

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

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



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)



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

LEVEL SETTING



@mortman
@alexhutton



#RSAC

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







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

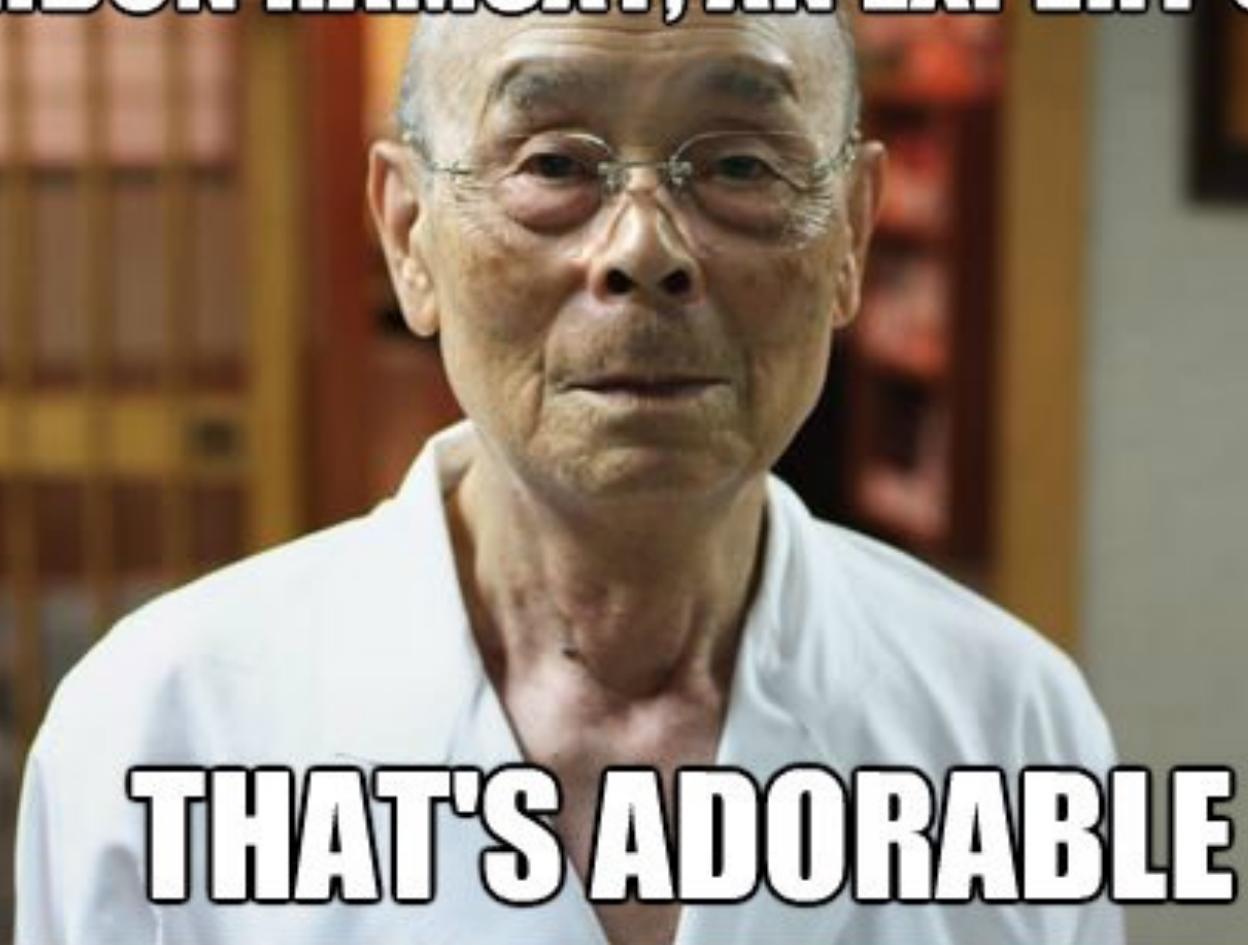
Three Michelin stars

One 85 year old perfectionist

JIRO DREAMS OF SUSHI

Fall in love with your work

GORDON RAMSAY, AN EXPERT CHEF?



THAT'S ADORABLE

- ◆ It's important for us understand...





- ◆ There is no “Secure”,
only Securing...

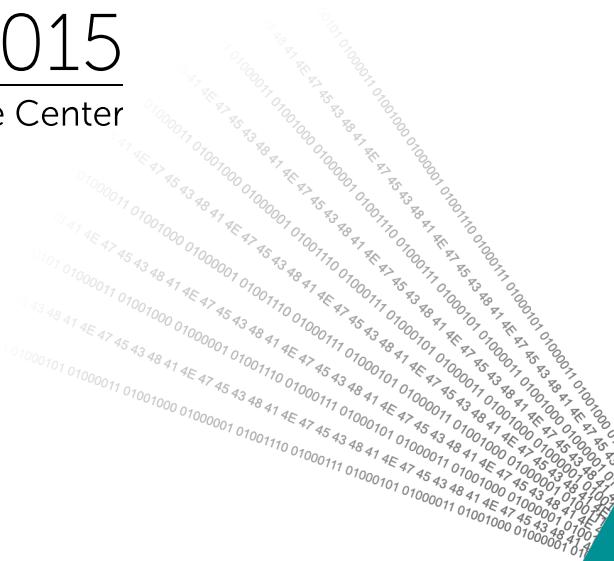


- ◆ ...and so there is no Mathematical “Proof” for “Secure”... and so
- ◆ ...metrics cannot provide “secure” any more than your controls can.



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center



INTRODUCTION

@mortman
@alexhutton

The current state of metrics in the industry...

NEW CUYAMA

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

Just Kidding



Just Kidding - It's Worse



WHY?

THIS BORK IS SO UNDERBORKED



THAT IT'S BORKING THE BORK

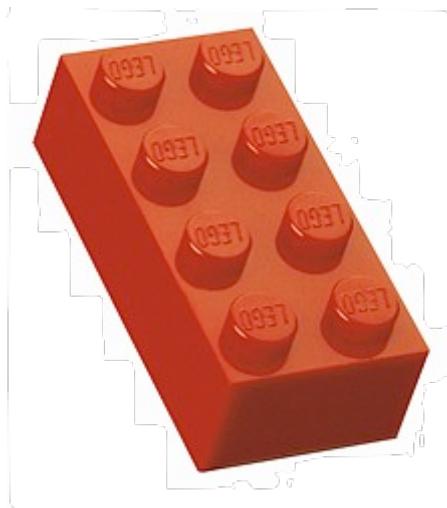
THIS BORK IS SO UNDERBORKED



SECURITY!

THAT IT'S BORKING THE BORK

Why? Aggregate Meaning, Context is missing.



Why? Aggregate Meaning, Context is missing.



Why? Aggregate Meaning, Context is missing.



Why? Aggregate Meaning, Context is missing.



Why? Aggregate Meaning, Context is missing.



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

PART ONE: KNOWING THE RIGHT INGREDIENTS MAKING A USEFUL METRIC



@mortman
@alexhutton



#RSAC

What is a metric?

Vurt da Furk!



What is a metric?

- ◆ Control Effectiveness is “medium”
- ◆ - arguably?



What is a metric?

- We have 53 “medium” control effectiveness ratings
- - now we’re getting somewhere.



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.



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!**



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***.



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...



What is a metric? - Definition

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



What is a metric? - Purpose



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).



What is a metric?

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



What is a metric?

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



WHAT ARE THE **RIGHT** INGREDIENTS?

Things to Make Metrics About

- ◆ Security Stuff
- ◆ Business Stuff

THE RIGHT INGREDIENTS - SECURITY STUFF

- ◆ Only four “types” of information



THE RIGHT INGREDIENTS - BUSINESS STUFF

What matters most to your organization?



