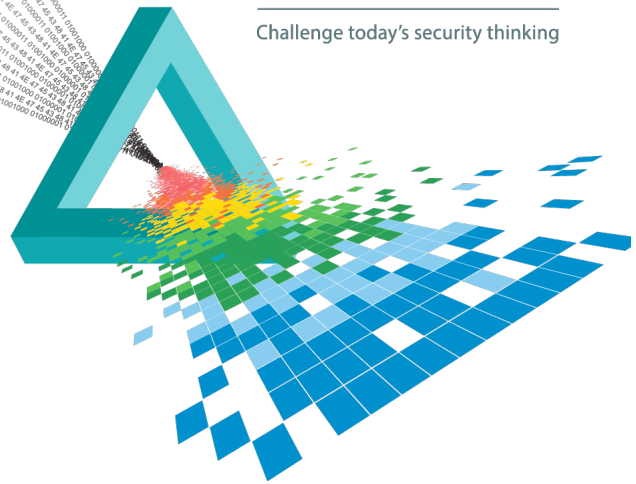
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: DSP-T09



Cookin' Up Metrics With Alex and David: A Recipe For Success!

David Mortman

Chief Security Architect, Dell Software Group
@mortman

Alexander Hutton

Society of Information Risk Analysts
(and I work for a SIFI bank)
@alexhutton

@mortman
@alexhutton

Agenda

LEVEL SETTING (ABOUT SECURITY, ABOUT METRICS)

INTRODUCTION (OR, WHY WE ARE STARVING)

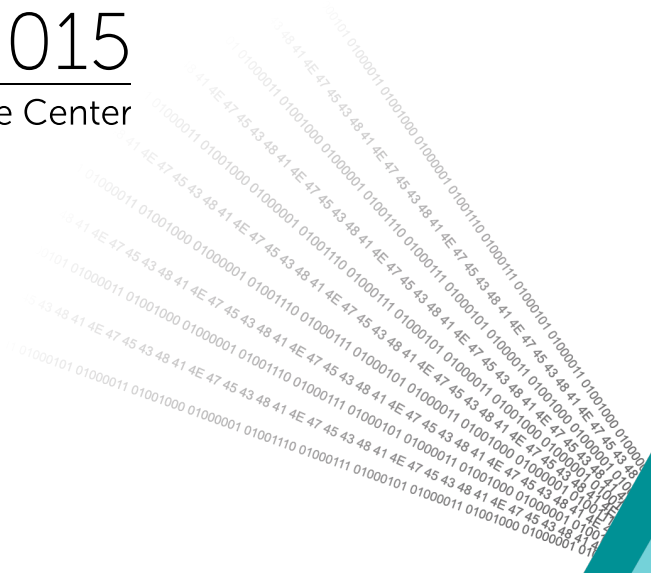
WHAT YOU NEED TO BECOME A METRICS "TOP CHEF"

- Part One - **Knowing and Using the Right Ingredients**,
  (or What's A Useful Metric? Metrics, Measurement, Models, & Meaning)
- Part Two - **Knowing How To Cook**
  (or Building Metrics with GQM for fun and profit)
- Part Three - **Knowing How To Plate**
  (or why your scorecards suck - the value of visualization)

AN EXAMPLE DISH - METRICS & THE NIST CYBERSECURITY FRAMEWORK (NIST CSF)

RSAConference2015

San Francisco | April 20-24 | Moscone Center



@mortman
@alexhutton

#RSAC

LEVELSETTING

@mortman
@alexhutton

- What does your boss want out of this?
- Who are we?
- Our goal for you is….

@mortman
@alexhutton

@mortman
@alexhutton

JIRO ONO IS MY NEW LIFE COACH.

(SORRY RON SWANSON.)

"THRILLING AND BEAUTIFUL"
ANTHONY BOURDAIN

"A WORK OF ART"
★★★★★
TIME OUT NEW YORK

"A FOODIE'S DREAM NIGHT AT THE MOVIES"
TIME

Ten-seat bar in a Tokyo subway station

Eight month waiting list

Three Michelin stars

One 85 year old perfectionist

JIRO DREAMS OF SUSHI

Fall in love with your work


GORDON RAMSAY, AN EXPERT CHEF?
THAT'S ADORABLE
quickmeme.com

@mortman
@alexhutton

- It’s important for us understand…

@mortman
@alexhutton

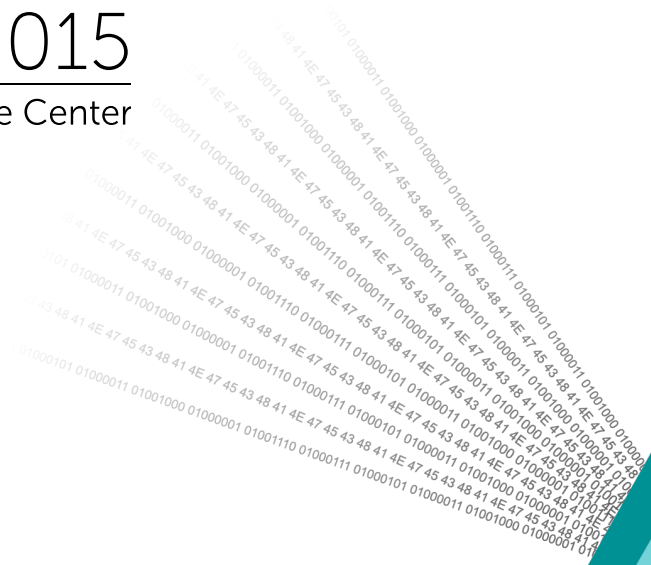
- There is no “Secure”, only Securing…

@mortman
@alexhutton

- …and so there is no Mathematical "Proof" for "Secure"… and so
- …metrics cannot provide "secure" any more than your controls can.

RSA Conference2015

San Francisco | April 20-24 | Moscone Center



@mortman
@alexhutton

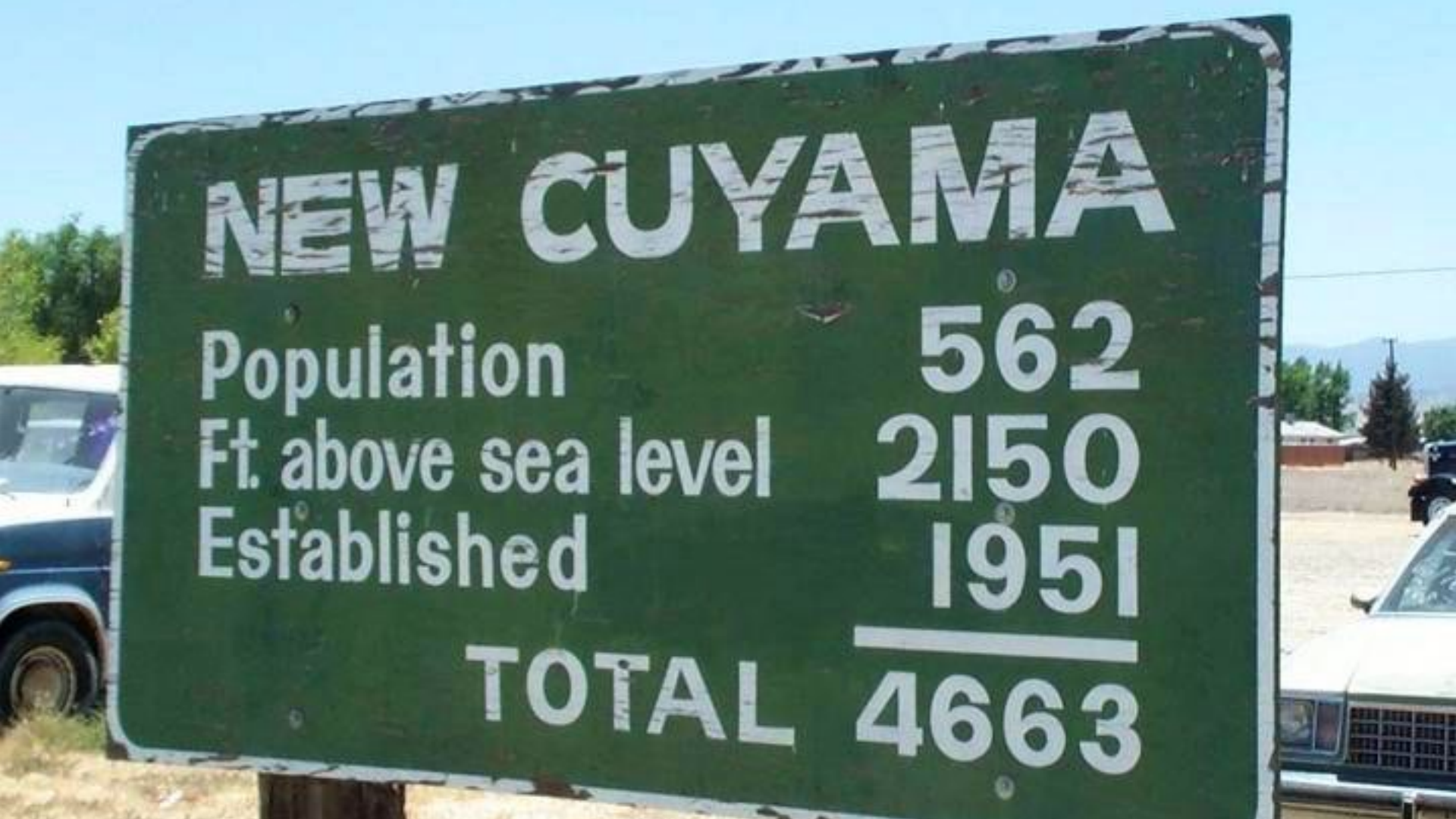
#RSAC

INTRODUCTION

*

@mortman
@alexhutton

The current state of metrics in the industry...


