RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Succeeding with Enterprise Software Security Key Performance Indicators

SESSION ID: ASEC-T08

Rafal M. Los

Principal, Strategic Security Services
HP Enterprise Services
@Wh1t3Rabbit

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Introduction to Key Performance Indicators (KPIs)

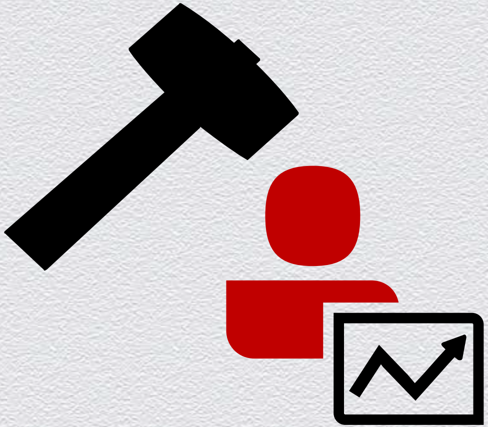
Reporting on progress is tricky

If you spend $1M, **then…**?

First things first…

Who here reports metrics?

How many metrics do you track?



I was once a victim of metrics

Do your metrics give you *insight*?

KPIs do.

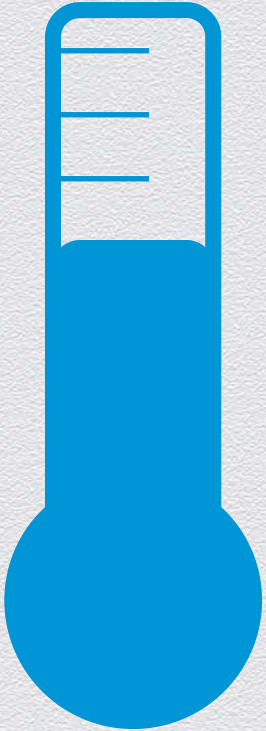
KPI = Key Performance Indicator

A key performance indicator (KPI) is a **measure of performance**, commonly used to help an organization define and evaluate how successful it is, typically in terms of making progress towards its long-term organizational goals.

…but implies you have long-term organizational goals!

TL;DR:

“Are you succeeding?”



..and how much, relative to goals?

Trademarks of good KPIs:

1) Show relative distance to a goal

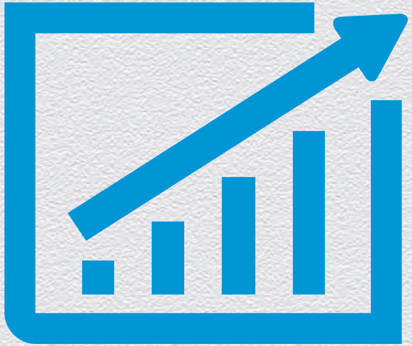
2) Establish relevance to org

3) Establish relevance to security

>> context <<

metrics vs KPIs

How do you convey “improving”?