MONEY & TIME

(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® Conference 2015

San Francisco | April 20-24 | Moscone Center

PART TWO: KNOWING HOW TO COOK TECHNIQUES FOR METRIC CREATION



@mortman
@alexhutton

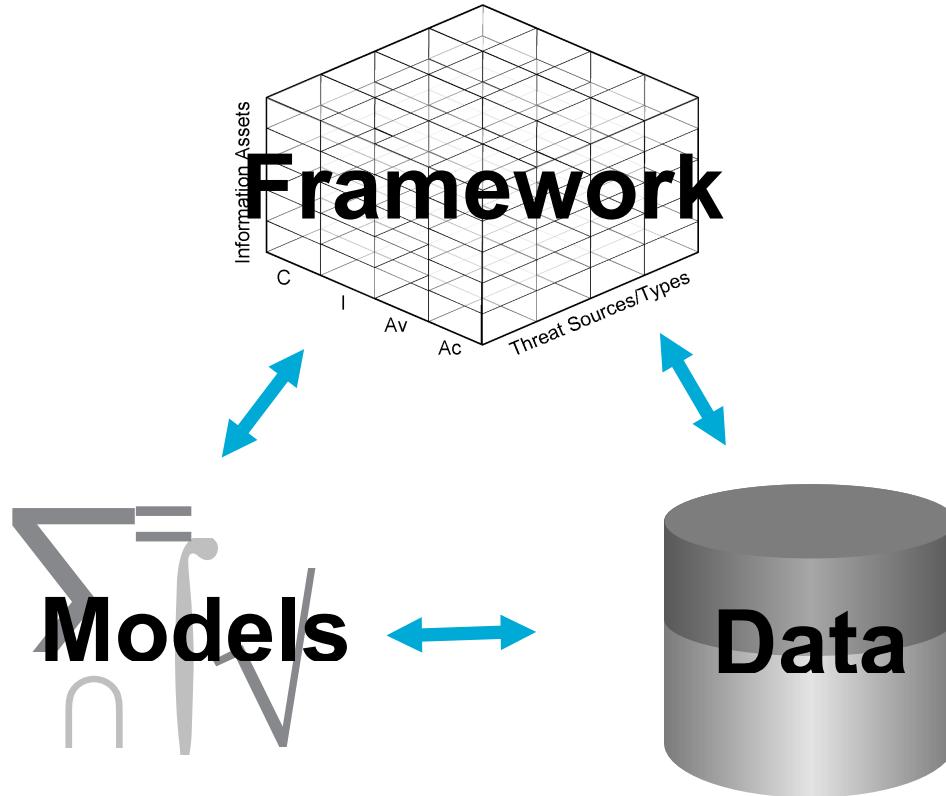


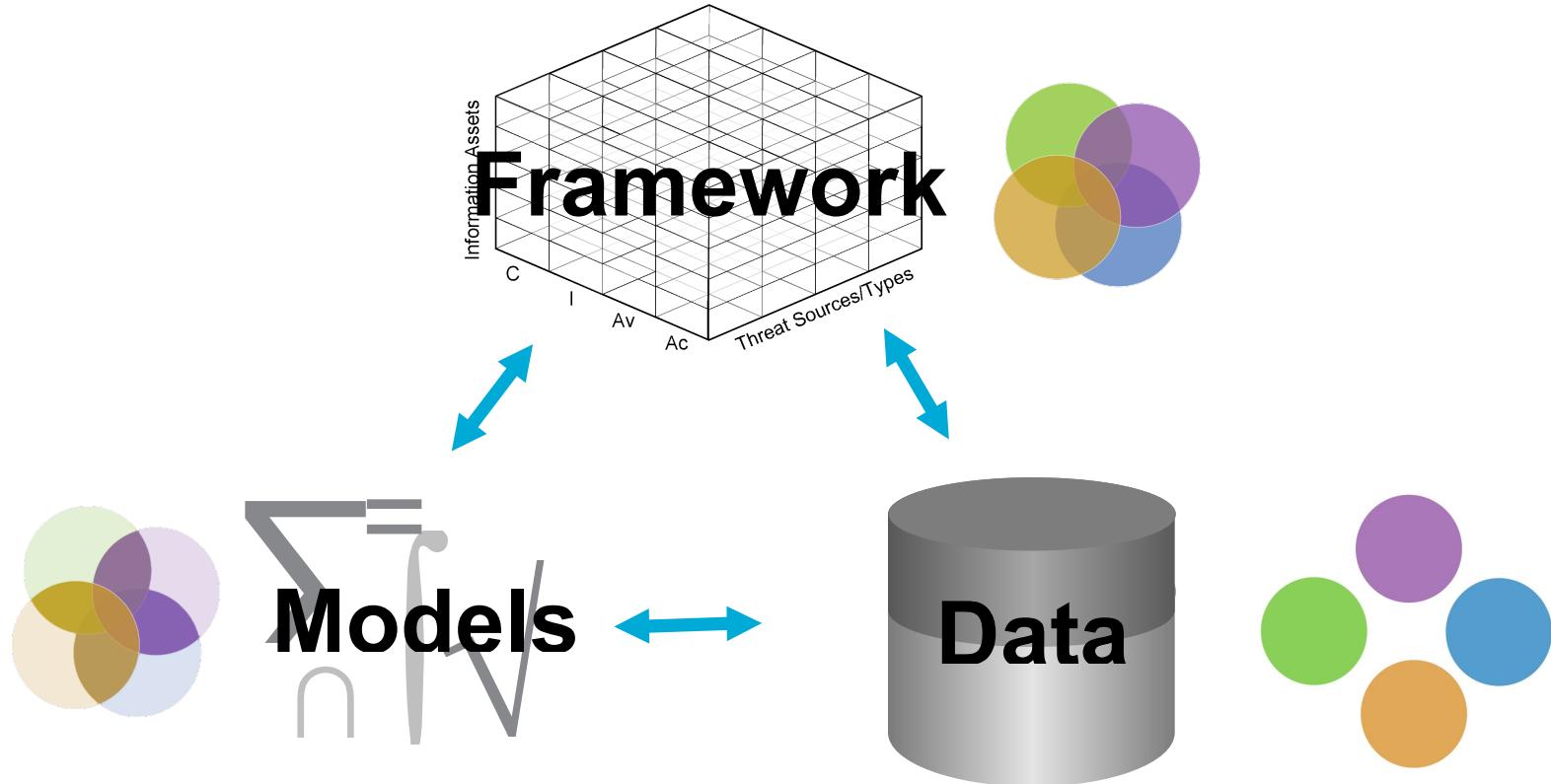
#RSAC

KNOWING HOW TO COOK BRINGING TOGETHER INGREDIENTS









RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

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



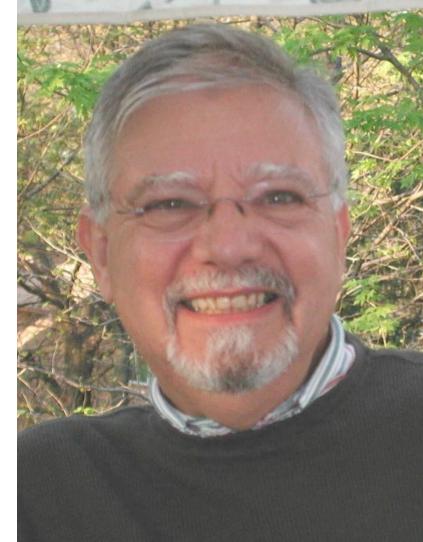
@mortman
@alexhutton



#RSAC

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

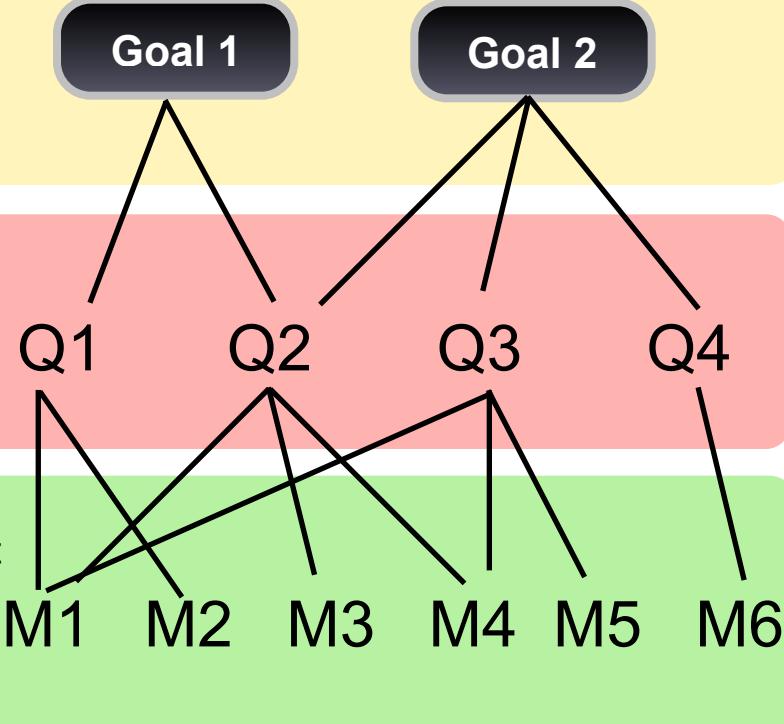


GQM For Fun & Profit

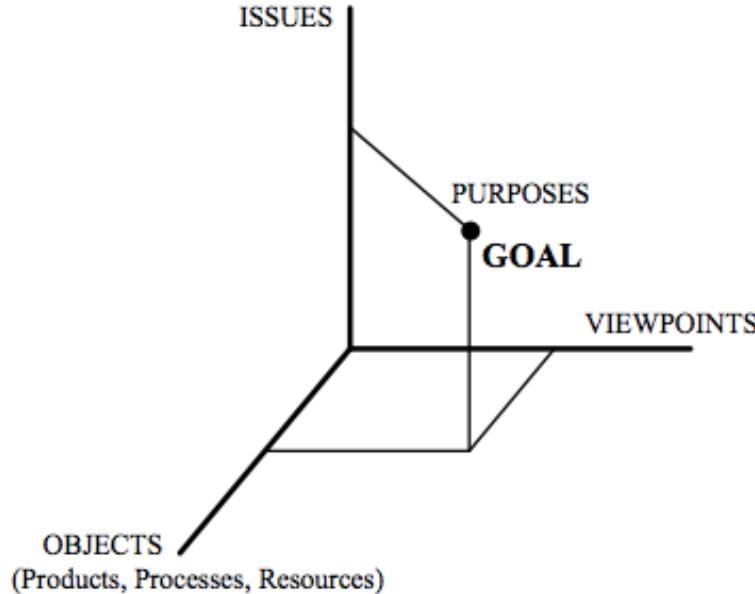
Goals establish what we want to accomplish.