NEW CUYAMA
Population 562
Ft. above sea level 2150
Established 1951
TOTAL 4663

@mortman
@alexhutton

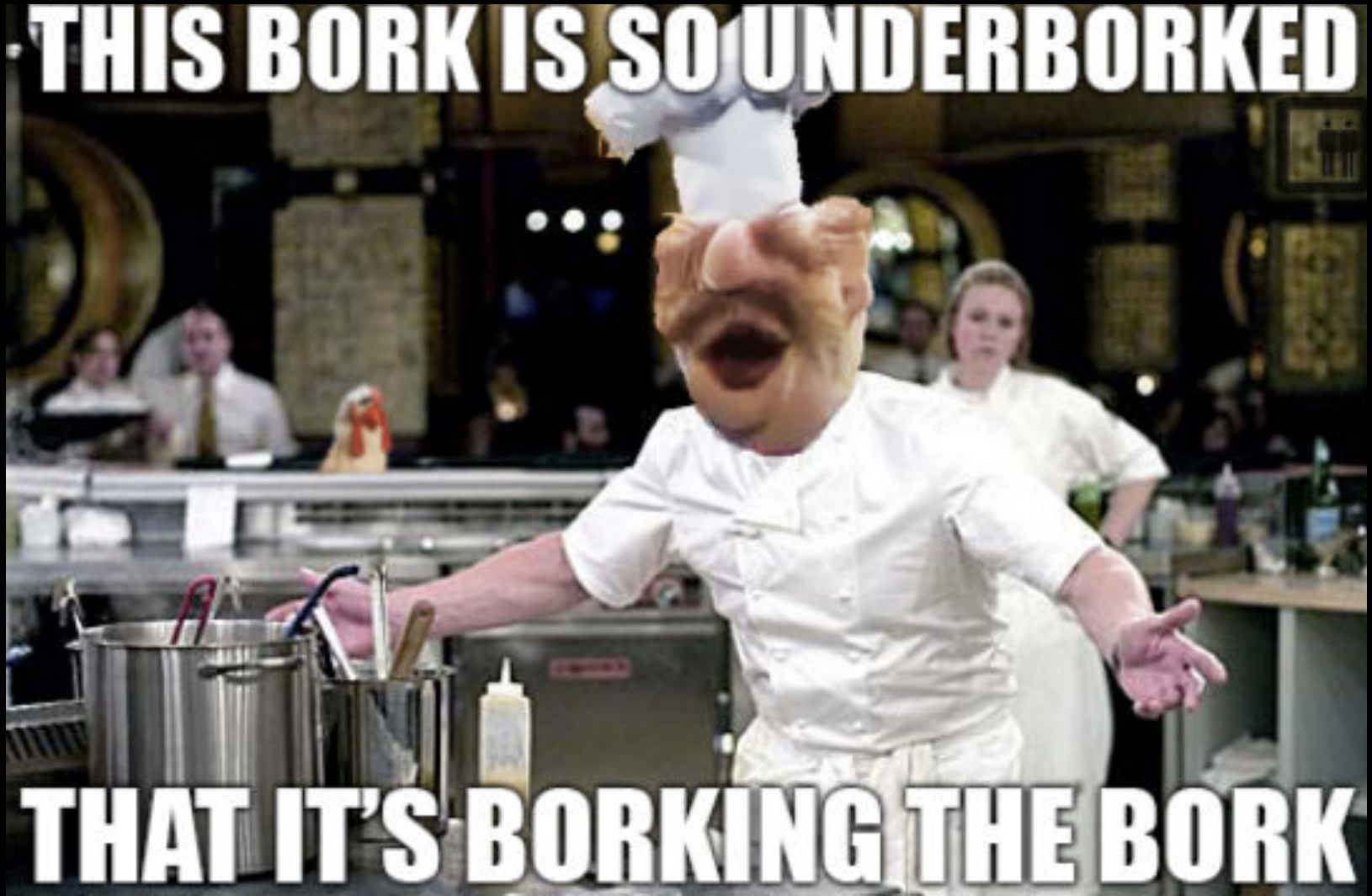
Just Kidding

@mortman
@alexhutton

Just Kidding - It's Worse

@mortman
@alexhutton

WHY?


THIS BORK IS SO UNDERBORKED
THAT IT'S BORKING THE BORK


THIS BORK IS SO UNDERBORKED
SECURITY!
THAT IT'S BORKING THE BORK

@mortman
@alexhutton

Why? Aggregate Meaning, Context is missing.

@mortman
@alexhutton

Why? Aggregate Meaning, Context is missing.

@mortman
@alexhutton

Why? Aggregate Meaning, Context is missing.

@mortman
@alexhutton

Why? Aggregate Meaning, Context is missing.

@mortman
@alexhutton

Why? Aggregate Meaning, Context is missing.

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

PART ONE:
KNOWING THE RIGHT INGREDIENTS
MAKING A USEFUL METRIC

@mortman
@alexhutton

#RSAC

What is a metric?

@mortman
@alexhutton

What is a metric?

- Control Effectiveness is “medium”

- - arguably?

@mortman
@alexhutton

What is a metric?

- We have 53 “medium” control effectiveness ratings

- - now we’re getting somewhere.

@mortman
@alexhutton

What is a metric?

- We have 53 “medium” control effectiveness ratings, which represents 1/3 of our overall ratings, the other 2/3 are all “strong”

- - now we’ve got a story.

@mortman
@alexhutton

What is a metric?

- We have 53 “medium” control effectiveness ratings, which represents 1/3 of our overall ratings, the other 2/3 are all “strong”

- % CONTROLS “EFFECTIVE - STRONG” = 67%

- **- now we’ve got a metric!**

@mortman
@alexhutton

What is a metric?

- We have 53 “medium” control effectiveness ratings, which represents 1/3 of our overall ratings, the other 2/3 are all “strong”

- % CONTROLS “LESS THAN EFFECTIVE - STRONG” = 33%

- - now we’ve got a BETTER metric, because we’ve highlighted the ***addressable space*.**

@mortman
@alexhutton

What is a metric?

- It would be easy for me to tell you that a metric is “quantitative information” and leave it at that.

- In fact most folks would...

@mortman
@alexhutton

What is a metric? - Definition

- A metric is quantitative information that (helps) ***tells a story.***

@mortman
@alexhutton

What is a metric? - Purpose

@mortman
@alexhutton

Why is a metric?

- A metric is quantitative information that (helps) ***tells a story.***

- That story is designed to cause a decision (action/no action).

@mortman
@alexhutton

What is a metric?

- That story can either be obvious or part of a larger picture.

@mortman
@alexhutton

What is a metric?

- That story can either be obvious or part of a larger picture.

@mortman
@alexhutton

WHAT ARE THE **RIGHT** INGREDIENTS?

@mortman
@alexhutton

Things to Make Metrics About

- Security Stuff
- Business Stuff

@mortman
@alexhutton

THE RIGHT INGREDIENTS - SECURITY STUFF

- Only four “types” of information

@mortman
@alexhutton

THE RIGHT INGREDIENTS - BUSINESS STUFF

What matters most to your organization?

MONEY & TIME

@mortman
@alexhutton

(The most important metrics = money & time)

- Anytime you can report a metric using **money** or **time** as a part of the equation, you win.
  - This is why the best **risk** statements are Frequency x Impact
- Even if you can just allude to money or time,

- it's what the executive is thinking about in the back of their head - so it's a win.

The purpose of your metrics/risk program?

- Create time or money
- Save time or money

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

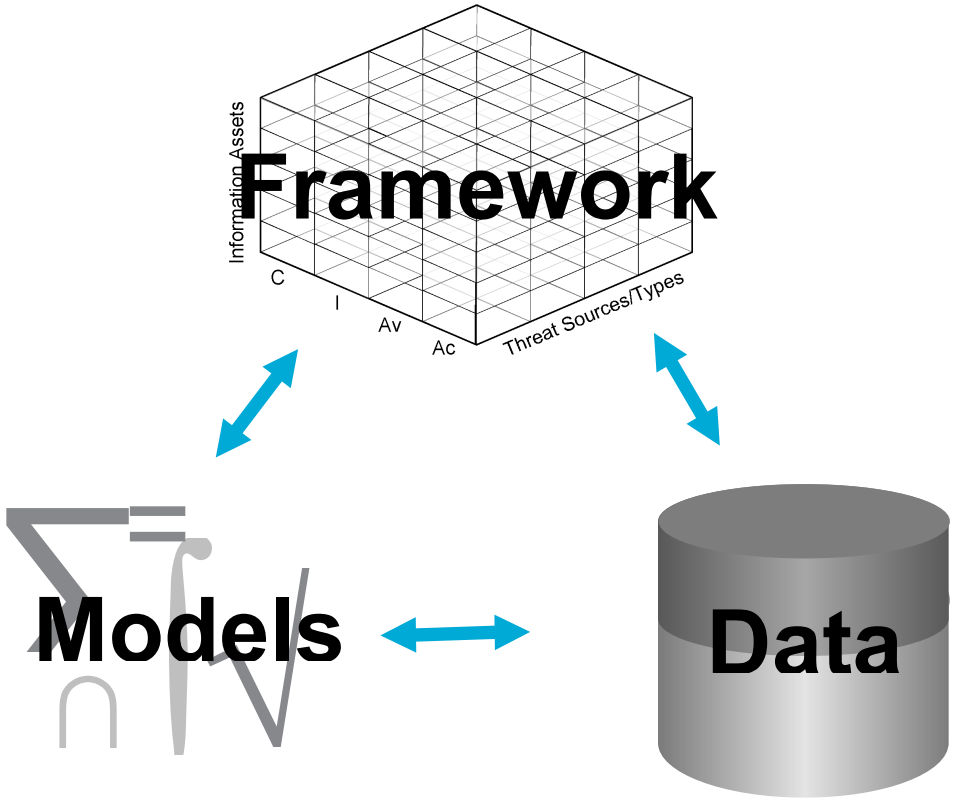
PART TWO:
KNOWING HOW TO COOK
TECHNIQUES FOR METRIC CREATION

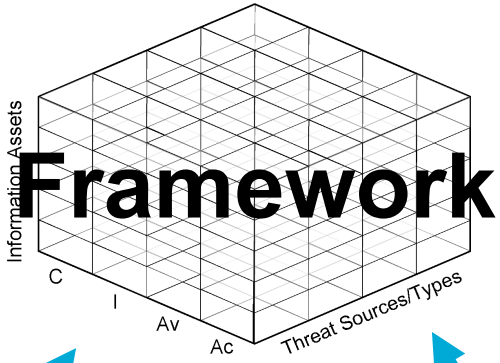
@mortman
@alexhutton

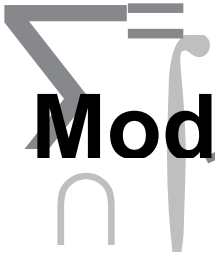
#RSAC

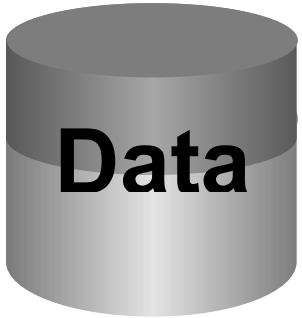
@mortman
@alexhutton

KNOWING HOW TO COOK
BRINGING TOGETHER INGREDIENTS


Framework
Information Assets
C
I
Av
Ac
Threat Sources/Types
Models
Data


Framework
Information Assets
C
I
Av
Ac
Threat Sources/Types


Models


Data

RSAConference2015

San Francisco | April 20-24 | Moscone Center

MASTER CHEF TECHNIQUE: GOAL, QUESTION, METRIC (GQM)