Improvement

as a result of

effort

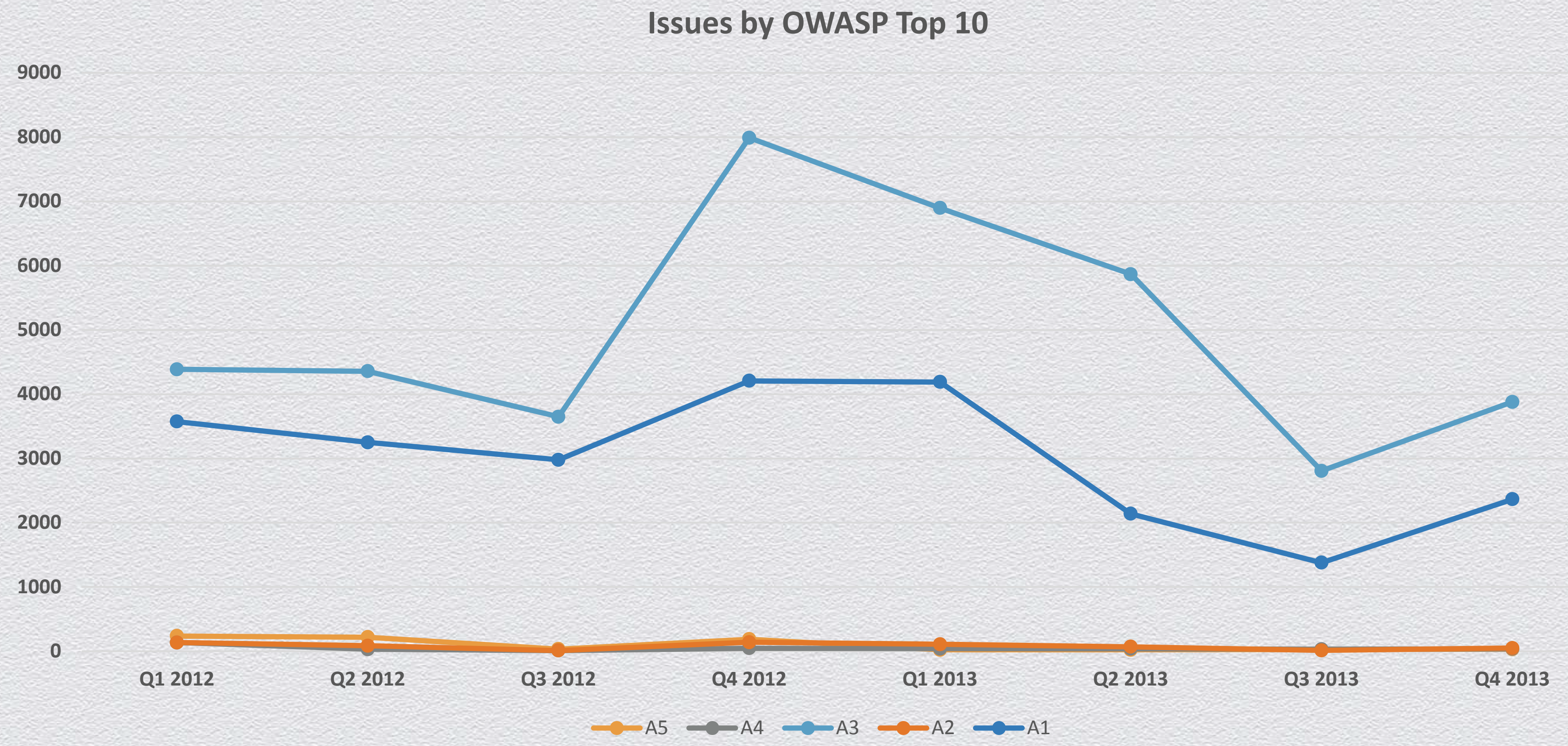
Easy right?