Questions help us understand how to meet the goal. They address context.

Metrics identify the measurements that are needed to answer the questions.

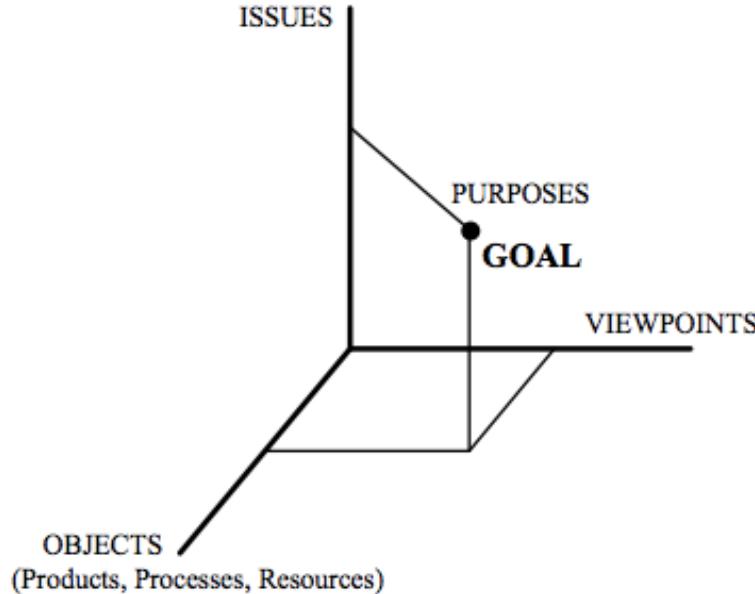


Regarding your Goals



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

Regarding your Goals



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

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

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

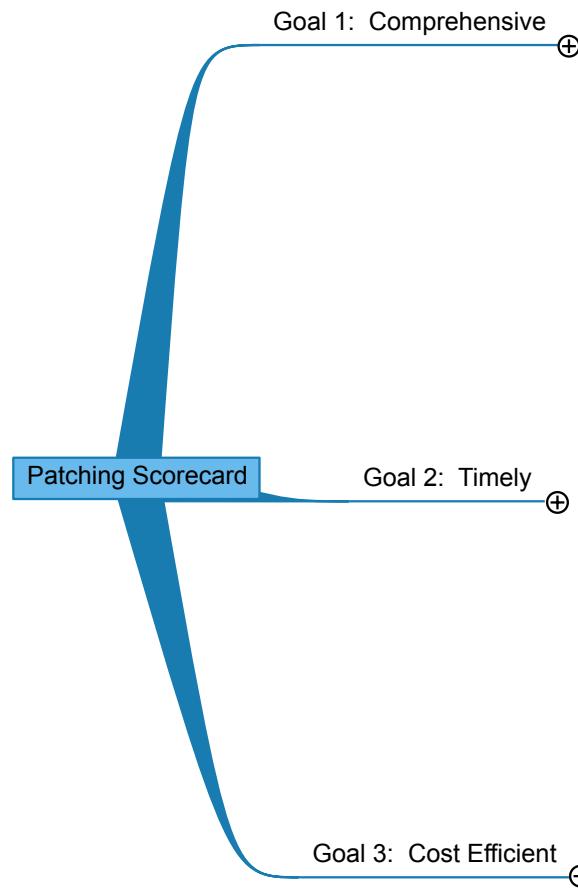
AN EXAMPLE - PATCH MANAGEMENT GQM SCORECARD

