

Initiative Scorecards Across Divisions

Initiative and control performances are weighted and aggregated across divisions

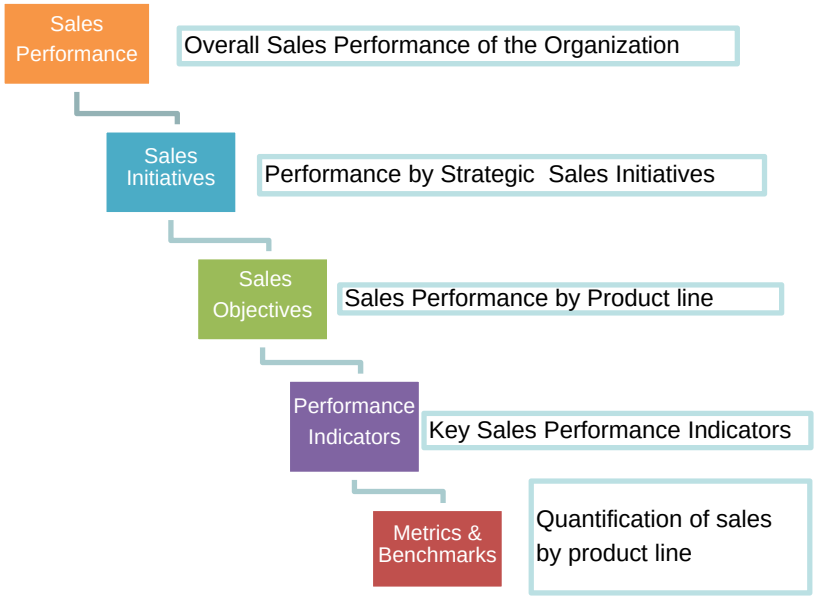
Control metrics are composed of metric results compared to policies and goals

Detailed Operational Security Metrics and Scorecards

Methodology

- Align operational tasks with strategic goals
- Drive performance organization-wide
- Based on hard facts and data