@mortman
@alexhutton

#RSAC

@mortman
@alexhutton

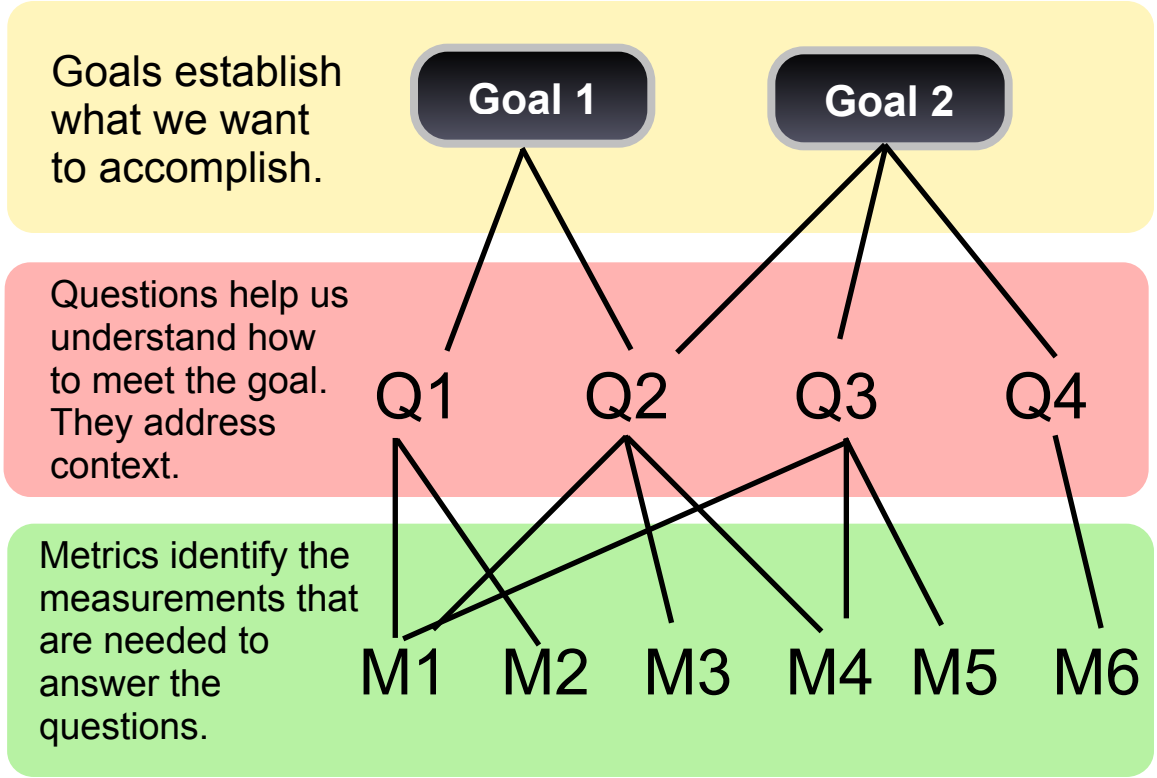
Goal, Question, Metric

- **Conceptual level (goal)**
- ***goals*** defined for an object for a variety of reasons, with respect to various models, from various points of view.
- **Operational level (question)**
- ***questions*** are used to define models of the object of study and then focuses on that object to characterize the assessment or achievement of a specific goal.
- **Quantitative level (metric)**
- ***metrics***, based on the models, is associated with every question in order to answer it in a measurable way.

Victor Basili

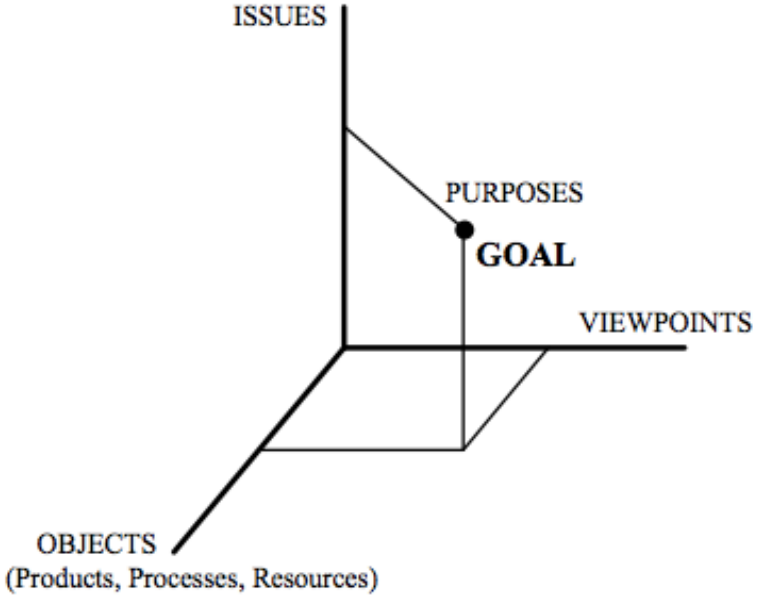
@mortman
@alexhutton

GQM For Fun & Profit



@mortman
@alexhutton

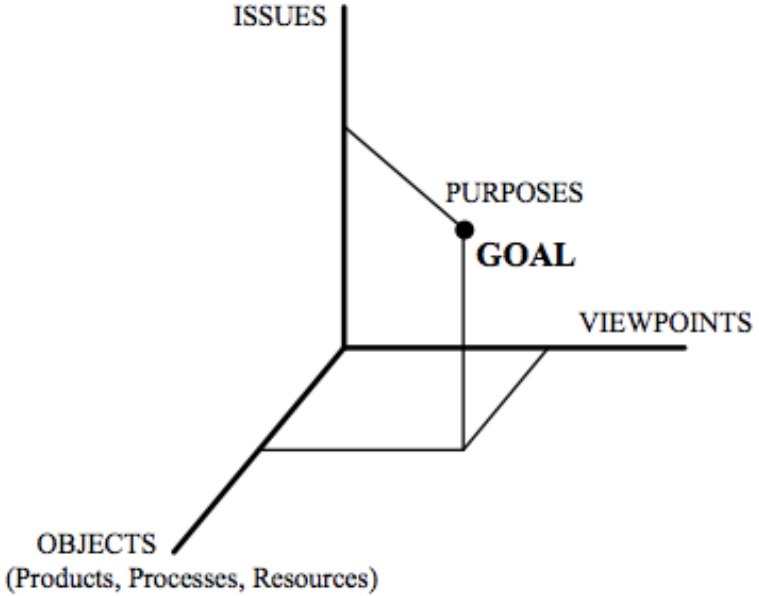
Regarding your Goals



1. Issue
2. Object (process)
3. Viewpoint
4. Purpose

@mortman
@alexhutton

Regarding your Goals



1. Issue: Timeliness
2. Object (process): Firewall Change Request Processing
3. Viewpoint: Project Manager
4. Purpose: Improve(?)

@mortman
@alexhutton

An Example

Goal	Purpose Issue Object (process) Viewpoint	Improve the timeliness of change request processing from the project manager's viewpoint
Question		What is the current change request processing speed?
Metrics		Average cycle time Standard deviation % cases outside of the upper limit
Question		Is the performance of the process improving?
Metrics		$\frac{\text{Current average cycle time}}{\text{Baseline average cycle time}} * 100$ Subjective rating of manager's satisfaction

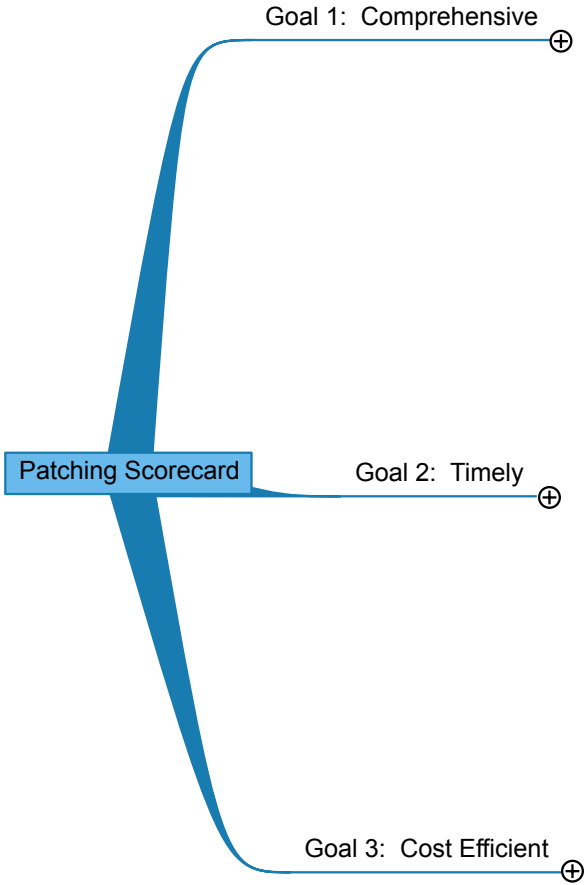
RSAConference2015

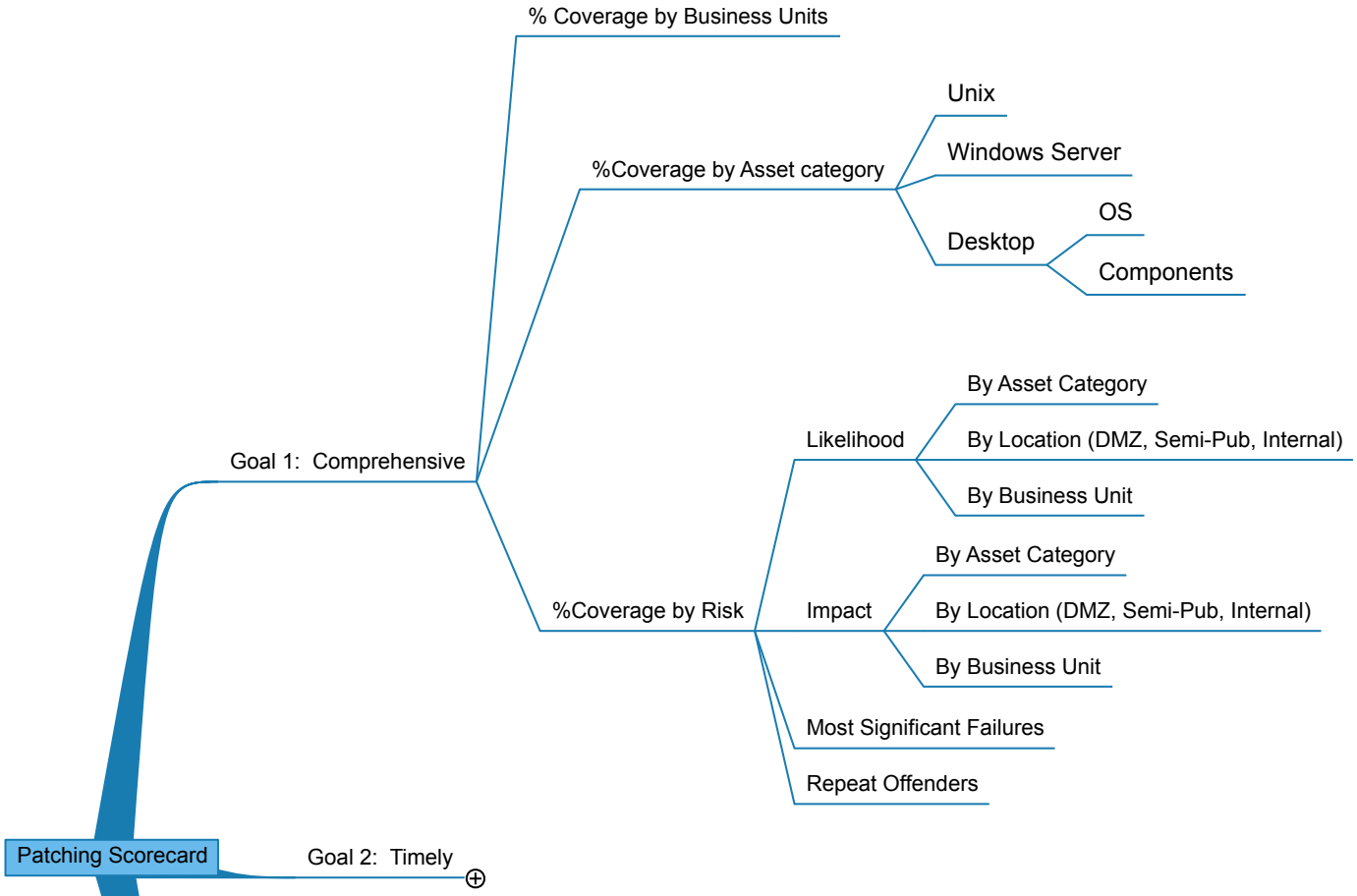
San Francisco | April 20-24 | Moscone Center