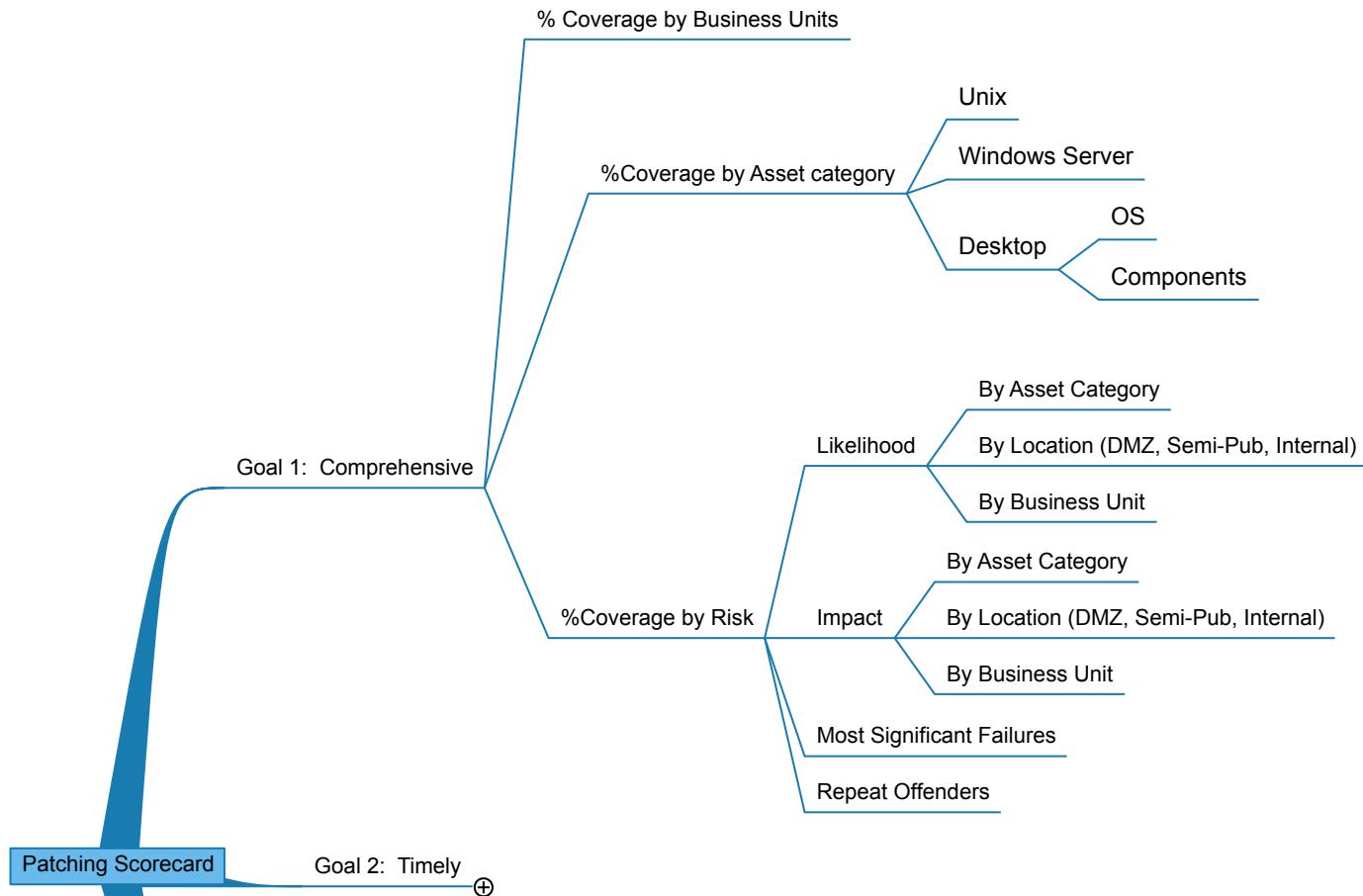


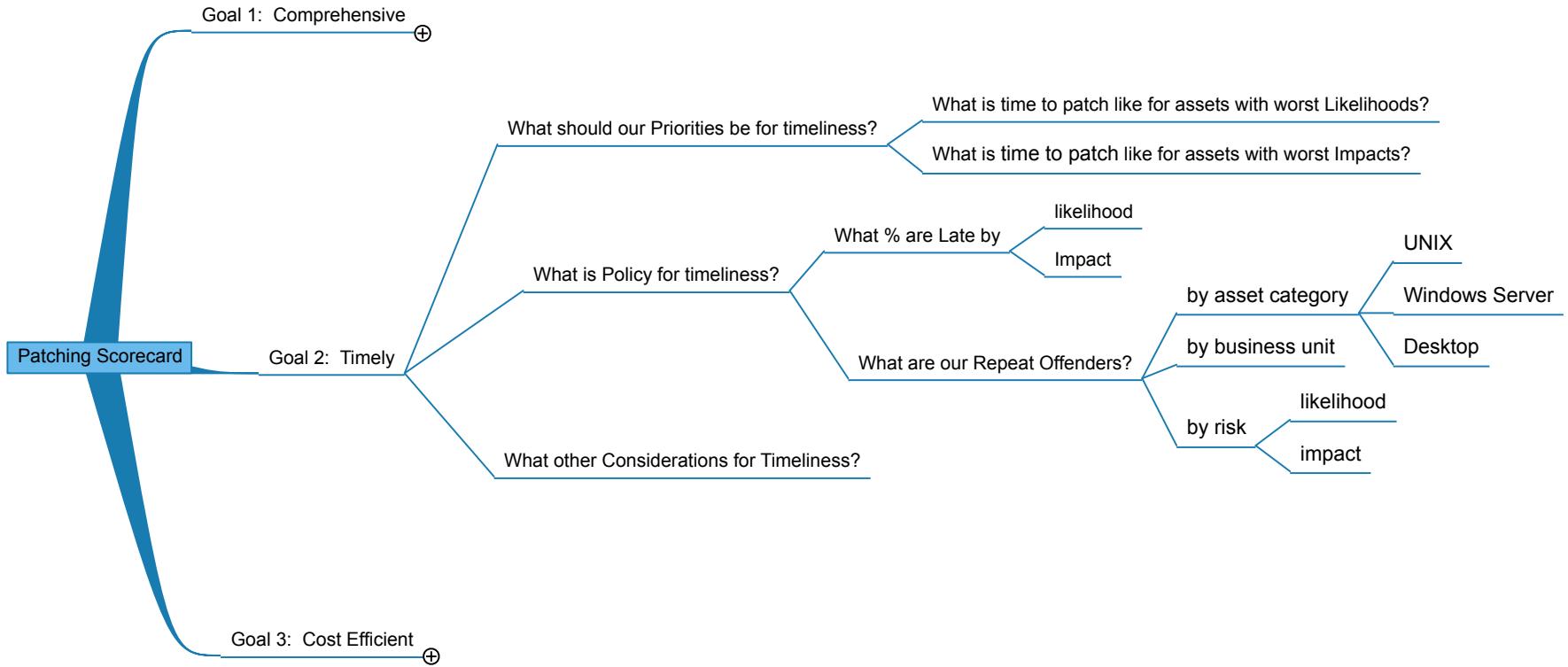
@mortman
@alexhutton



 #RSAC







Patching Scorecard

Goal 2: Timely

Goal 3: Cost Efficient

Cost

Risk Reduction

Hour per Asset spent Patching

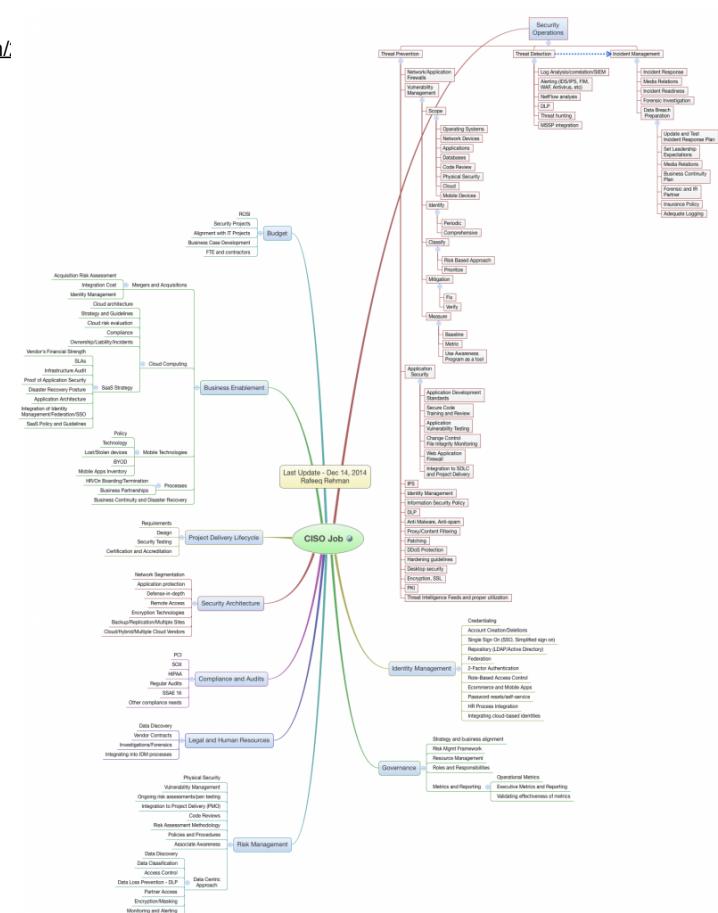
Hour per Asset, by ALE per Hour

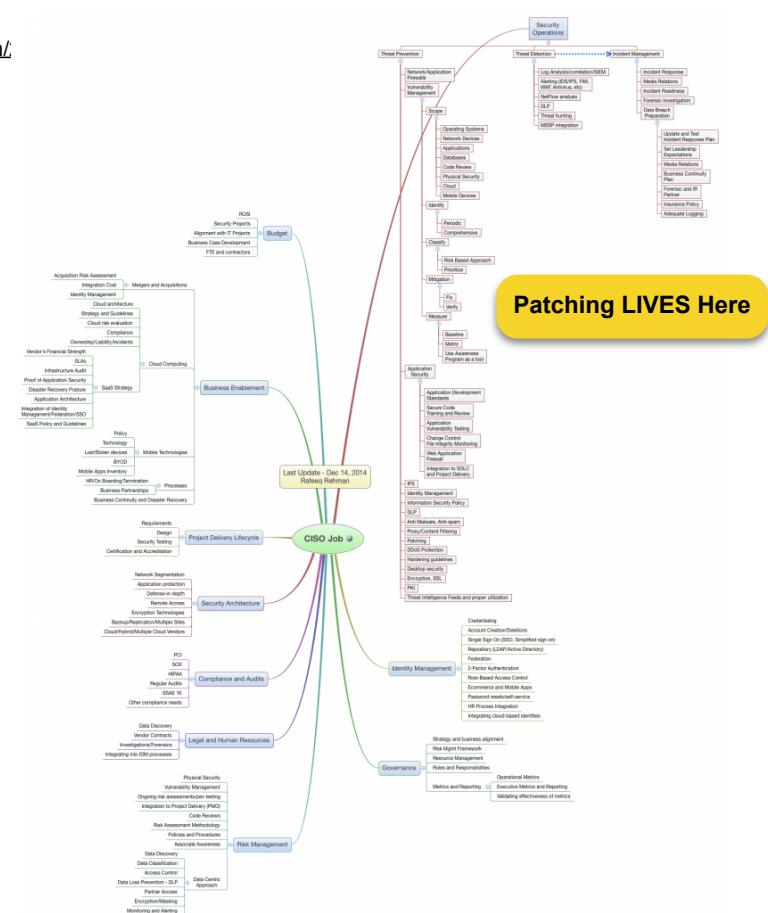
Hour per asset category

By Asset Category

By Location (DMZ, Semi-Pub, Internal)

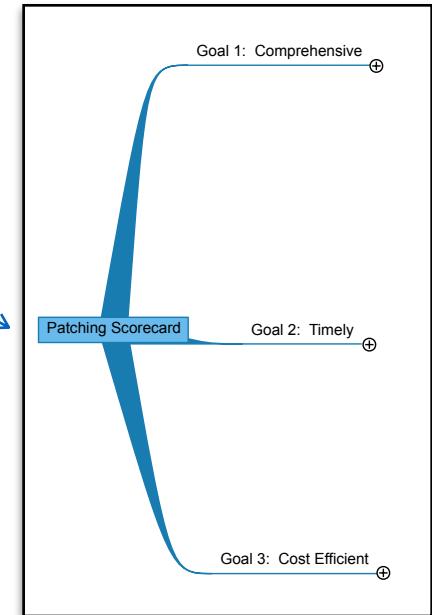
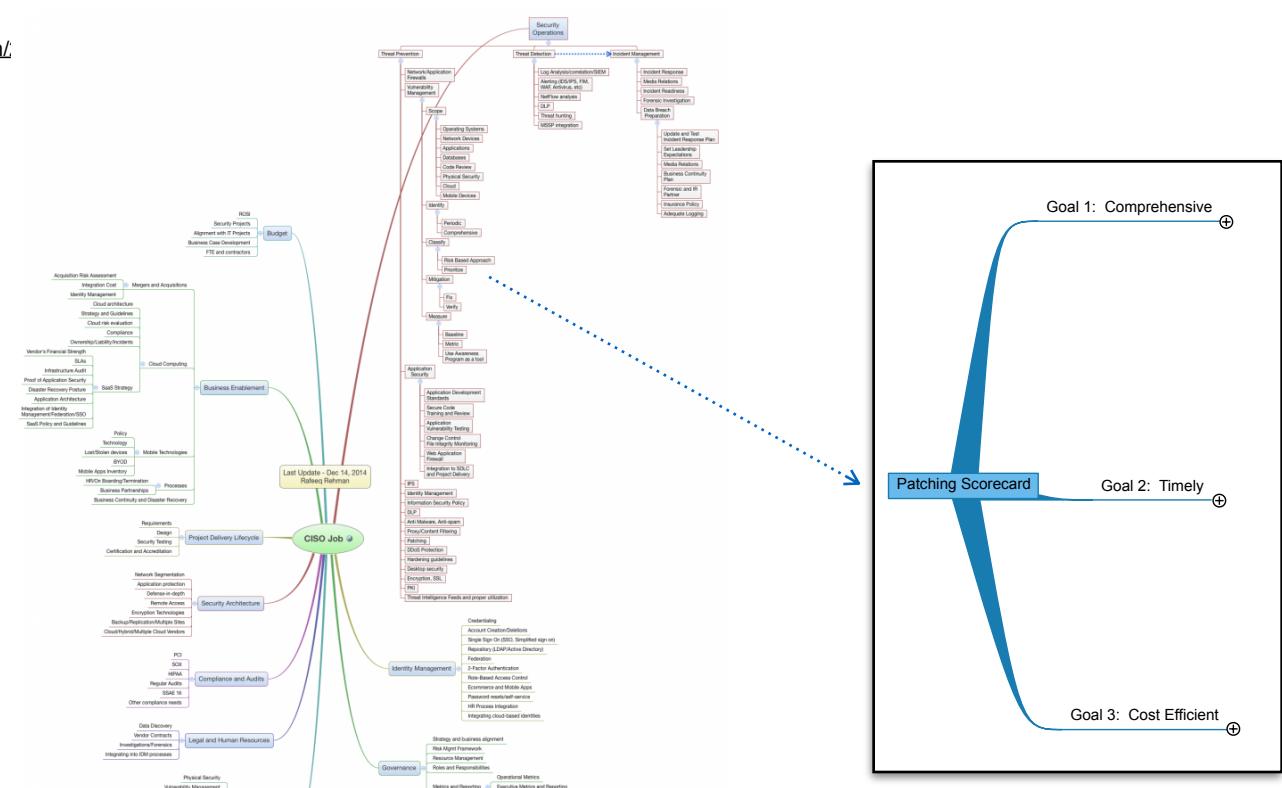
By Cost Per Hour