Financial Reporting Roll Up Example



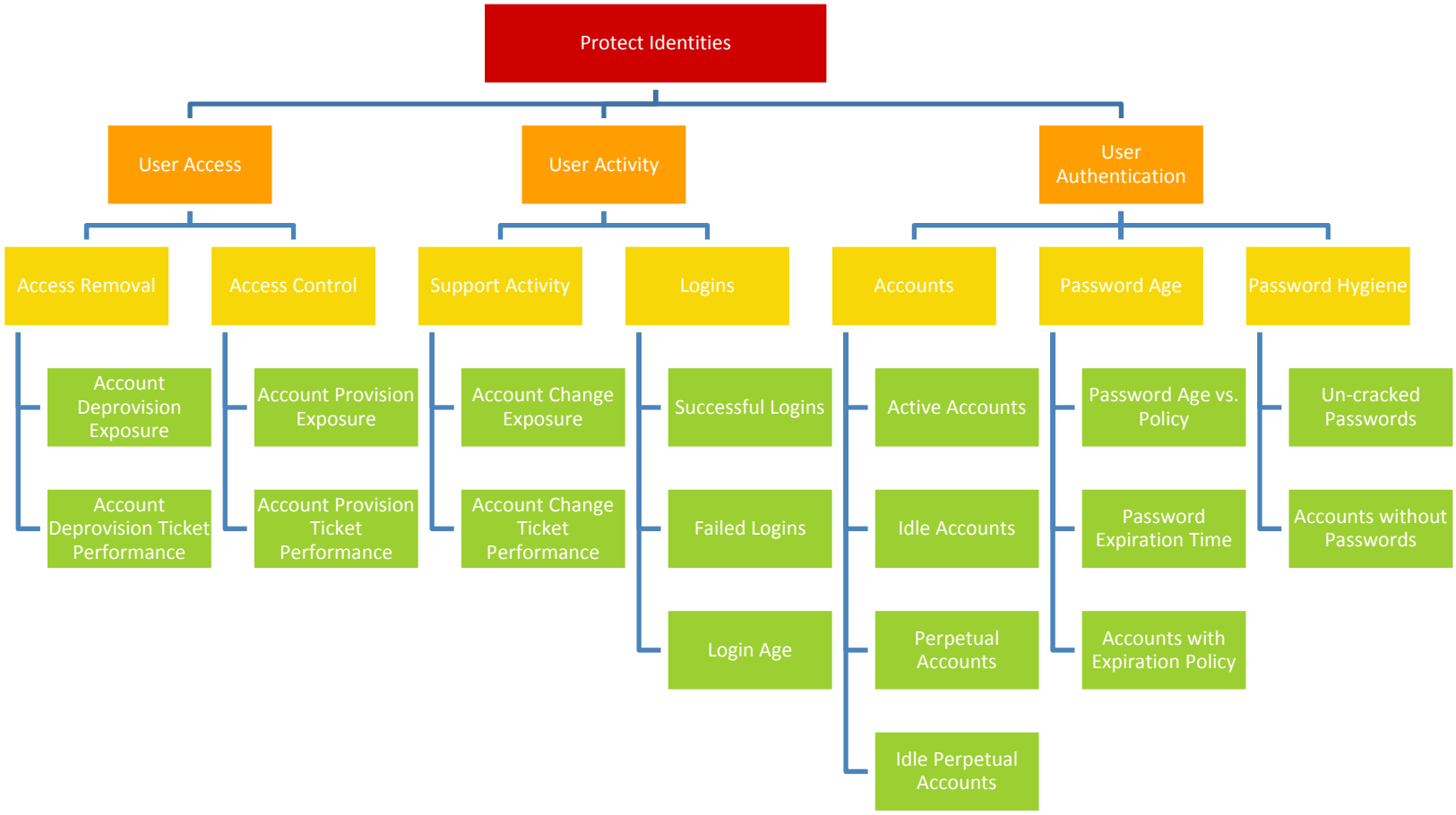
Security Performance Roll Up Example

Attributes of an Actionable Metrics and Scorecards

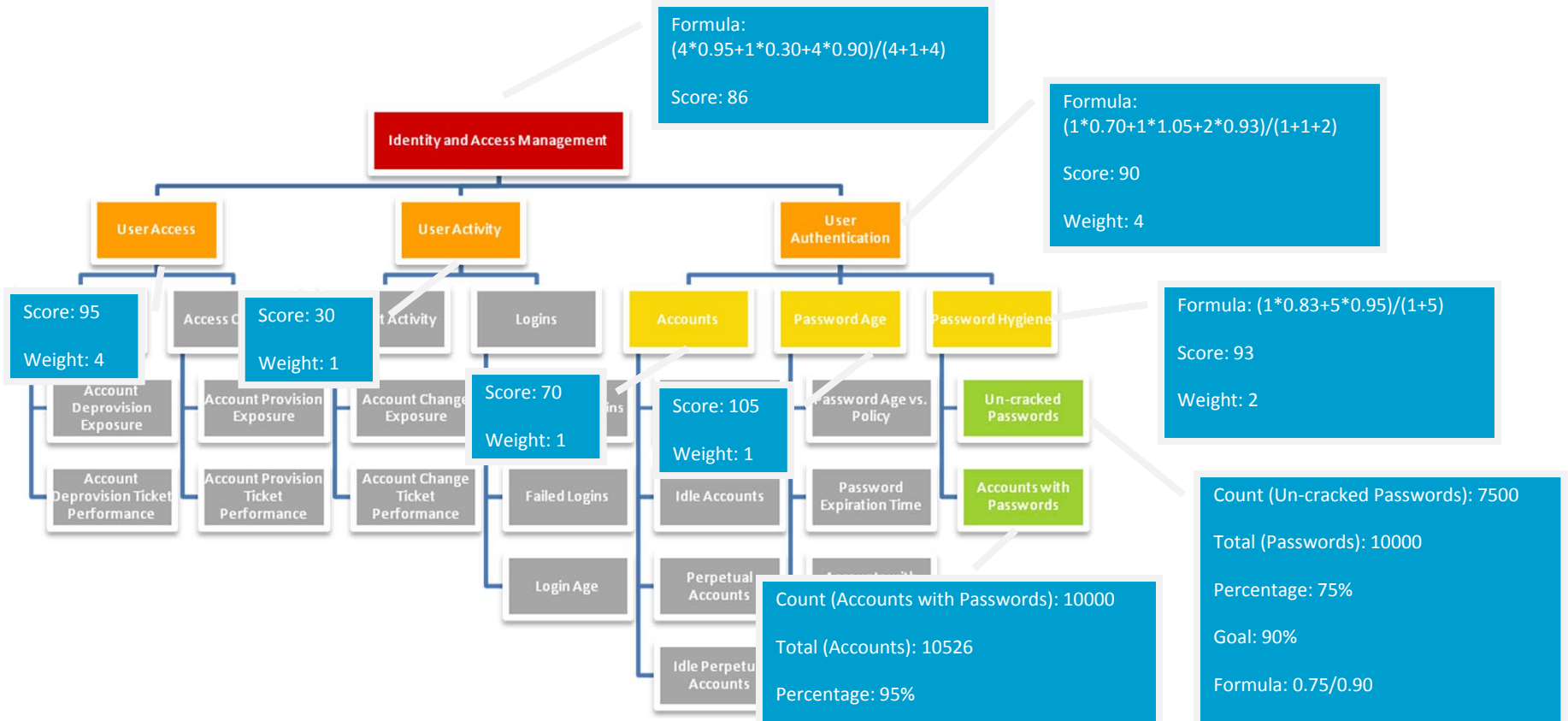
- Controls aligned with GRC objectives
- Assigned ownership
- Measured against specific goals & standards
- Benchmarked against peer performance
- Aggregated by meaningful asset groupings
- Visuals targeted at audience