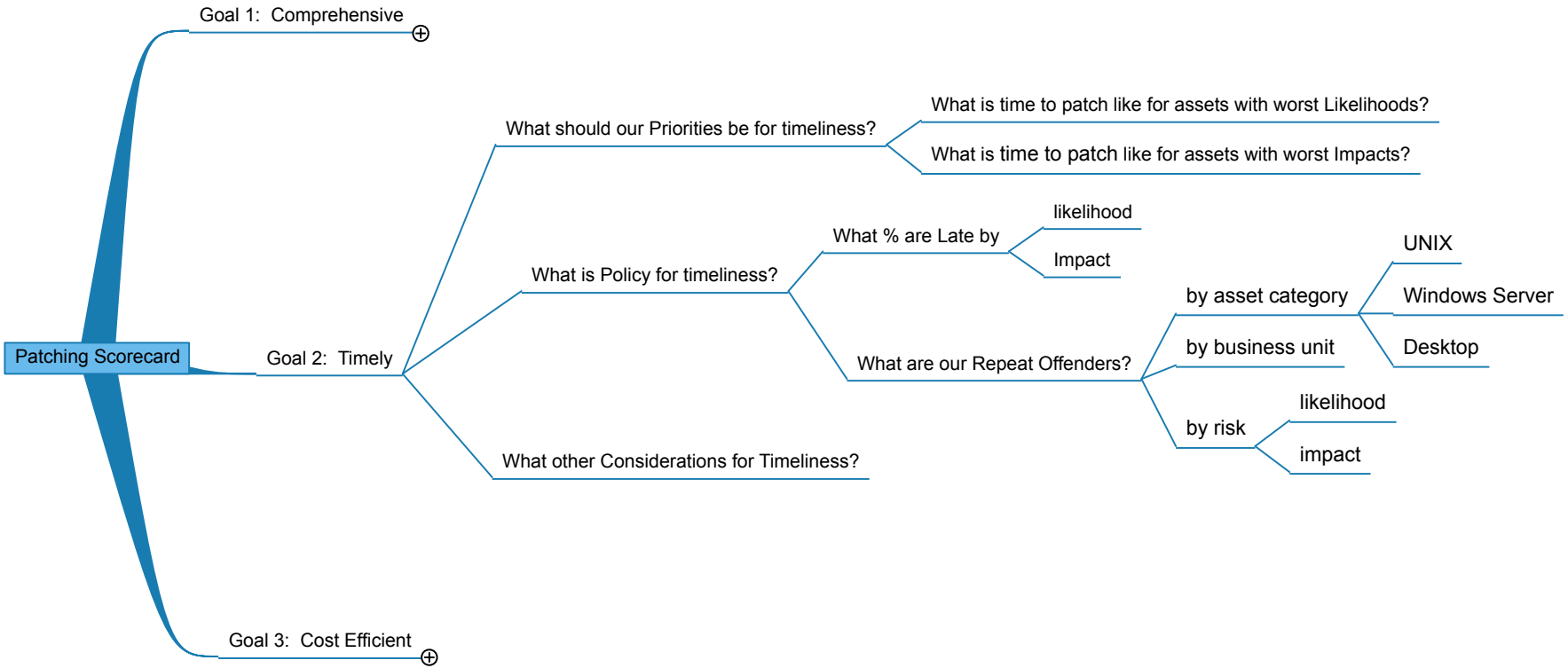
AN EXAMPLE - PATCH MANAGEMENT GQM SCORECARD

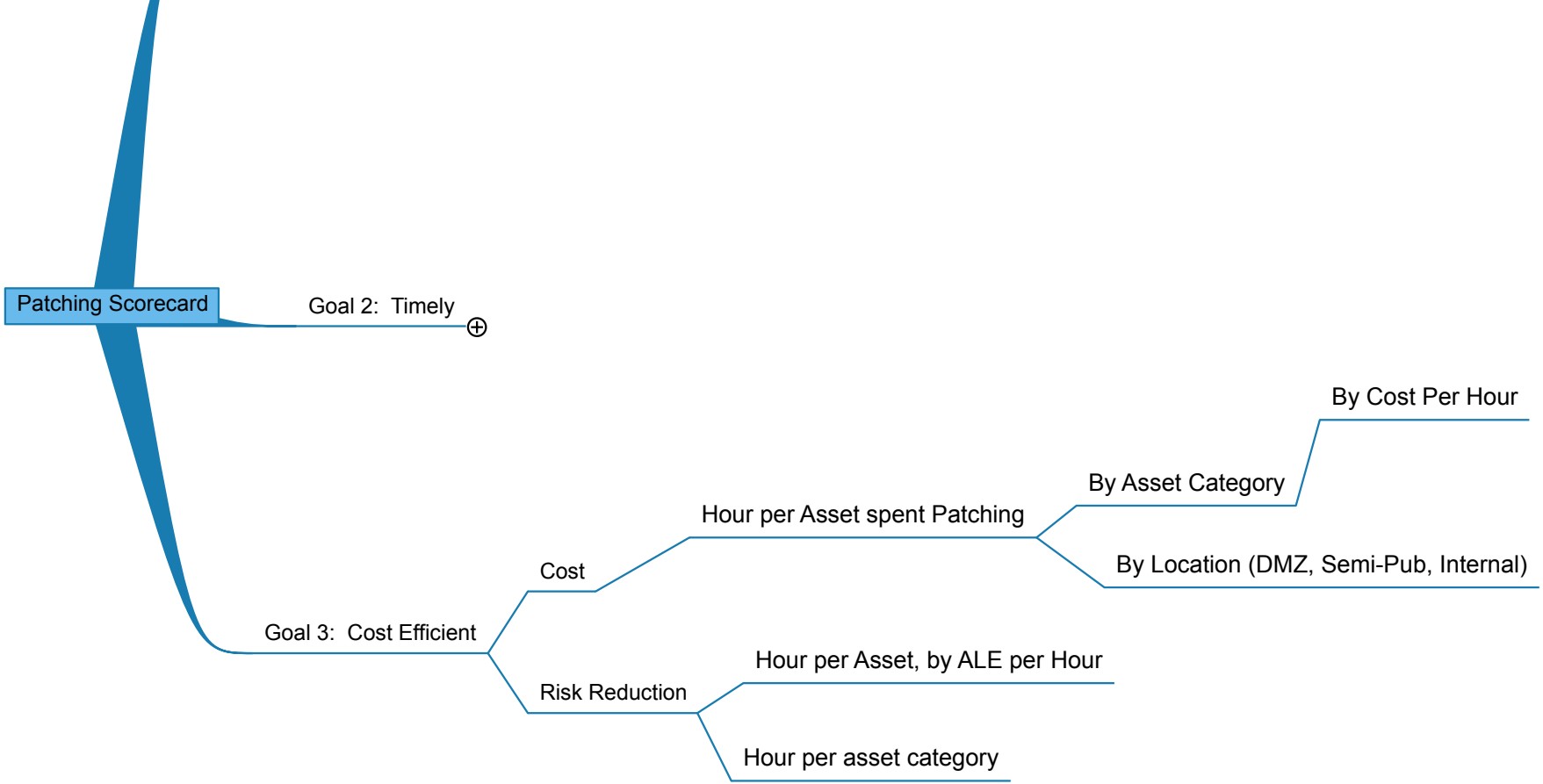
@mortman
@alexhutton

#RSAC

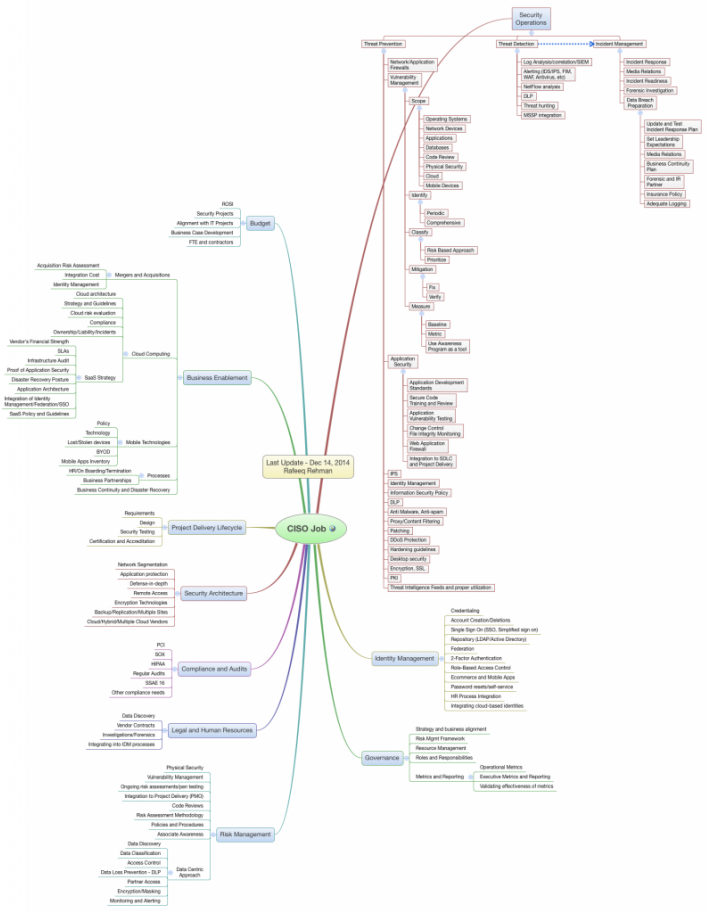

Goal 1: Comprehensive
Patching Scorecard
Goal 2: Timely
Goal 3: Cost Efficient


Patching Scorecard
Goal 1: Comprehensive
% Coverage by Business Units
%Coverage by Asset category
Unix
Windows Server
Desktop
OS
Components
%Coverage by Risk
Likelihood
By Asset Category
By Location (DMZ, Semi-Pub, Internal)
By Business Unit
Impact
By Asset Category
By Location (DMZ, Semi-Pub, Internal)
By Business Unit
Most Significant Failures
Repeat Offenders
Goal 2: Timely