Patching LIVES Here



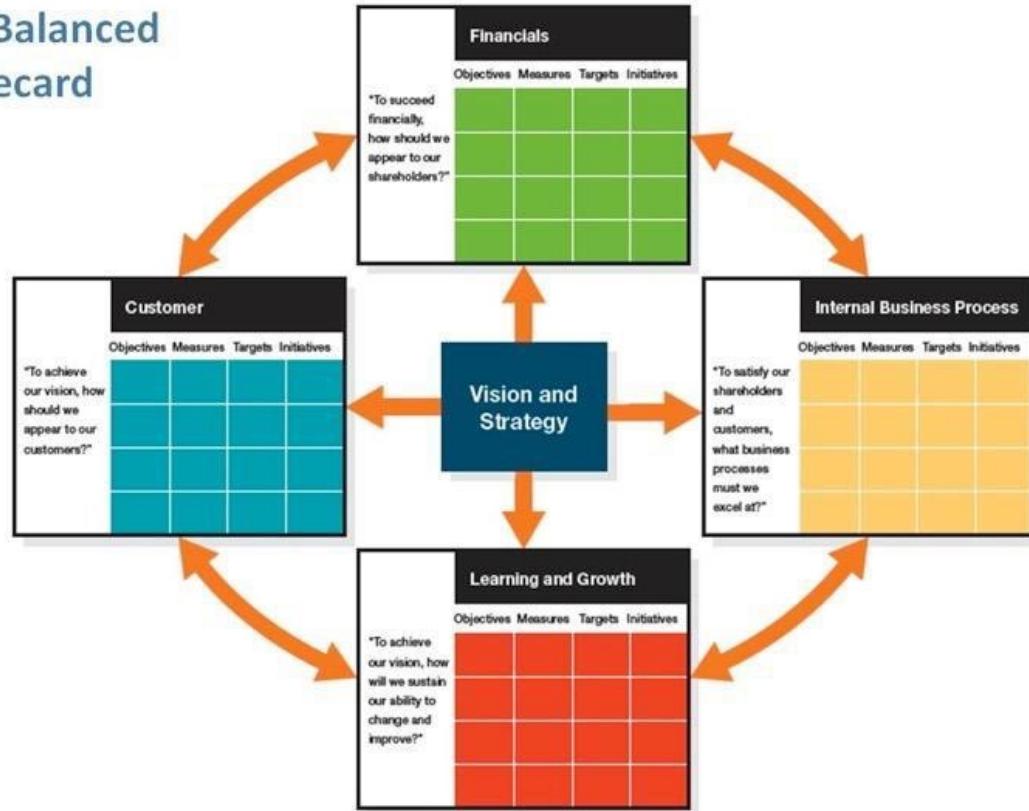


A Note On GQM

- 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

The Balanced Scorecard



Balanced Scorecard for Security Stuff

Impact



Balanced Scorecard for IT GRC

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

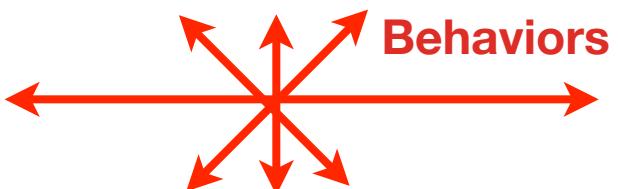
IT Strategic Planning &

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

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

PART THREE: KNOWING HOW TO PLATE OR, SCORECARDS!



@mortman
@alexhutton
 #RSAC

 josh russell
@josh_emerson

my school lunch today :

12:50 PM - 21 Nov 2014



65 RETWEETS 17 FAVORITES





 josh russell
@josh_emerson

my school lunch today :

12:50 PM - 21 Nov 2014

 Follow

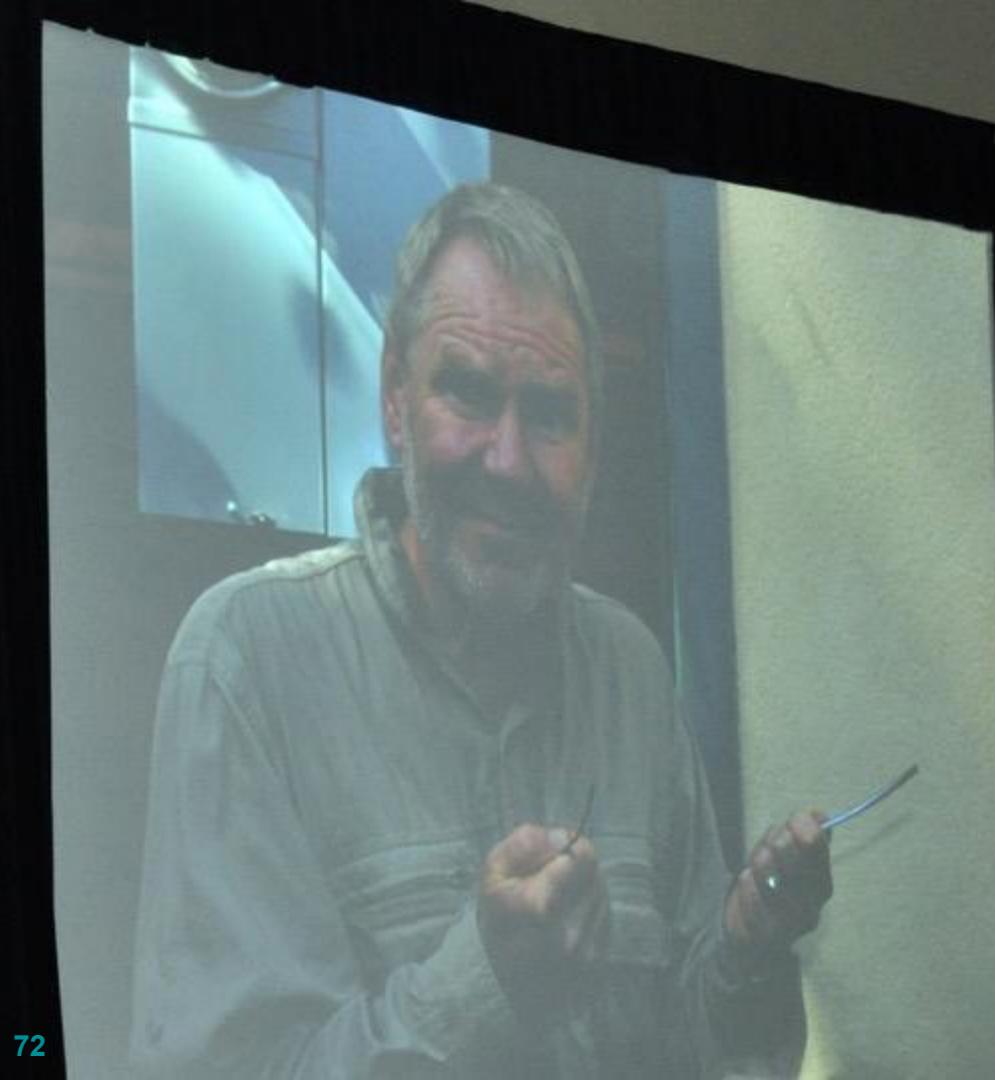
65 RETWEETS 17 FAVORITES



Stephen Few.

**Buy everything he
makes.**

Do everything he says.