Initiative Roll Up

Example - Identity & Access Management



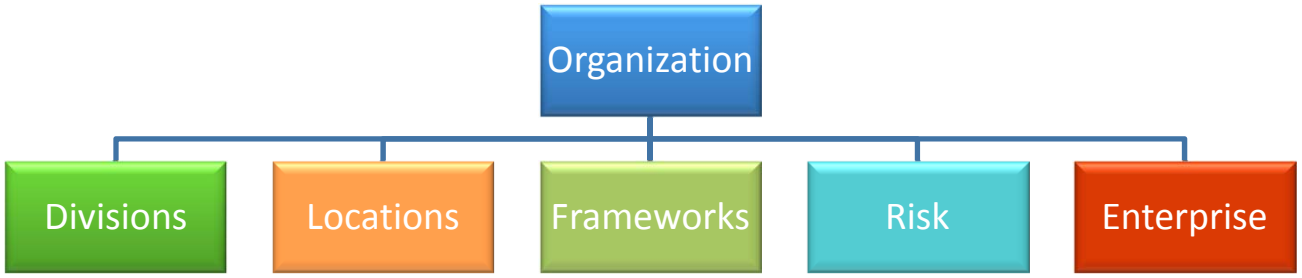
Score Calculation Overview



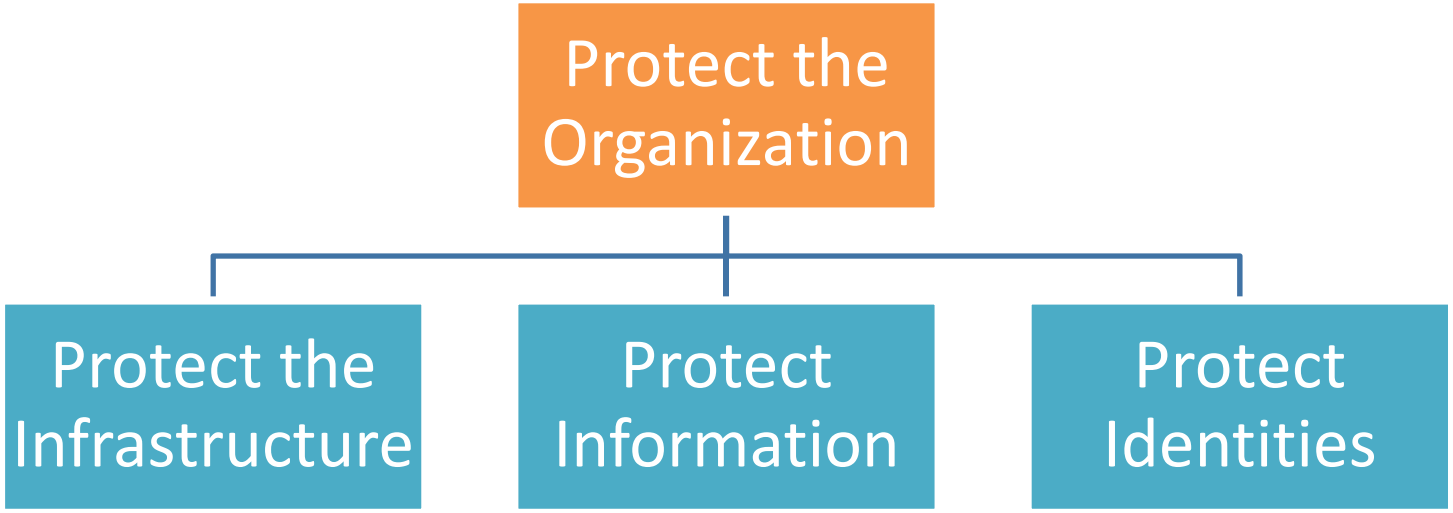
IT Security Governance Program Example Screenshots

Section 1: Enterprise Rollup Scorecards

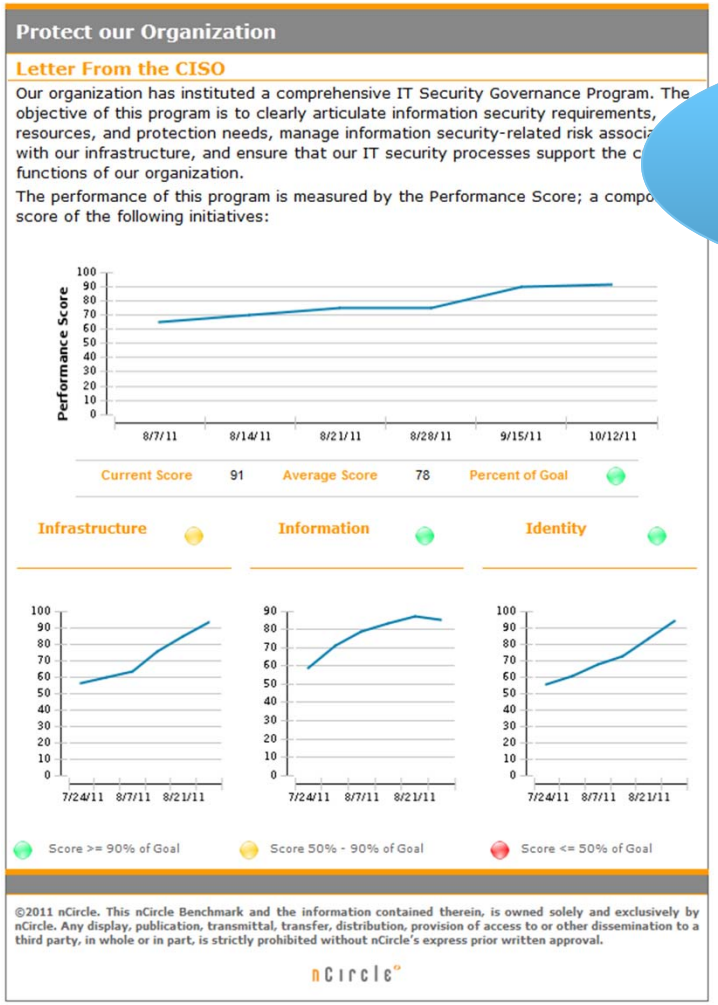
Section 2: Internal Benchmark Scorecards, by Asset Group



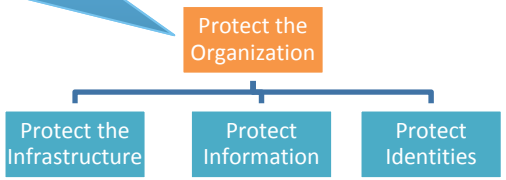
Section 1: Governance Objectives & Initiatives