So why are we *so bad at it?*

More importantly…

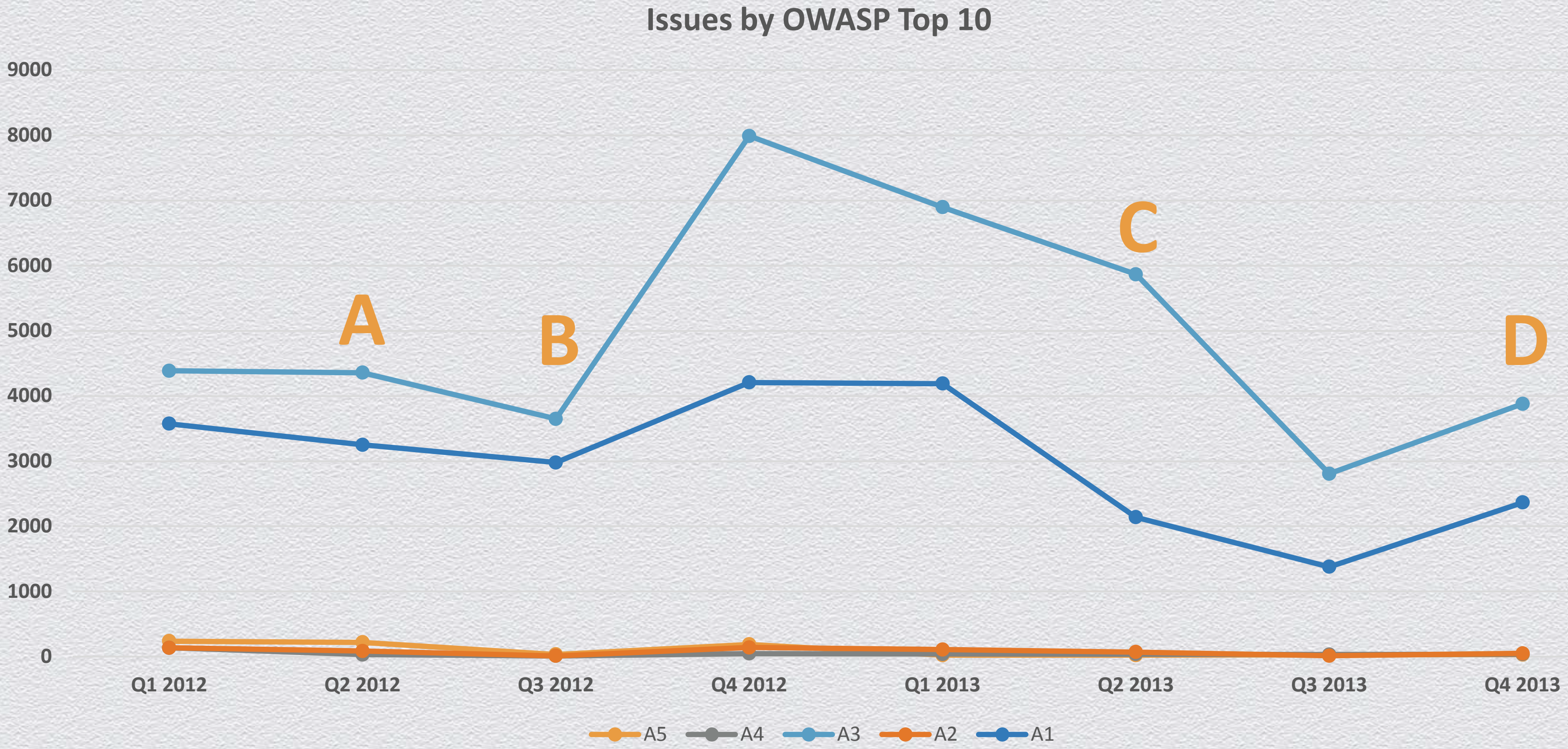
..how do you define success?

Study the following graph:


Issues by OWASP Top 10
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013
Q4 2013
A5
A4
A3
A2
A1

What does it show?

Look again…



Issues by OWASP Top 10
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
A
B
C
D
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013
Q4 2013
A5
A4
A3
A2
A1

#RSAC

A: Implemented mandatory testing

B: Major acquisition

C: Integration into primary dev cycle

D: Switched s/w sec testing tools

#RSAC

Clearly, the graph is inadequate

Raw data:

Q1 2012	3575	135	4387	135	237
Q2 2012	3250	87	4357	31	219
Q3 2012	2978	12	3648	12	35
Q4 2012	4208	141	7989	47	187
Q1 2013	4189	109	6897	41	24
Q2 2013	2138	71	5867	39	23
Q3 2013	1378	14	2807	31	28
Q4 2013	2366	51	3879	38	31
	A1	A2	A3	A4	A5

Q1-Q2 2013: 49% decrease in A1

Q3-Q4 2013: 72% increase in A1

Clearly this is data without context

This shows no **impact**

Defining effective KPIs

What makes a good KPI?

1. Relative distance to goal
2. Relevance to organization
3. Relevance to security

Focus on 4 key SwSec areas

“Impact to effort”

Impact of a security item to the overall effort of the project

[security item] → [dev effort]

Security items (examples)