Cost, Budget and Anticipated Cost

Network Project CRM System Sales Modules Help Desk Sales Tracking Production Suite North Dashboards South Dashboards SBI Project Executive Intranet Company Documents SNI Project

* Budget * Actual Spend * Anticipated Final Cost

Full size Export Data Filter: inactive Settings



-13%

Red = behind schedule
Amber = on target
Green = ahead of schedule

Full size Export Data Settings

Current Risks

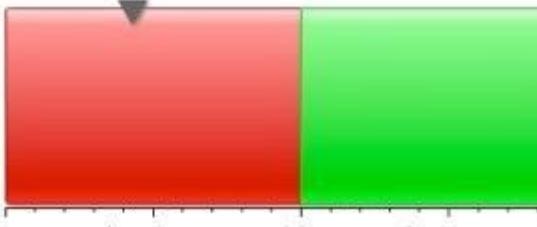
Showing 1 to 44 of 44

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

Full size Export Data Filter: inactive Prev | Next

General Budget Trend

\$-57,000



100,000.0 \$-50,000.0 \$0.0 \$50,000.0

Full size Export Data

General Project Trend

High Risk (number)

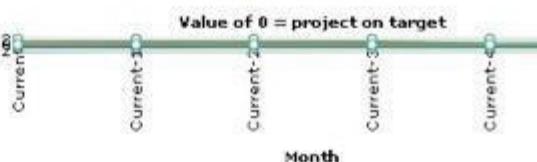


12 18 24
6
13 Low High

Full size Export Data Settings

Last 6 months trend by Project

Value of 0 = project on target



Month

Network Project CRM System Sales Modules Help Desk Sales Tracking Production Suite North Dashboards South Dashboards SBI Project Executive Intranet Company Documents SNI Project

Full size Export Data Filter: inactive

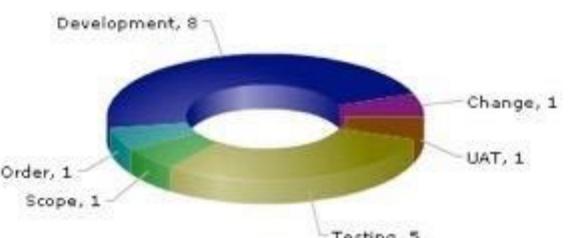
Percent Complete v Due

Network Project CRM System Sales Modules Help Desk Sales Tracking Production Suite North Dashboards South Dashboards SBI Project Executive Intranet Company Documents SNI Project

* Actual % * Anticipated %

Full size Export Data Filter: inactive Settings

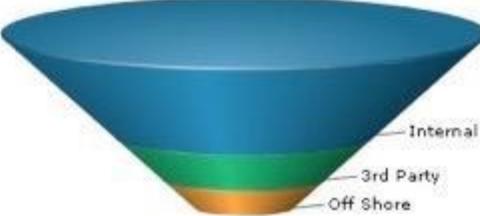
Project by Current Lifecycle Stage



Development, 8
Change, 1
UAT, 1
Testing, 5
Order, 1
Scope, 1

Full size Export Data Settings

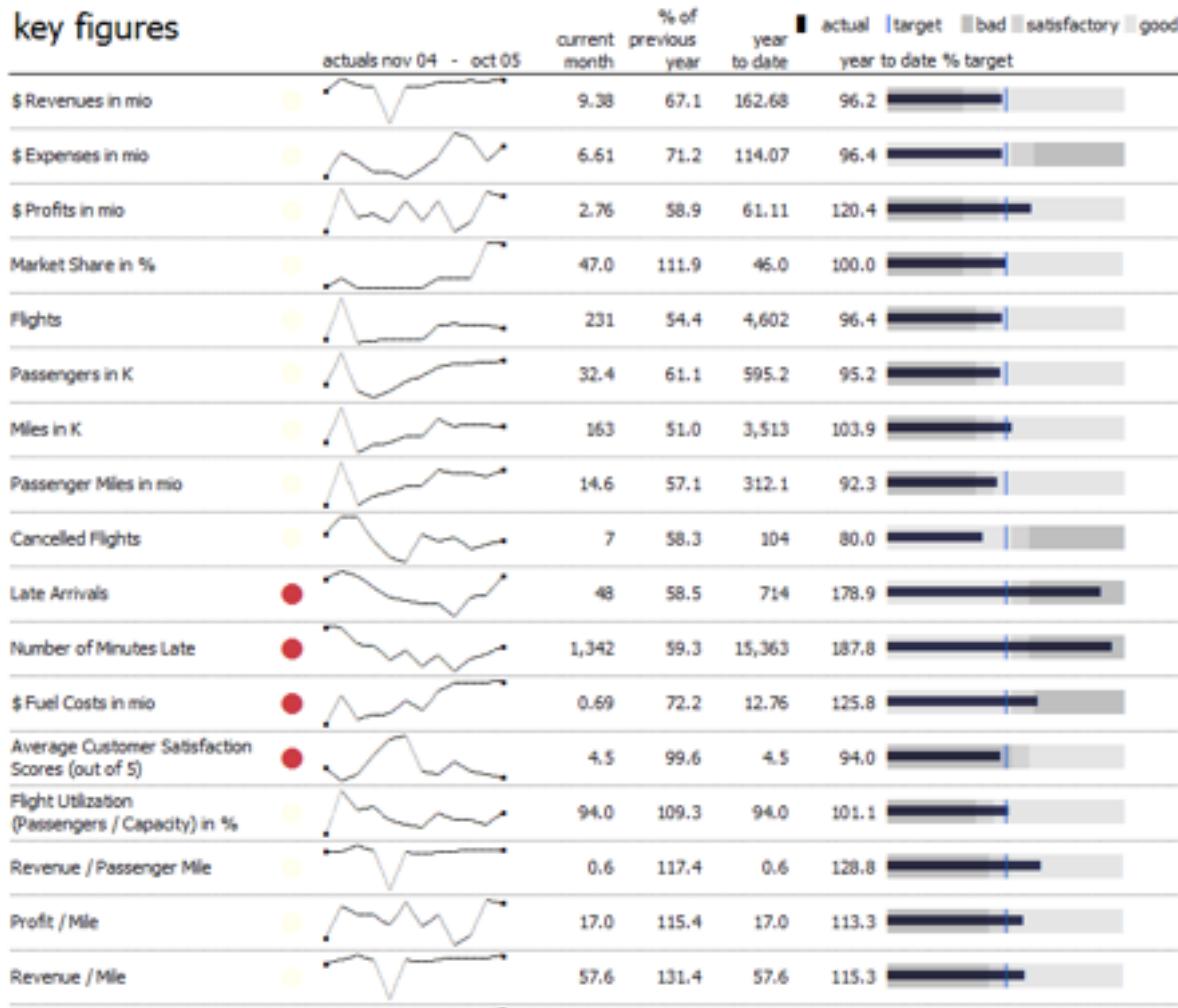
Project by Resource



Internal
3rd Party
Off Shore

Full size Export Data

key figures



top 10 routes (last 30 days)

#	from	to	passenger 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

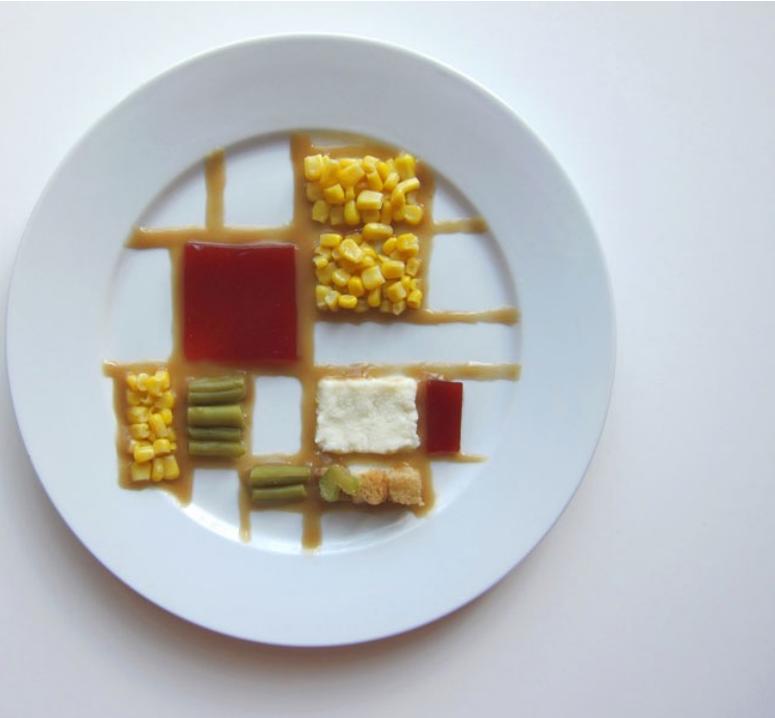
Another Master Chef Technique: Use the “Scorecard Sniff Test”

- ◆ 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.