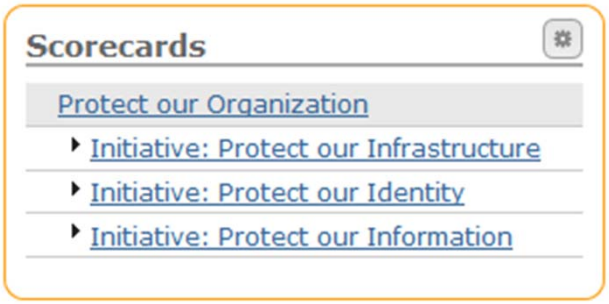


Organizational Overview

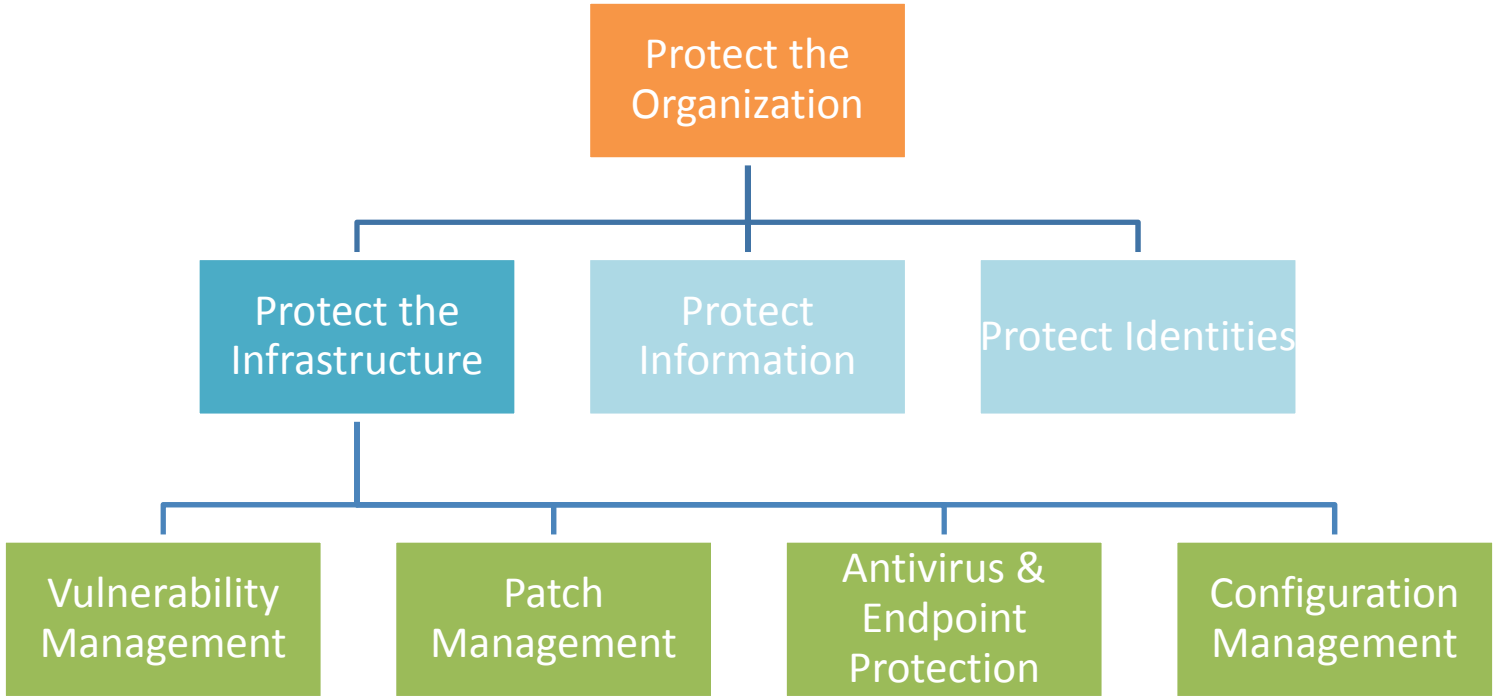


Scorecard Design and Navigation reflect Governance Program





Control Objectives – Protect the Infrastructure



Control Objectives

Protect our Information Performance Summary

Protect our Information is comprised of a series of controls:

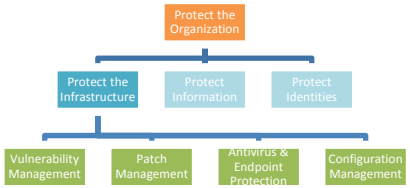
Control Objective	Trend	Current Score	Average Score	Goal
Protect our Infrastructure		85	88	
Antivirus and Endpoint Protection		94	93.0	
Configuration Auditing		92	92.0	
Patch Management		93	72.0	
Vulnerability Management		66	77.0	

Each row in the table above shows the performance for each of the control objectives:

- Control Objective: Name of the control objective. Link to the Control Objective Performance Summary
- Trend: Performance score for the prior 6-weeks. Performance score is the average of the control's performance score.
- Current score: Current performance score.
- Average score: Average of the 6-week performance score.
- Goal: Performance relative to goal.