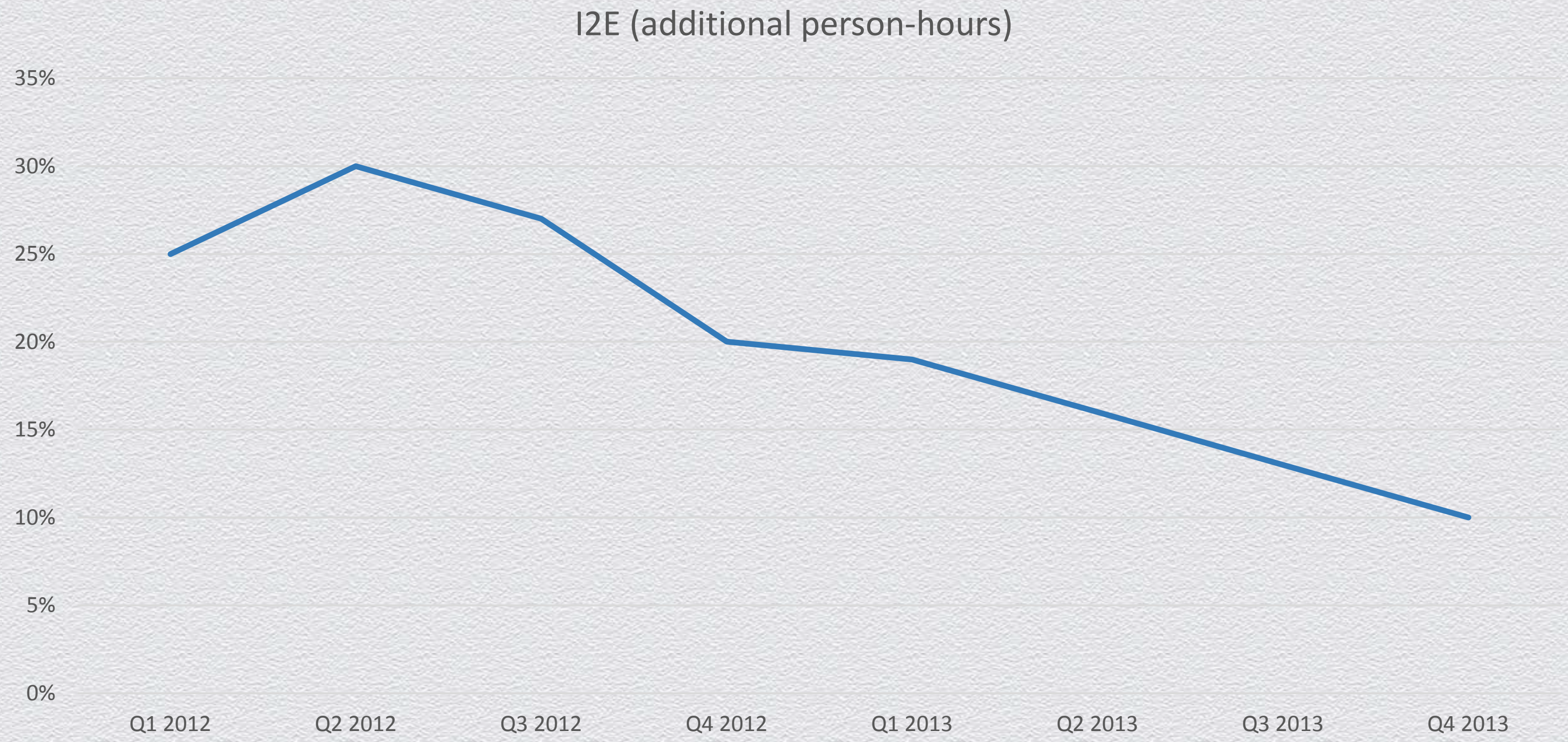
- static analysis process
- dynamic analysis process
- integrating testing tools
- developer awareness

Development effort

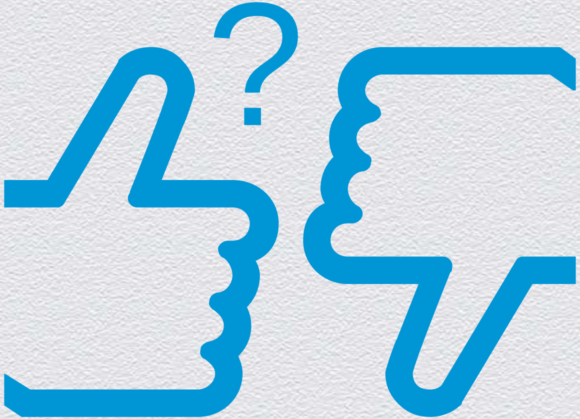
- person-hours required to complete existing task

"By adding a dynamic testing process we initially added 25% effort but over 4 quarters now only add 10%"

– AppSec Prog Mgr


I2E (additional person-hours)
35%
30%
25%
20%
15%
10%
5%
0%
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013
Q4 2013

We’re showing that we’re impacting the AppDev process less over time



Doesn’t tell us if it’s helping security …

“Impact to release”

Impact of a security item to the release timeline

[security item] → [release timeline]