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







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

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

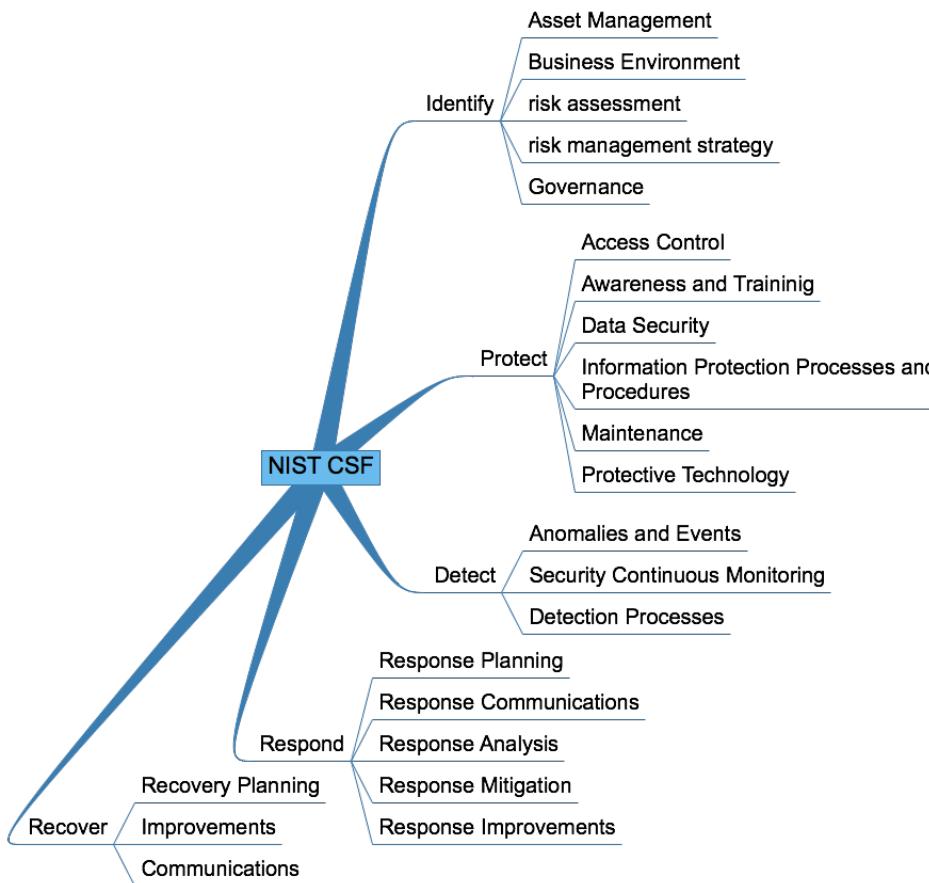
EXAMPLE DISH: GQM METRICS FRAMEWORK FOR NIST CSF

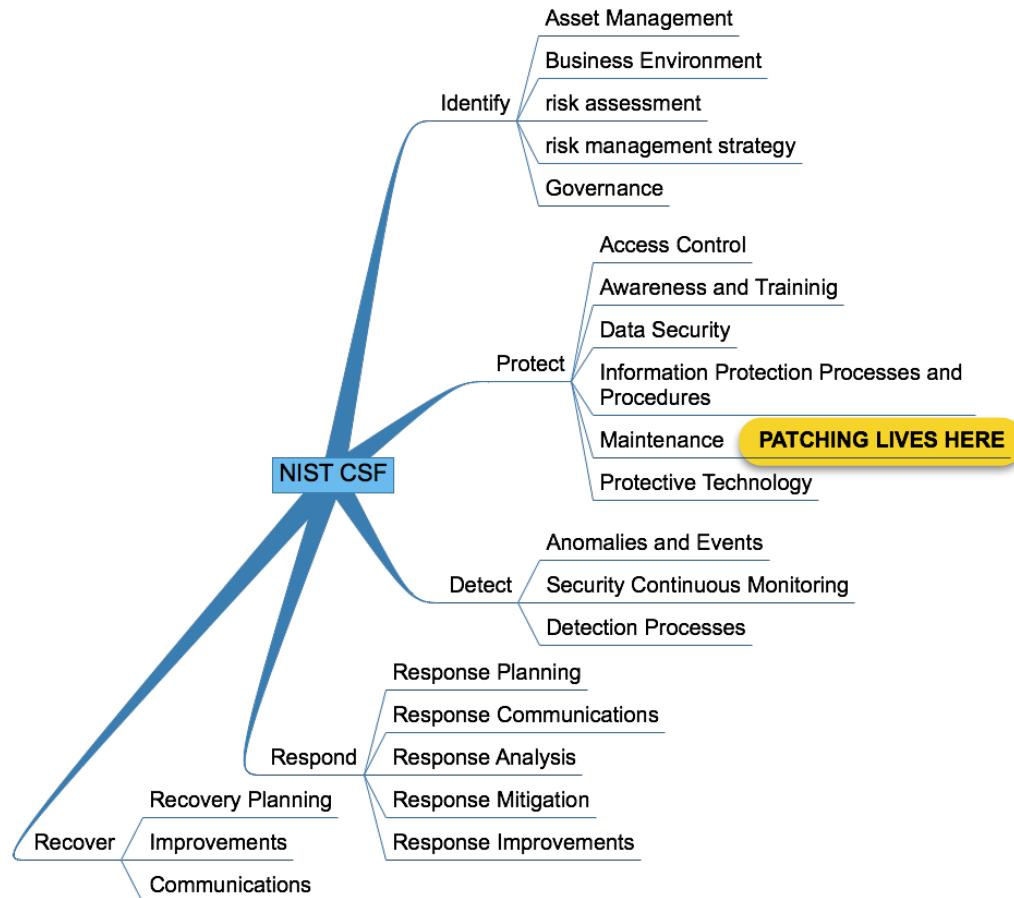


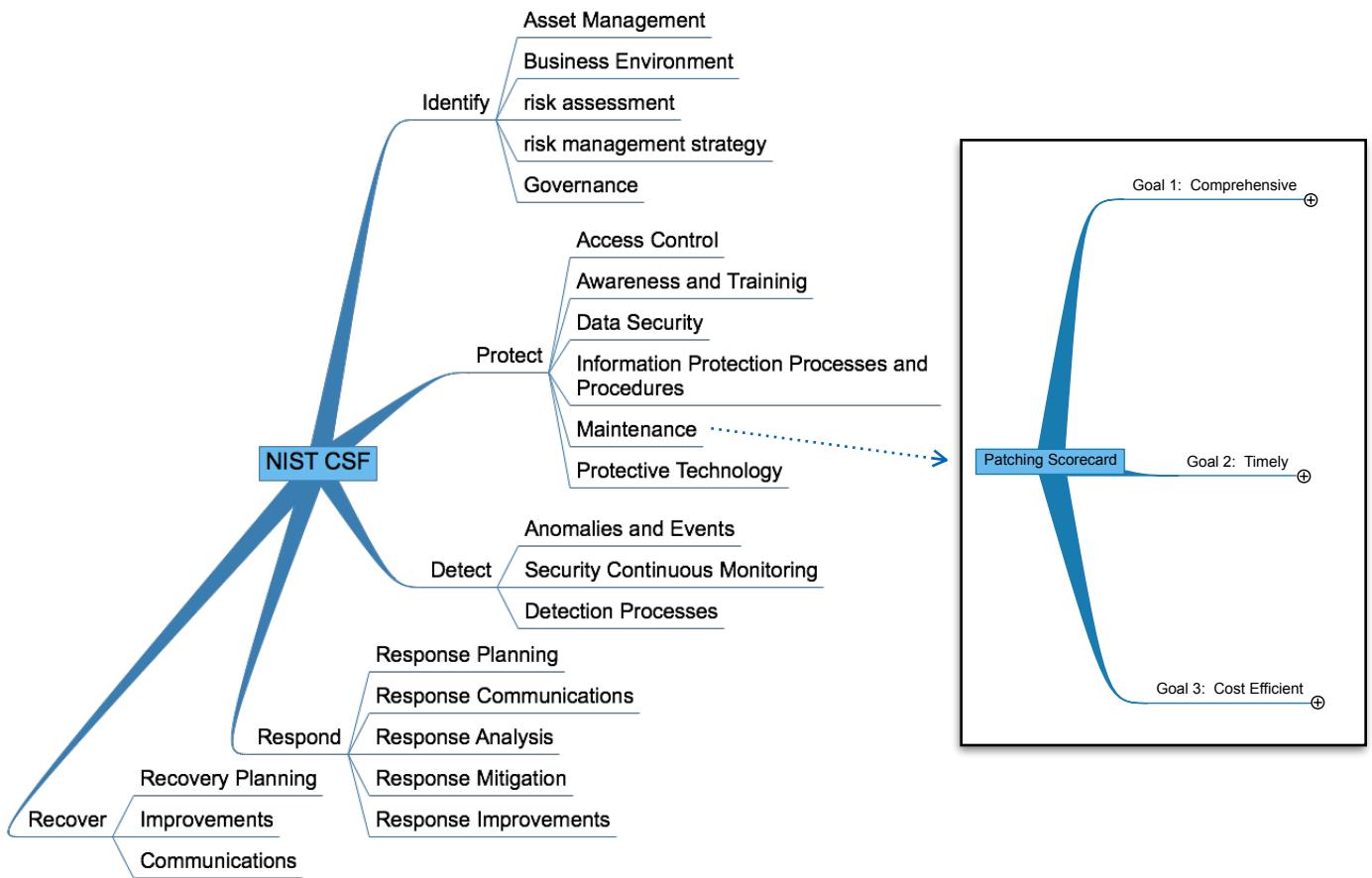
@mortman
@alexhutton

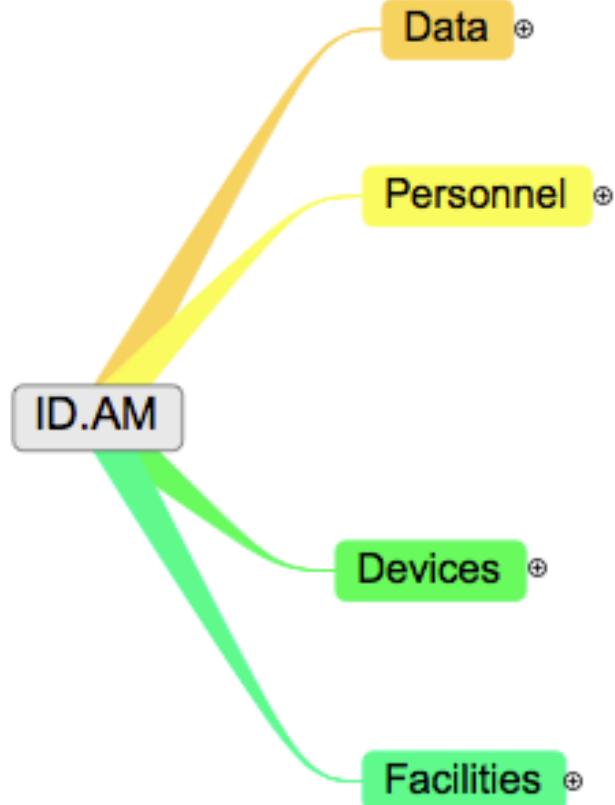


#RSAC



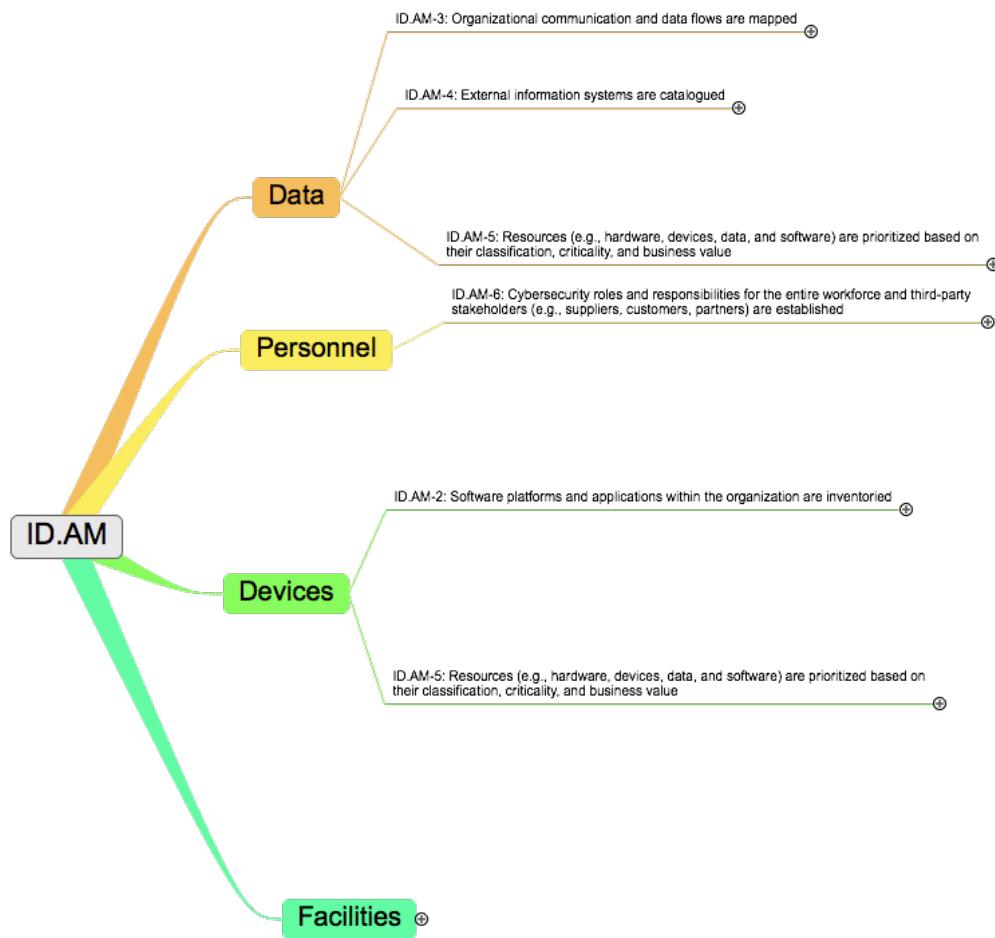