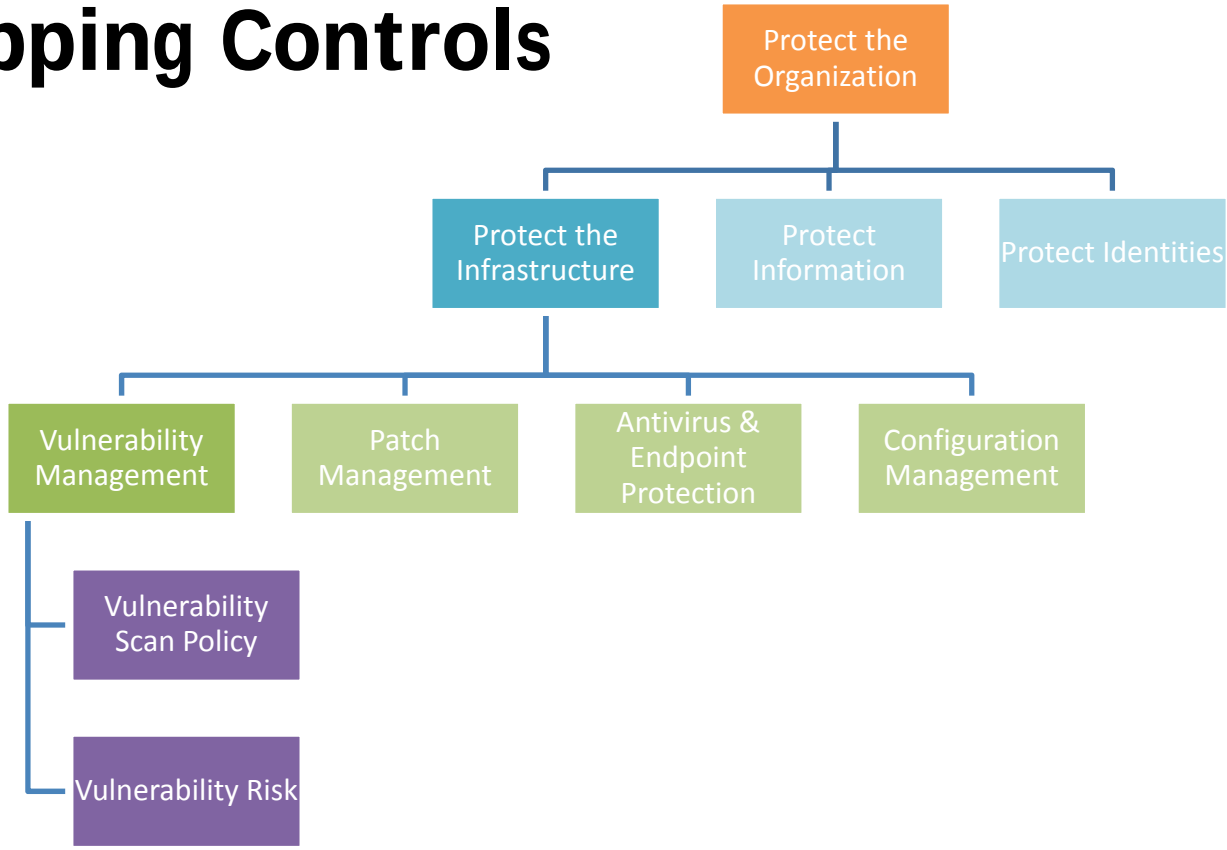
Score >= 90% of Goal Score 50% - 90% of Goal Score <= 50% of Goal

nCircle

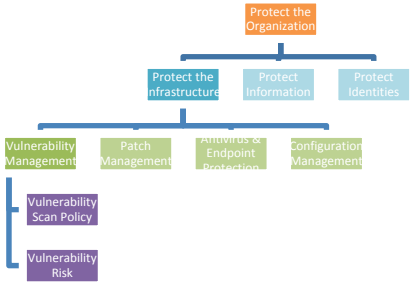


Drilling in to Quickly Identify Problem areas

Mapping Controls



Controls



Vulnerability Management Performance Summary

Vulnerability Management is comprised of several controls:

Controls	Trend	Current Score	Average Score	Goal
Vulnerability Management		66	73	
Vulnerability Risk		48	74.0	
Vulnerability Scan Policy		84	70.0	

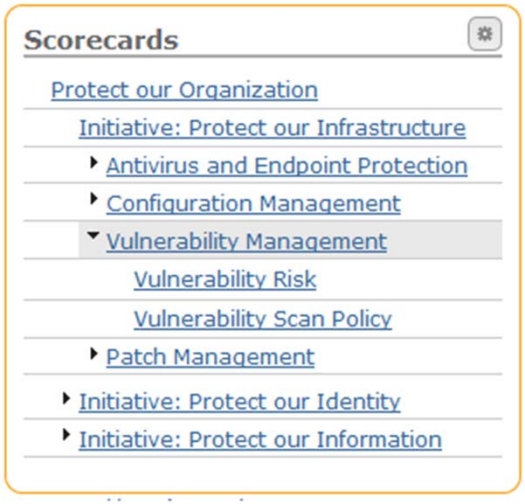
...v in the table above shows the performance for each of the controls that comprise the control objective:

- ...ntrols: Name of the control. Link to Control Performance Summary.
- ...rend: Performance score for the prior 6-weeks. Performance score is the average of the control's performance score.
- Current score: Current performance score.
- Average score: Average of the 6-week performance score.
- Goal: Performance relative to goal.