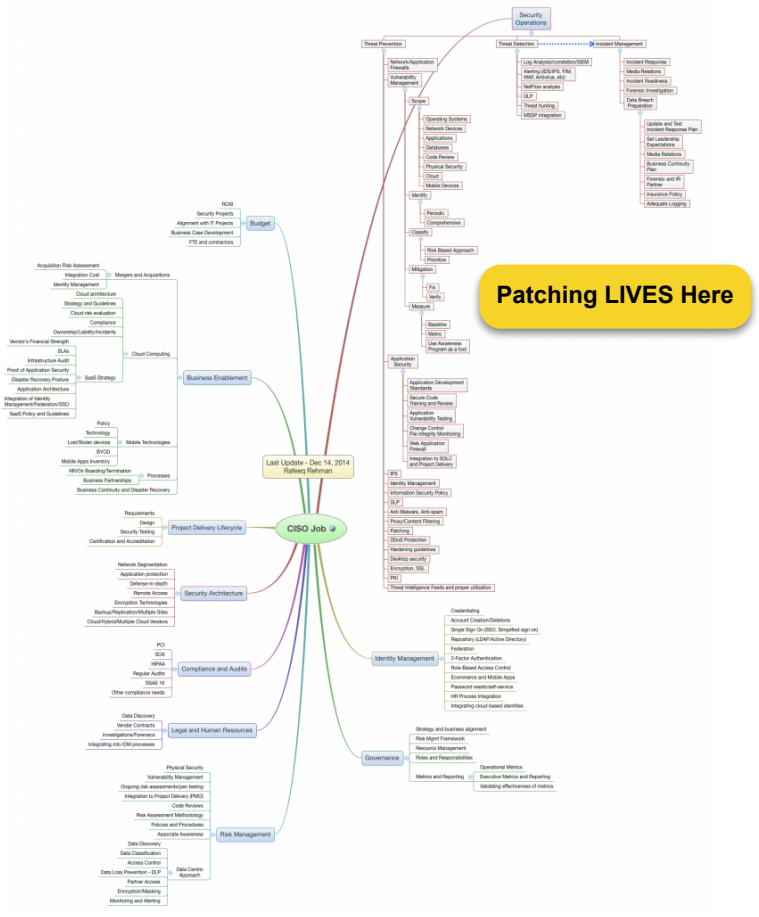

Patching Scorecard
Goal 1: Comprehensive
Goal 2: Timely
Goal 3: Cost Efficient
What should our Priorities be for timeliness?
What is time to patch like for assets with worst Likelihoods?
What is time to patch like for assets with worst Impacts?
What is Policy for timeliness?
What % are Late by
likelihood
Impact
What are our Repeat Offenders?
by asset category
UNIX
Windows Server
Desktop
by business unit
by risk
likelihood
impact
What other Considerations for Timeliness?


Patching Scorecard
Goal 2: Timely
Goal 3: Cost Efficient
Cost
Hour per Asset spent Patching
By Asset Category
By Cost Per Hour
By Location (DMZ, Semi-Pub, Internal)
Risk Reduction
Hour per Asset, by ALE per Hour
Hour per asset category

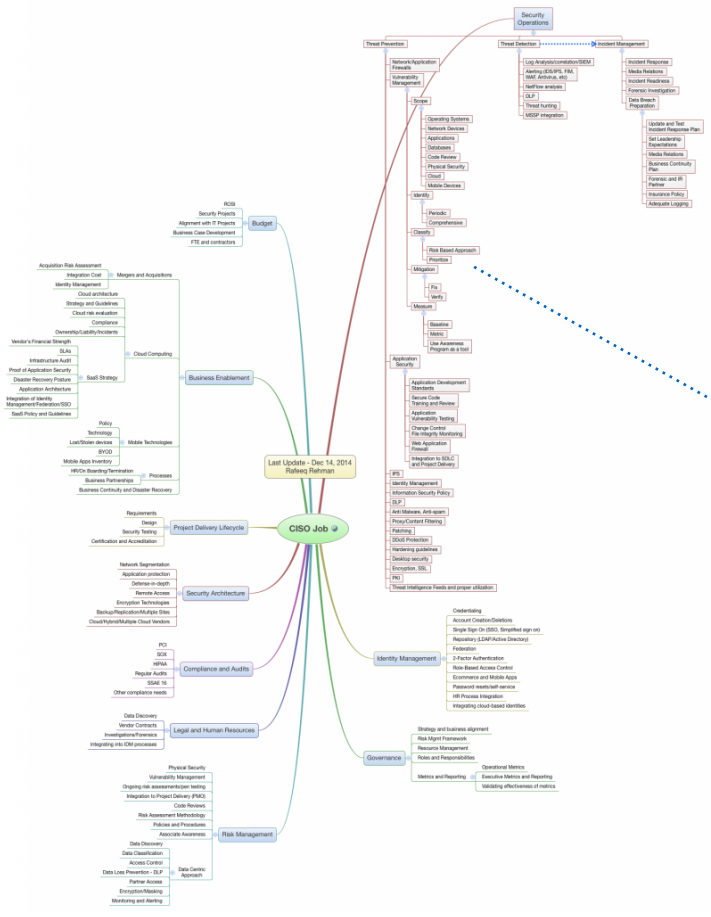
Work of Rafeeq Rehman: http://rafeeqrehman.com/

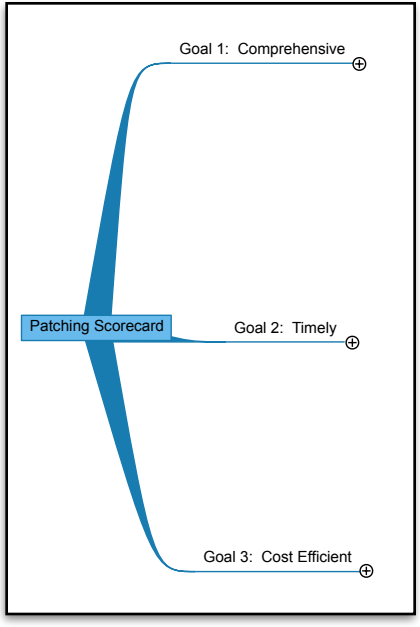


Work of Rafeeq Rehman: http://rafeeqrehman.com/



Work of Rafeeq Rehman: http://rafeeqrehman.com/

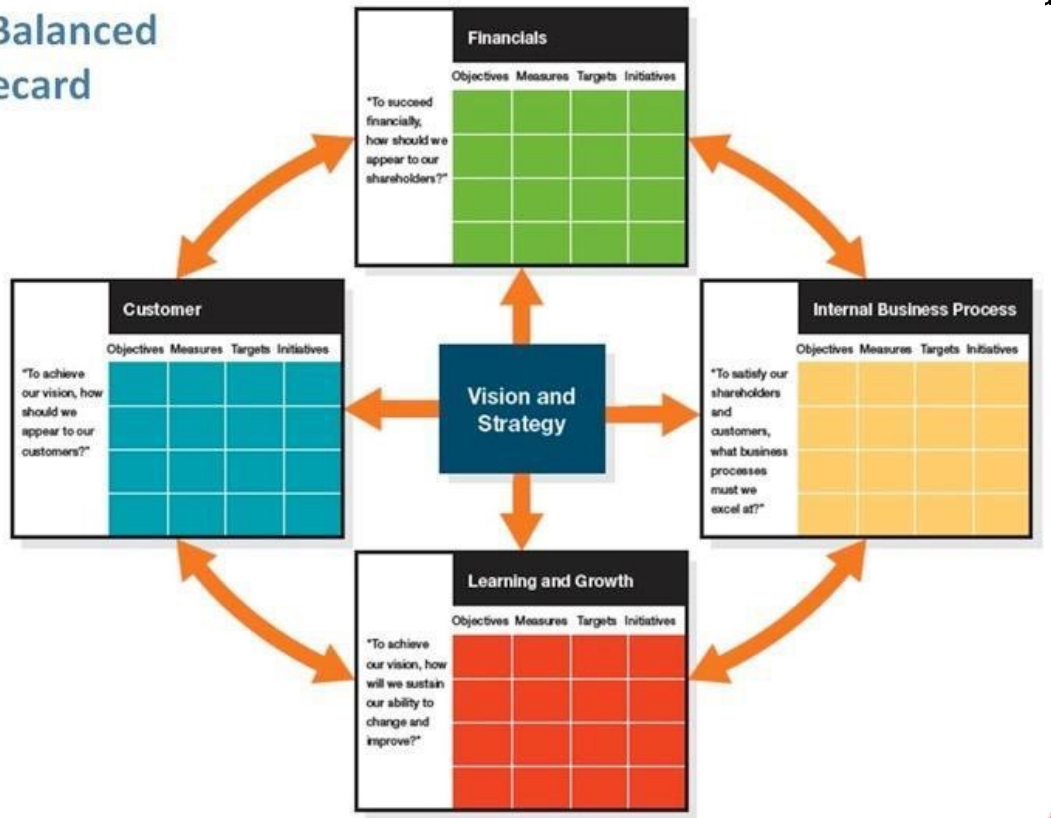




A Note On GQM

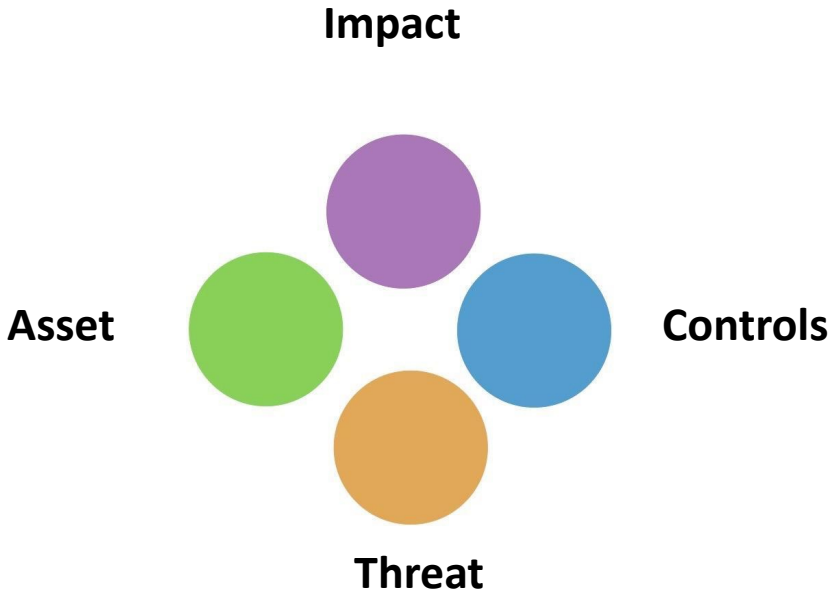
- Works really well in conjunction with a **Balanced Scorecard**
- Can be used well with COBIT's concepts of **outcome measures** and **performance indicators**
- More importantly, it can work in your environment with, say, **VERIS categories**.