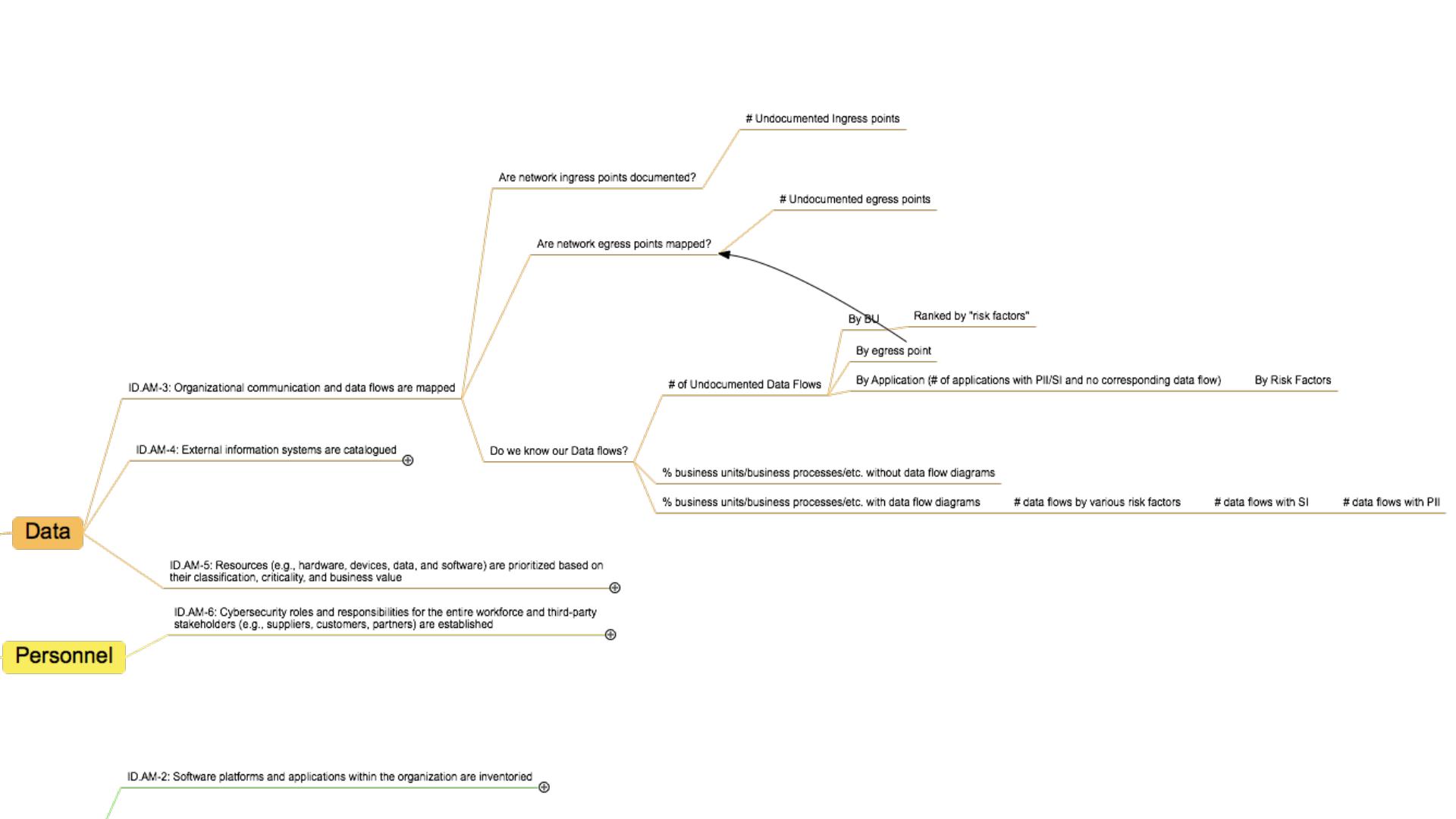




Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

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.





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

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.

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

- NISTCSF.SOCIETYINFORISK.ORG

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

015
e Center

THANK YOU.



@mortman
@alexhutton



#RSAC