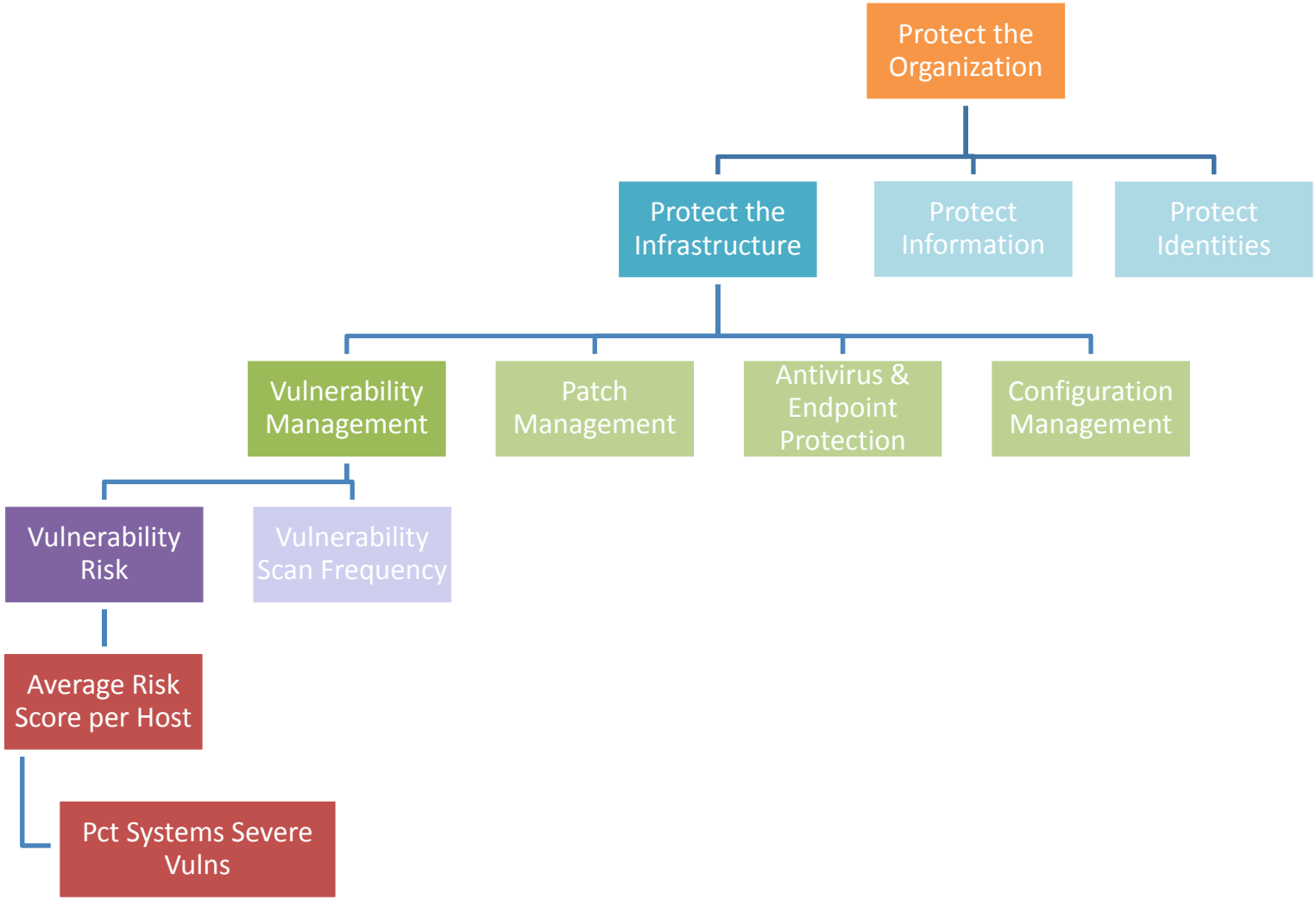
Score >= 90% of Goal Score 50% - 90% of Goal Score <= 50% of Goal

nCircle

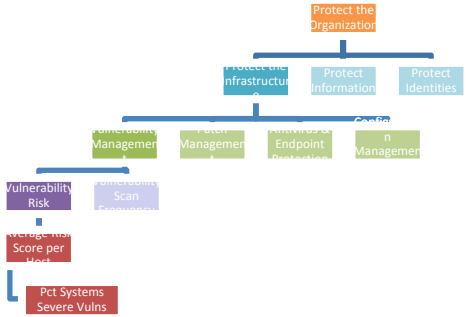
Drill in to detail to determine root cause



Key Performance Indicators



Key Performance Indicators



Vulnerability Risk Performance Summary

Vulnerability Risk is comprised of several key performance indicators:

Key Performance Indicators	Trend	Current Score	Average Score	Goal
Vulnerability Risk		48	74	
Average Risk Score per Host		21	47.0	
Percent of Systems with Severe Vulnerabilities		75	83.0	

Each row in the table above shows the performance for each of the key performance indicators that comprise the control:

- Key Performance Indicators: Name and link to key performance indicator.
- Trend: Performance score for the prior 6-weeks. Performance score is the average of the key performance indicator's performance score.
- Current score: Current performance score.
- Average score: Average of the 6-week performance score.
- Goal: Performance relative to goal.