Scorecarding



@mortman
@alexhutton

Balanced Scorecard for Security Stuff

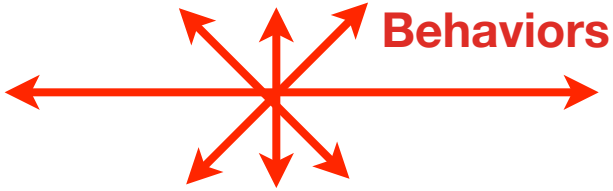


Balanced Scorecard for IT GRC

@mortman
@alexhutton

IT Operations
Applications development
- Project management
- System development life cycle
Production support
- Production control & operation
- job scheduling
System backups
Technical architecture
Network design management &
Help desk
Information security Governance
BCP/DR
Contract administration & vendor

IT Strategic Planning &
IT Steering Committee / Priority Process
IT Strategy & Architectural standards
IT Project Tracking
Support for strategic enterprise initiatives



IT Financials
IT Operating budget
IT Capital budget
IT Asset management
IT Contract management
IT Resource allocation and planning

IT Control
Information Management Policies
- Corporate
- IT departmental
Standards - CoBIT, ITIL, ISO, etc.
Practices & procedures
System documentation management
Quality assurance
Regulatory compliance
- FFIEC Requirements
- Escalation procedures
- Disclosure procedures

RSAConference2015

San Francisco | April 20-24 | Moscone Center

PART THREE:
KNOWING HOW TO PLATE
OR, SCORECARDS!

@mortman
@alexhutton

#RSAC

@mortman
@alexhutton

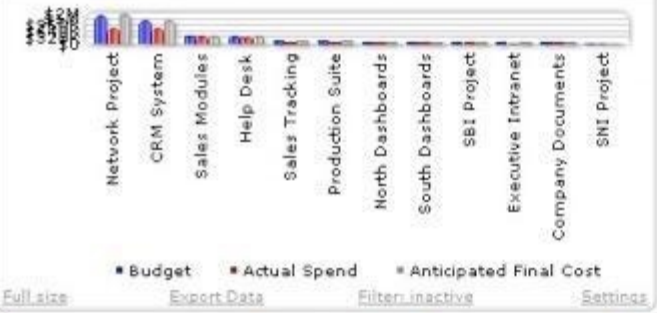
@mortman
@alexhutton

Stephen Few.

Buy everything he makes.

Do everything he says.

Cost, Budget and Anticipated Cost



Full size | Export Data | Filter: inactive | Settings

Current Risks

Showing 1 to 44 of 44

Category	Risk	Project	Milestone	Issue	Action	Respons
Category A	High	Network Project	Order	Budget discussions ongoing as potentially overbudget already	Continue to examine costs etc	PM
Category A	High	Network Project	Order	Resources not yet confirmed due to budget Order not	Track Resource problem	PM

Full size | Export Data | Filter: inactive | Prev | Next

General Budget Trend

Full size | Export Data

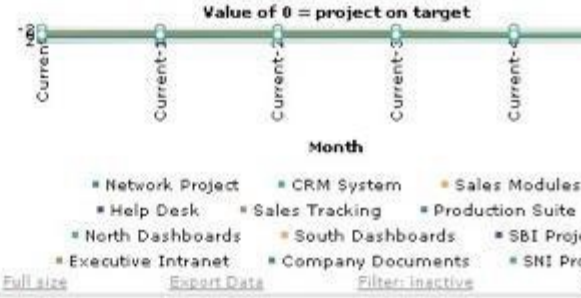
General Project Trend

Full size | Export Data | Settings

High Risk (number)

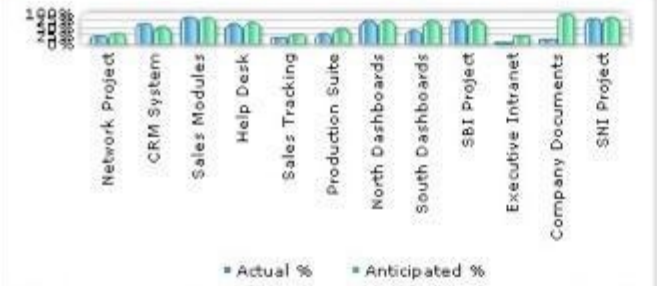
Full size | Export Data | Settings

Last 6 months trend by Project



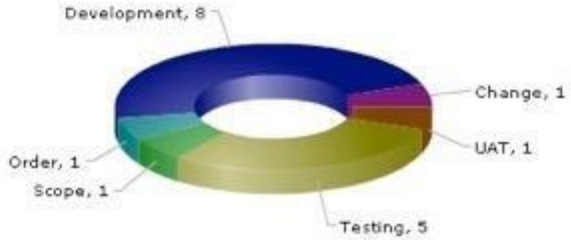
Full size | Export Data | Filter: inactive

Percent Complete v Due



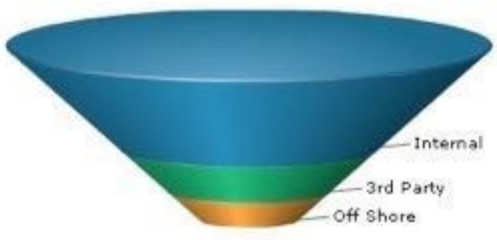
Full size | Export Data | Filter: inactive | Settings

Project by Current Lifecycle Stage



Full size | Export Data | Settings

Project by Resource



Full size | Export Data

executive dashboard

this data is as of november 15, 2005

Help

key figures

actual | target | bad | satisfactory | good

	actuals nov 04 - oct 05	current month	% of previous year	year to date	year to date % target
$ Revenues in mio		9.38	67.1	162.68	96.2
$ Expenses in mio		6.61	71.2	114.07	96.4
$ Profits in mio		2.76	58.9	61.11	120.4
Market Share in %		47.0	111.9	46.0	100.0
Flights		231	54.4	4,602	96.4
Passengers in K		32.4	61.1	595.2	95.2
Miles in K		163	51.0	3,513	103.9
Passenger Miles in mio		14.6	57.1	312.1	92.3
Cancelled Flights		7	58.3	104	80.0
Late Arrivals		48	58.5	714	178.9
Number of Minutes Late		1,342	59.3	15,363	187.8
$ Fuel Costs in mio		0.69	72.2	12.76	125.8
Average Customer Satisfaction Scores (out of 5)		4.5	99.6	4.5	94.0
Flight Utilization (Passengers / Capacity) in %		94.0	109.3	94.0	101.1
Revenue / Passenger Mile		0.6	117.4	0.6	128.8
Profit / Mile		17.0	115.4	17.0	113.3
Revenue / Mile		57.6	131.4	57.6	115.3

top 10 routes (last 30 days)

#	from	to	passengers in %	profit in %
1	Los Angeles	Oakland	12.6	10.5
2	Los Angeles	Vegas	9.7	10.2
3	Oakland	Dallas	8.2	8.7
4	Dallas	Houston	6.3	7.5
5	Oakland	Seattle	6.3	6.9
6	Houston	Orlando	3.9	4.2
7	Chicago	Dallas	2.6	3.2
8	Chicago	Orlando	2.0	2.1
9	Los Angeles	Orlando	2.1	1.8
10	Oakland	Orlando	1.9	1.7

worse 10 routes (last 6 months)

#	from	to	cancelled in %	delayed in %
1	Detroit	Orlando	5.1	31.4
2	Chicago	Dallas	4.6	26.3
3	Minneapolis	Denver	4.2	29.7
4	Houston	Orlando	4.1	21.7
5	Chicago	Orlando	3.9	25.6
6	Memphis	Detroit	3.2	15.8
7	Salt Lake City	Boston	2.8	19.7
8	Oakland	Orlando	1.9	14.9
9	Dallas	Houston	1.1	16.7
10	Oakland	Seattle	0.9	14.3

cancel./delays by reason (last 30 days)

#	reason	cancelled	delayed
1	Weather	6	76
2	Missing or late flight crew	2	17
3	Mechanical failure	1	15
4	Missing or late ground crew	1	4
5	Inefficient gate handling	0	2
6	Other	2	3

@mortman
@alexhutton

Another Master Chef Technique: Use the "Scorecard Sniff Test"

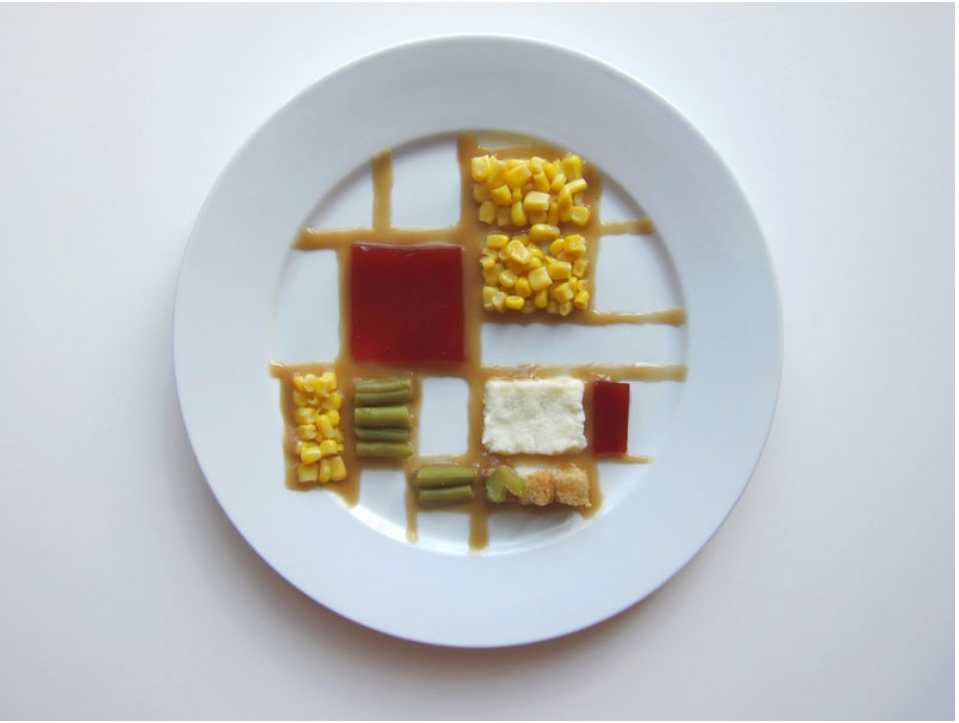
- Find a non-security audience
- Show them the scorecard for 10 seconds (and 10 seconds only)
- Hide the scorecard
- Ask them "What needs Action or Discussion?"
- Listen intently
- Revise, Rinse, Repeat.