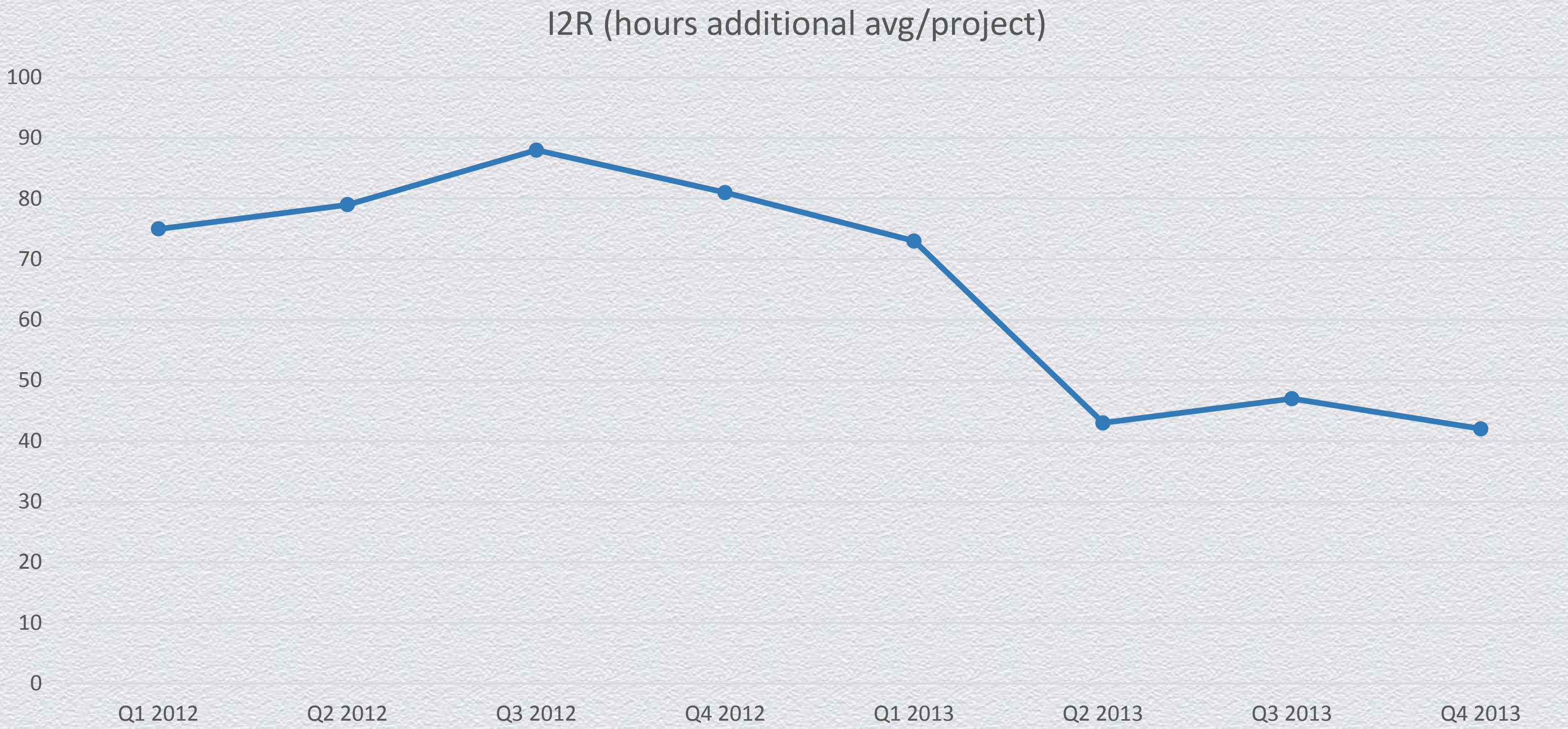
Security items (examples)

- integrating security testing early in development
- providing templates for ‘fixes’
- defining pre-built code modules

Release timeline

- person-hours required to complete existing task

“We were able to show that we could release faster if security was involved earlier on in development”
– AppSec Prog Mgr


I2R (hours additional avg/project)
100
90
80
70
60
50
40
30
20
10
0
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013
Q4 2013

We’re showing that we’re impacting the release process less over time

“Impact to uptime”

Impact of a security item to the uptime of the application/service

[security item] → [uptime]