Score >= 90% of Goal Score 50% - 90% of Goal [illegible] 50% of Goal

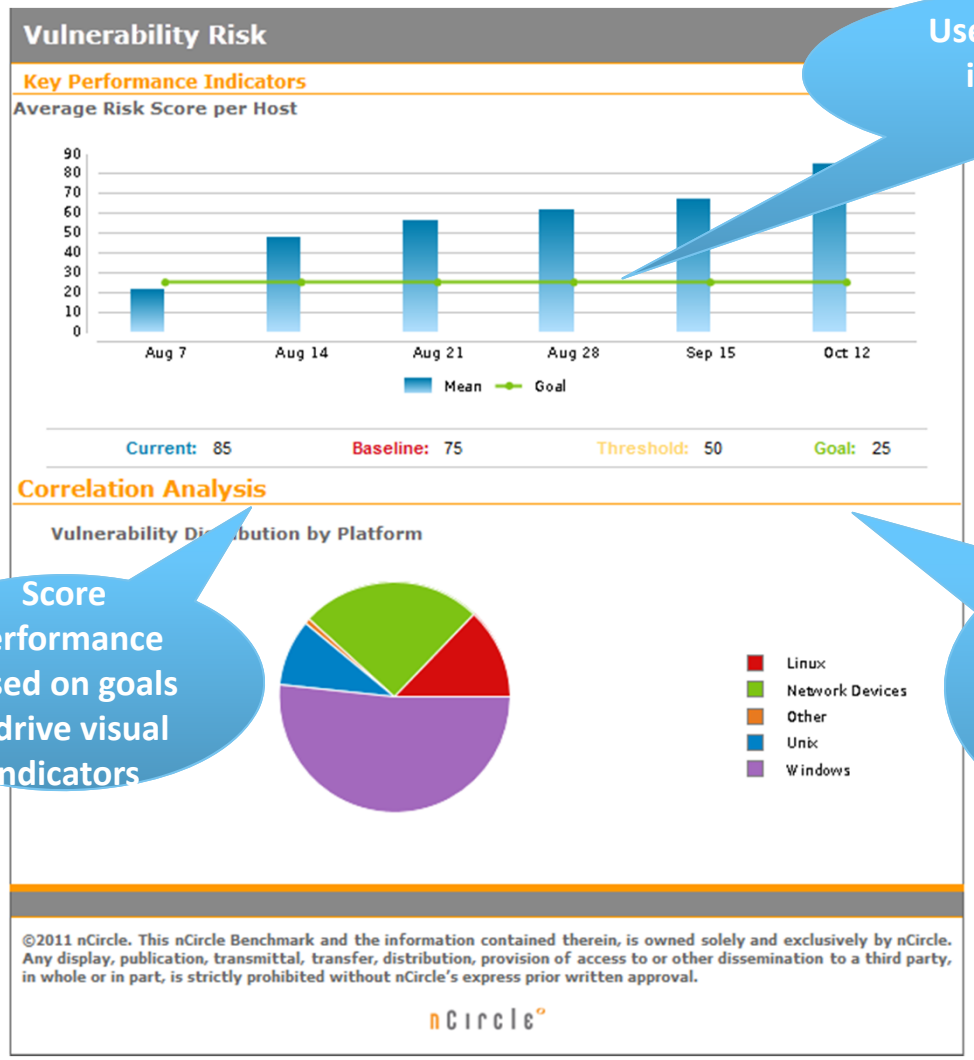
nCircle

Scorecards

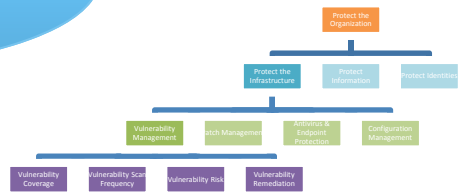
- Protect our Organization
  - Initiative: Protect our Infrastructure
    - Antivirus and Endpoint Protection
    - Configuration Management
    - Vulnerability Management
      - Vulnerability Risk
        - Average Risk Score
        - Severe Vulnerabilities
      - Vulnerability Scan Policy
        - Scan Coverage
  - Initiative: Protect our Identity
  - Initiative: Protect our Information

Map Individual Metrics to KPIs

Performance Analysis



Use Benchmarks to set internal goals and baselines

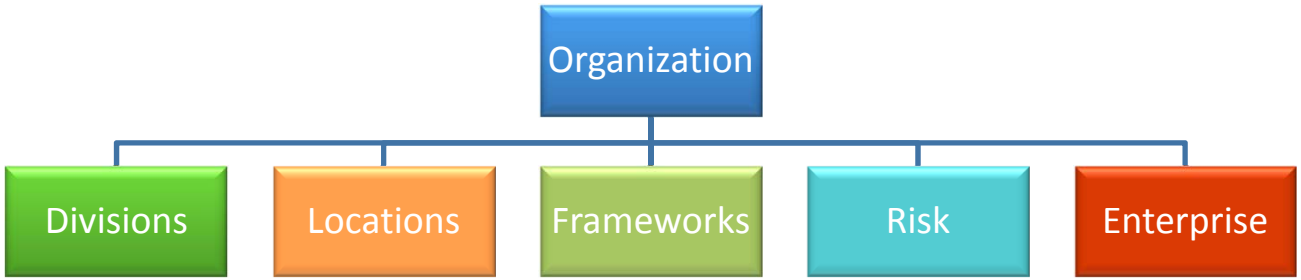


Score performance based on goals & drive visual indicators

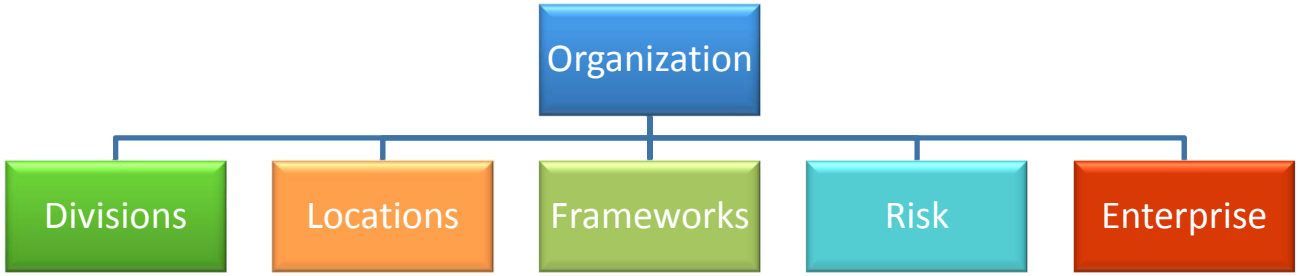
Analyze trends and build correlations between Benchmarks to establish KPI's