@mortman
@alexhutton

Dave & Alex's Metric Cooking Tips

- **Every Pixel Has A Purpose**
- **Cute is Evil, So are Bullets**
- **Appreciate the Purpose of White Space**
- **Colors aren't always as necessary as you think they are**
  - But when they are, use them wisely (treat them like ammo)
- **Consistency is Key**
- **Rationalize Copiously**
  - When you think you're done, walk away, come back, start removing things
- **When in Doubt, Do What Stephen Few Would Do**
- **If It Needs Explanation, it's Not Right**

@mortman
@alexhutton




EVEN WITH GOOD PLATING, GQM, ETC,
SOMETIMES WHAT YOU PRODUCE WILL STILL BE UNAPPETIZING

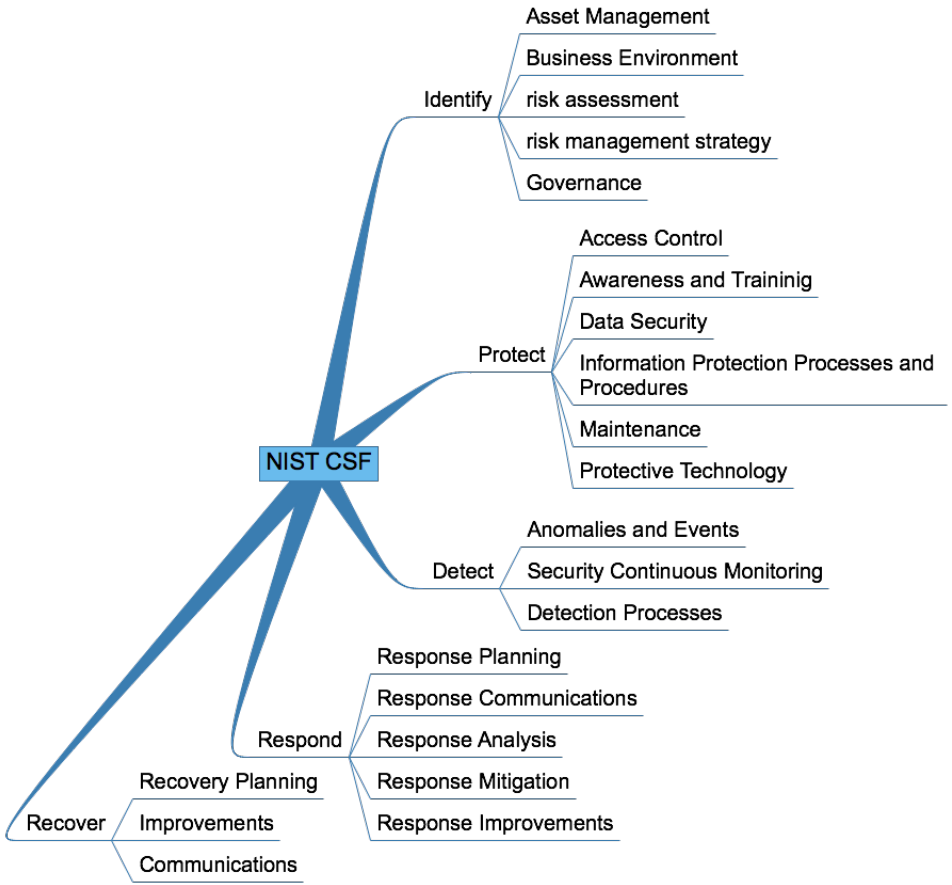
RSA Conference2015

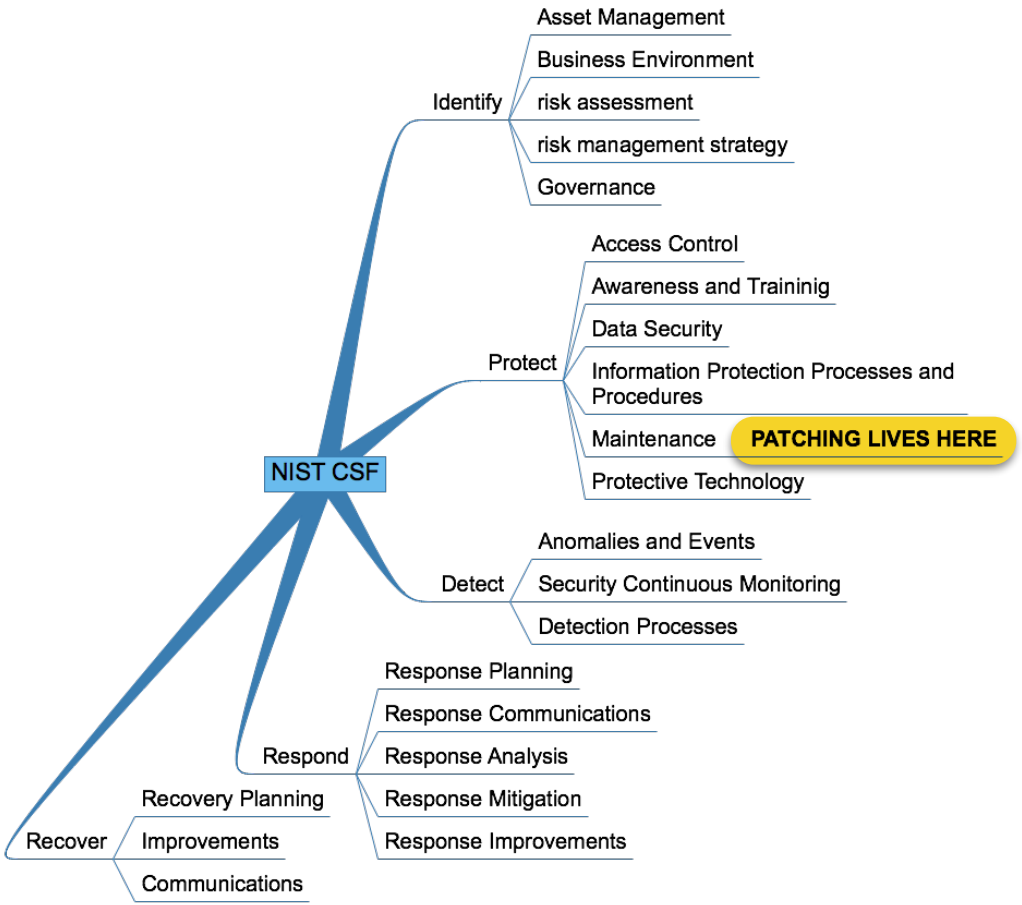
San Francisco | April 20-24 | Moscone Center

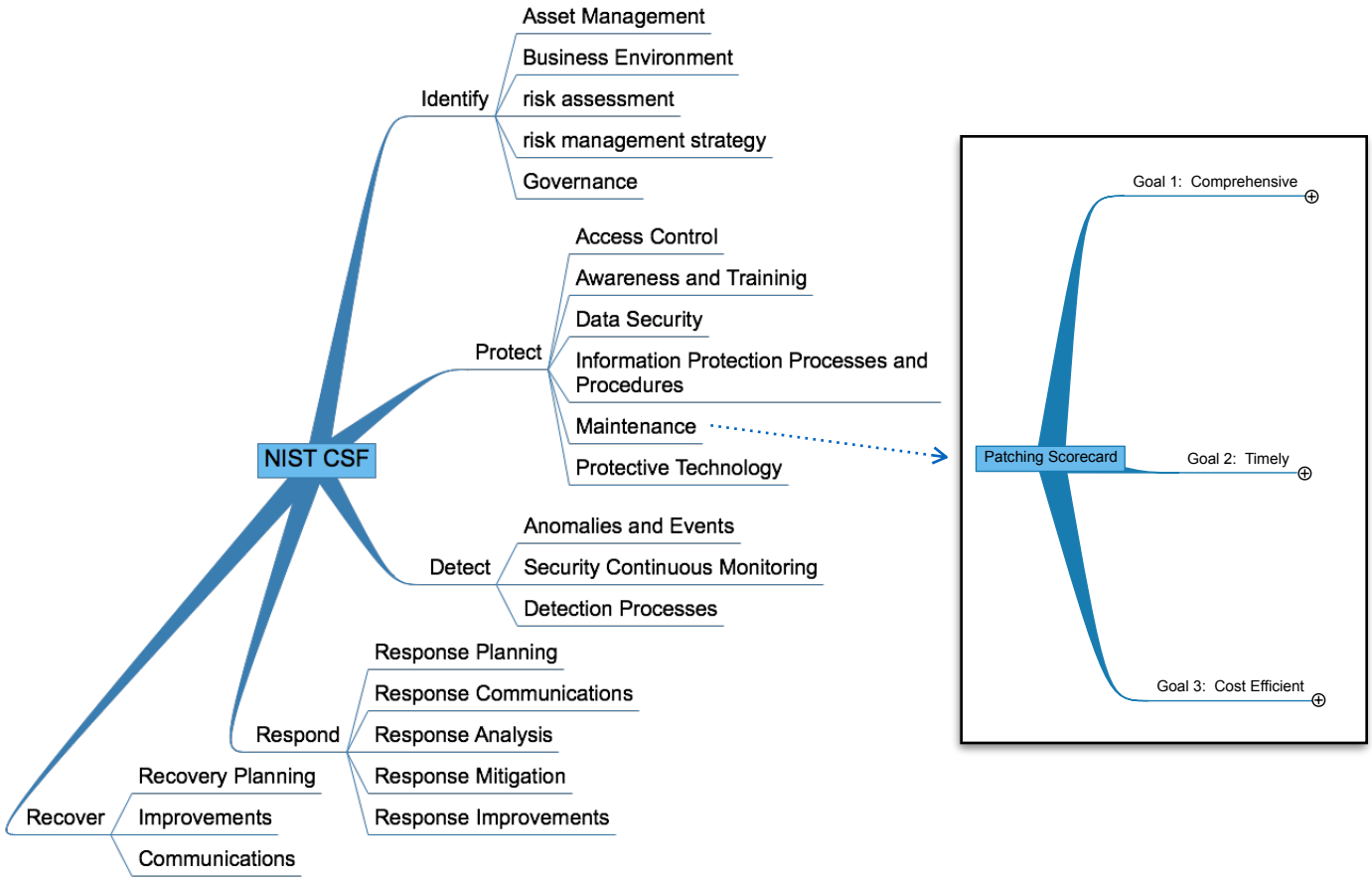
EXAMPLE DISH:
GQM METRICS FRAMEWORK FOR NIST CSF

@mortman
@alexhutton

#RSAC

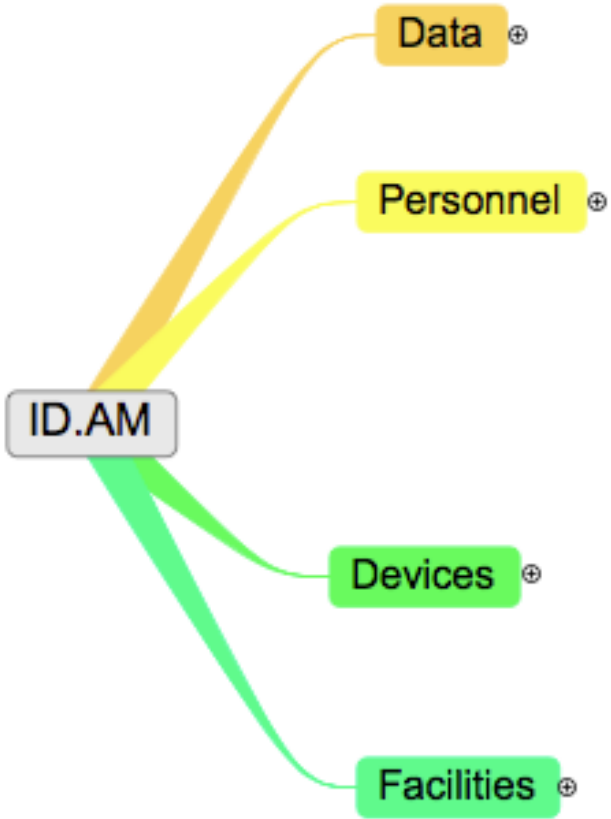

NIST CSF
Identify
Asset Management
Business Environment
risk assessment
risk management strategy
Governance
Protect
Access Control
Awareness and Traininig
Data Security
Information Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Response Communications
Response Analysis
Response Mitigation
Response Improvements
Recover
Recovery Planning
Improvements
Communications