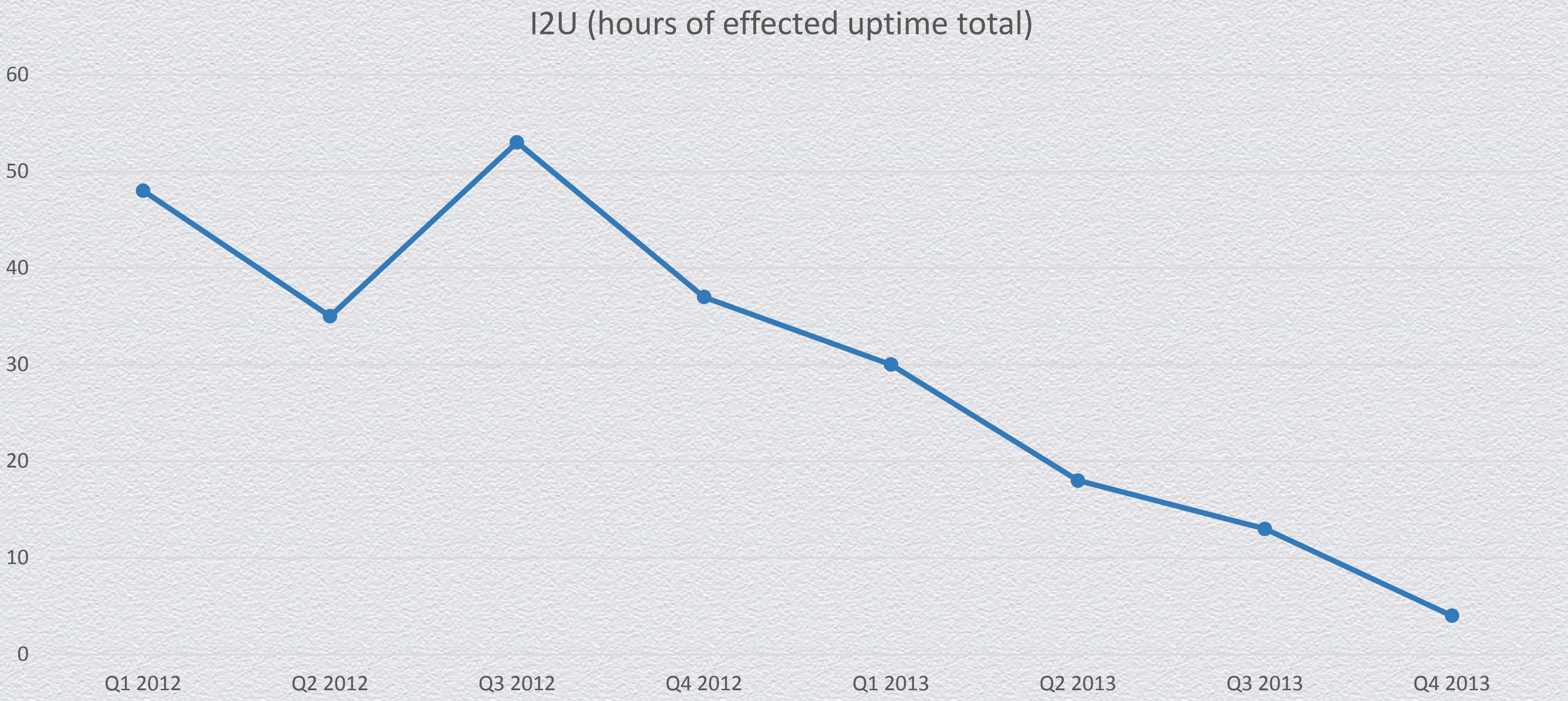
Security items (examples)

- continuous security monitoring
- continuous/regular testing
- remediation of exploitable vulns

Uptime

- an application/service event that causes downtime due to security-related issue (configuration, attack, etc.)

“We were able to prove that remediating all discovered SQL injection issues caused less application downtime”
– AppSec Prog Mgr


I2U (hours of effected uptime total)
60
50
40
30
20
10
0
Q1 2012
Q2 2012
Q3 2012
Q4 2012
Q1 2013
Q2 2013
Q3 2013
Q4 2013

We’re showing that removing injection vulnerabilities, which are easily exploitable, reduces downtime.