Example Organization

- Cambridge Transportation Company
- ‘Green’ transportation company with the following structure:



- Each section will internally benchmark specific areas:
  - Divisions: (Bicycles, Tricycles, Scooters, Wagons, Carriages)
  - Locations: (San Francisco, Boston, Atlanta, London, Toronto)
  - Frameworks: (SOX)
  - Risk: (Sensitive, Non-Sensitive Assets)



Protect our Infrastructure

Asset Scope: Enterprise

Metric	Trend	Current	Goal
Total Hosts Total number of hosts known to the asset management system.		2,180	N/A
Remediated Critical Viruses This metric calculates number and percentage of critical virus events successfully cleaned, quarantined, or detected by an endpoint protection solution.		95	94
Scanned Within Policy This metric calculates average number of days between the last known vulnerability scan date and the end date of the period. Ideally, the average should be within the scan frequency policy.		84	80
Host Risk Score This metric calculates average risk score for all hosts under vulnerability management in the organization. The higher the average risk score, the higher the level of risk for system compromise.		84	50

Control
Antivirus & Endpoint Protectio
Asset Management
Vulnerability Management

Performance Relative to Goal
Not Meeting Goal
Meeting Goal
Not Applicable

©2011 nCircle. This nCircle ... Circle. Any display, publication, tr... arty, in whole or in part, is strictly ...

Scorecards

- Antivirus and Endpoint Protection
  - Enterprise
  - Division
  - Location
  - Framework
  - Risk
- Vulnerability Management
  - Enterprise
  - Division
  - Location
  - Framework
  - Risk

Tell me...

- *What is a Benchmark?*
- *What does this scorecard ...*
- *What can I use ...*
- *What metrics ...*
- *What do the me...*
- *How are the metrics calcul...*
- ***Tell me more...***

Invite Colleagues ▶

Scorecards for each organizational view, can by managed by ACL

Scorecards provide results across security product/domain

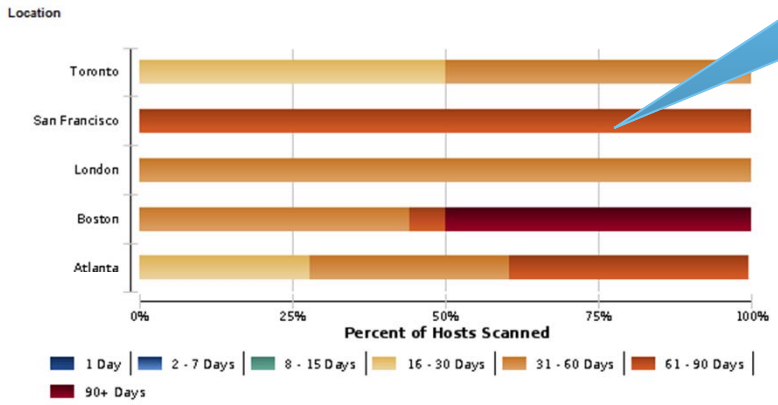
Contextual Scorecards (By Location, By Division)

Vulnerability Scan Schedule Distribution

What is the distribution in time since the last vulnerability scan across systems?

Purpose

This Configuration Scorecard charts distribution in time of when systems are scan
This information can help us assess adherence to scan policy and determine if the
policy is adequate.

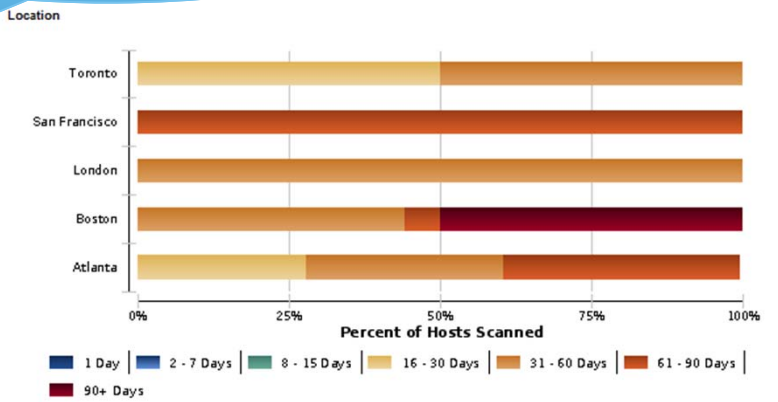


Location	1 Day	2-7 Days	8-15 Days	16-30 Days	31-60 Days	61-90 Days	90+ Days
Atlanta	0	0	0	28	33	39	0
Boston	0	0	0	0	44	6	50
London	0	0	0	0	100	0	0
San Francisco	0	0	0	0	0	100	0
Toronto	0	0	0	50	50	0	0

Internally Benchmark by comparing asset groups

Vulnerability Scan Schedule Distribution

What is the distribution in time since the last vulnerability scan across systems?



...cation	1 Day	2-7 Days	8-15 Days	16-30 Days	31-60 Days	61-90 Days	90+ Days
	0	0	0	28	33	39	0
					44	6	50
						0	0
						100	0
					50	0	0

Standardized metrics and scorecards across asset classes.

Lessons Learned – Attributes of Successful Security Metric Initiatives

- Aligned with the organizations governance objectives & organizations strategy
- Measured against specific goals & standards
- Metrics are derived from real facts and data obtained from the enterprise.