NIST CSF
Identify
Asset Management
Business Environment
risk assessment
risk management strategy
Governance
Protect
Access Control
Awareness and Traininig
Data Security
Information Protection Processes and Procedures
Maintenance
PATCHING LIVES HERE
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Response Communications
Response Analysis
Response Mitigation
Response Improvements
Recover
Recovery Planning
Improvements
Communications

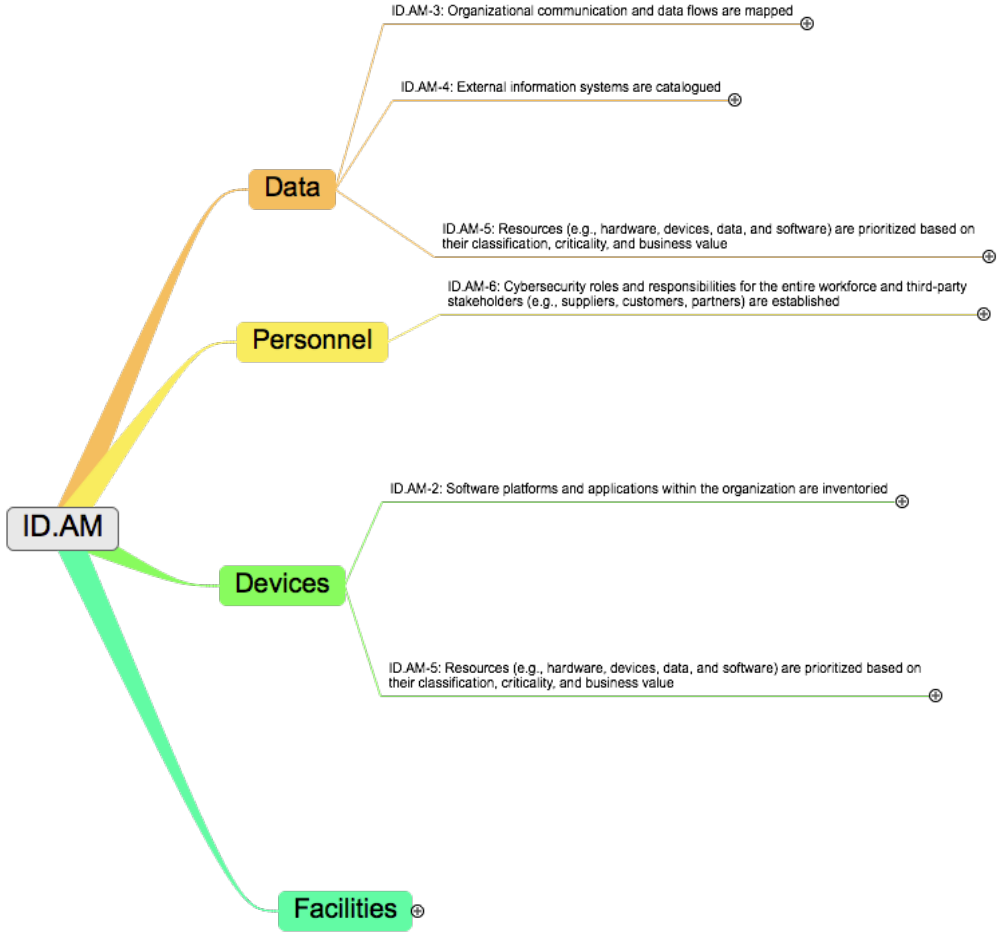

NIST CSF
Identify
Asset Management
Business Environment
risk assessment
risk management strategy
Governance
Protect
Access Control
Awareness and Traininig
Data Security
Information Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Response Communications
Response Analysis
Response Mitigation
Response Improvements
Recover
Recovery Planning
Improvements
Communications
Patching Scorecard
Goal 1: Comprehensive
Goal 2: Timely
Goal 3: Cost Efficient

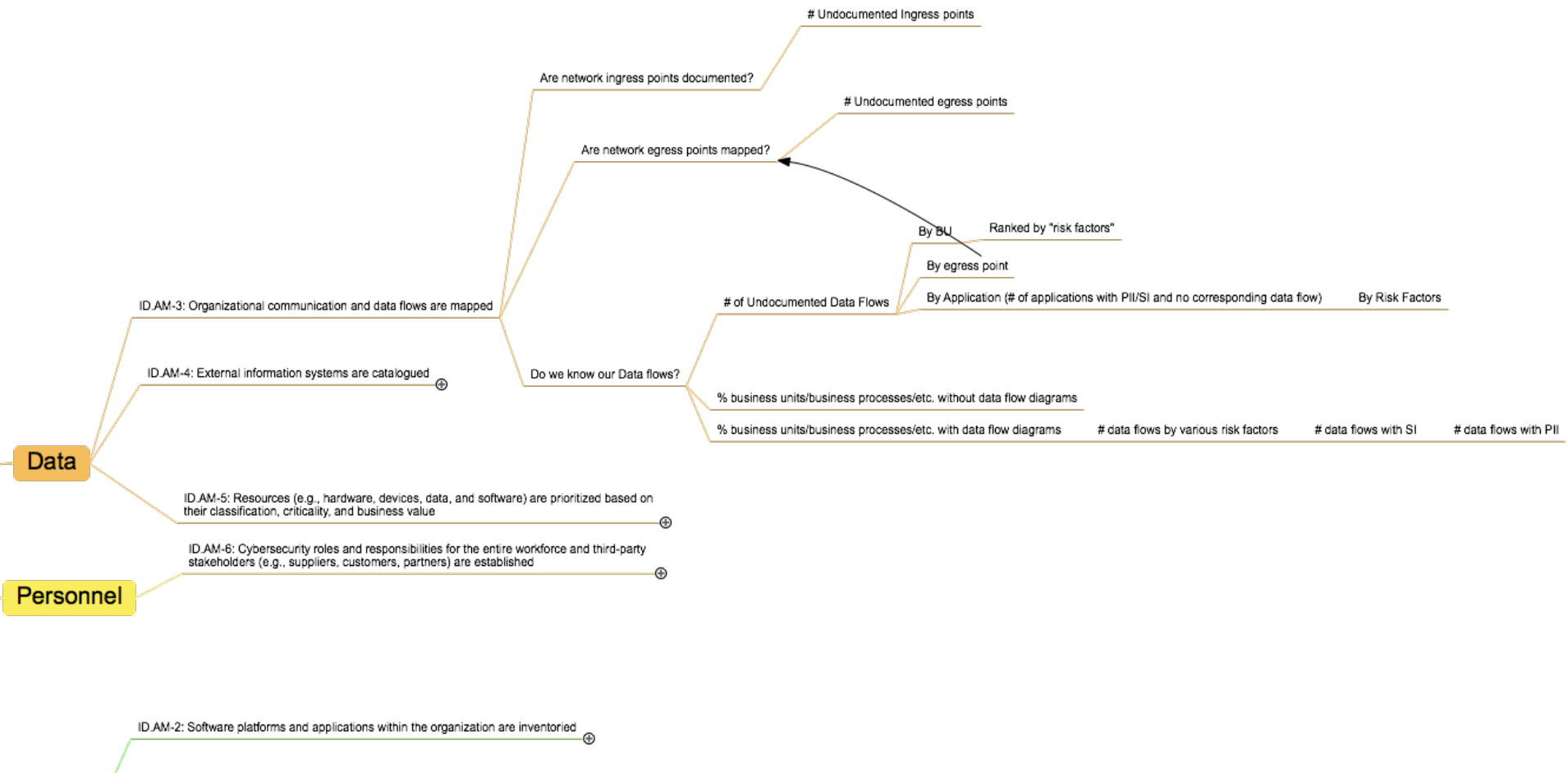
@mortman
@alexhutton

Asset Management (ID.AM): The **data, personnel, devices, systems,** and **facilities** that enable the organization to achieve business purposes are **identified** and **managed** consistent with their **relative importance** to business objectives and the organization's risk strategy.



Asset Management (ID.AM): The **data, personnel, devices, systems,** and **facilities** that enable the organization to achieve business purposes are **identified** and **managed** consistent with their **relative importance** to business objectives and the organization's risk strategy.




Data
ID.AM-3: Organizational communication and data flows are mapped
Are network ingress points documented?
Undocumented Ingress points
Are network egress points mapped?
Undocumented egress points
Do we know our Data flows?
# of Undocumented Data Flows
By BU
Ranked by "risk factors"
By egress point
By Application (# of applications with PII/SI and no corresponding data flow)
By Risk Factors
% business units/business processes/etc. without data flow diagrams
% business units/business processes/etc. with data flow diagrams
# data flows by various risk factors
# data flows with SI
# data flows with PII
ID.AM-4: External information systems are catalogued
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Personnel
ID.AM-2: Software platforms and applications within the organization are inventoried

@mortman
@alexhutton

INTERESTING LESSONS/OBSERVATIONS ABOUT NIST CSF THANKS TO GQM

- Some category elements don't even have sub-categories
- Some sub-categories don't really support the category description
- There's no guarantee the categories fully support the function
- NIST CSF's value as a framework to be pragmatically used by a CISO is suspect
  - based on metrics that support sub-categories

@mortman
@alexhutton

INTERESTING LESSONS/OBSERVATIONS ABOUT NIST CSF THANKS TO GQM

- Some category elements don't even have sub-categories

In other words, GQM can be a useful tool to test the real world value of security dogma

  - based on metrics that support sub-categories

GOVERNANCE, WITHOUT MEASUREMENT, IS **DOGMA.**

GOVERNANCE, **WITH** MEASUREMENT, IS RISK MANAGEMENT**.**

@mortman
@alexhutton

WHERE TO FIND THIS EFFORT IF YOU WANT TO USE IT-

- NISTCSF.SOCIETYINFORISK.ORG

RSAConference2015

San Francisco | April 20-24 | Moscone Center

THANK YOU.

@mortman
@alexhutton

#RSAC