“Impact to residual risk”

Impact of a security item to residual risk of an application or service

[security item] → [residual risk]

Security items (examples)

- mandatory peer review of code
- required stage-gates to production w/security sign*-off
- accountability by LoB VP

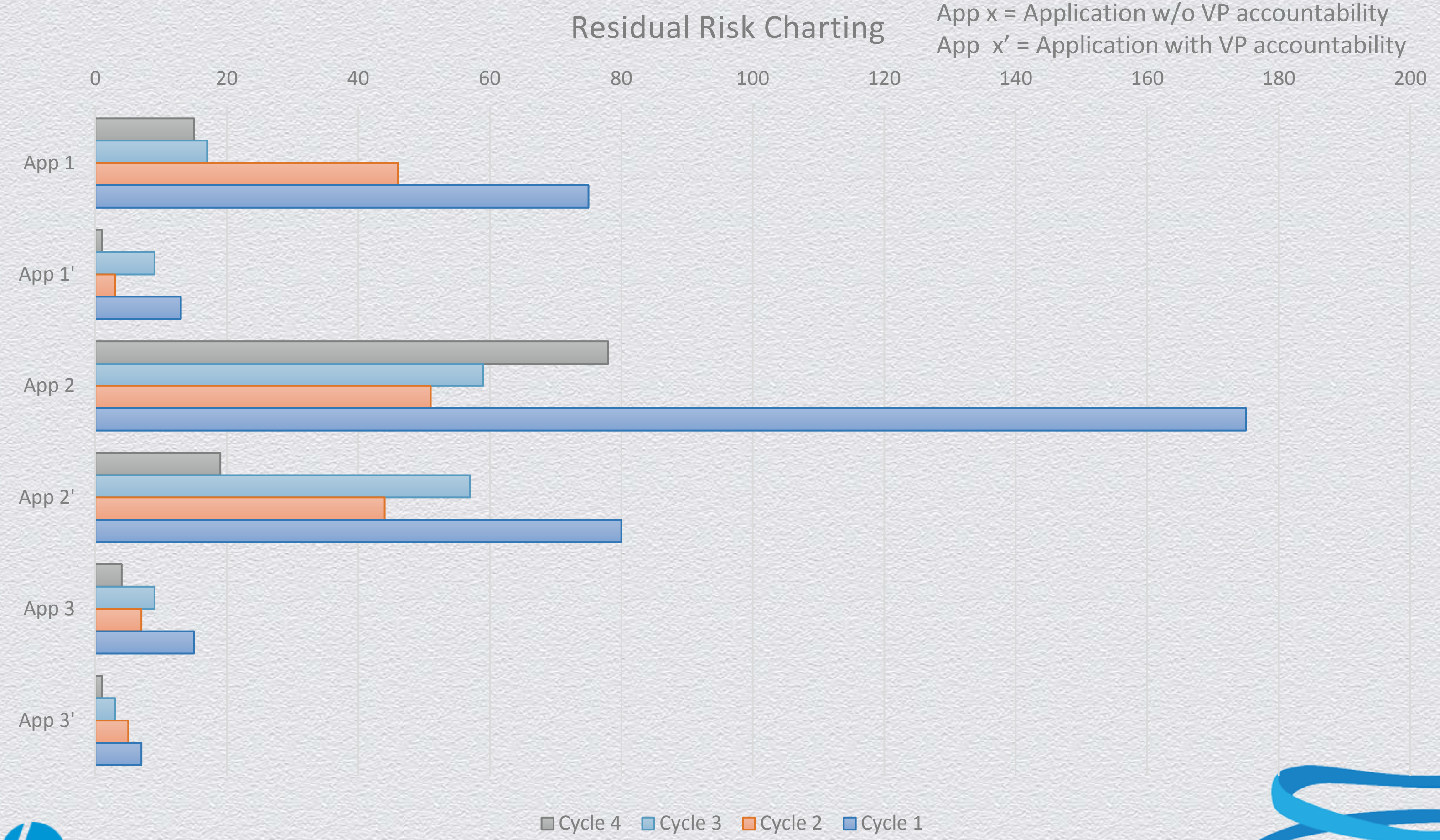
Residual risk

- a level of residual risk in the application as a result of security effort(s)

"For each line of business that reported risk metrics up to the VP successfully, residual risk decreased."

– AppSec Prog Mgr

App x = Application w/o VP accountability
App x’ = Application with VP accountability



We’re showing that raising accountability to the LoB VP, residual risks fall greatly

Defining a set of KPIs

What is the goal of your effort?

Minimize injection (A1) defects in new software releases

“Let’s show progress”

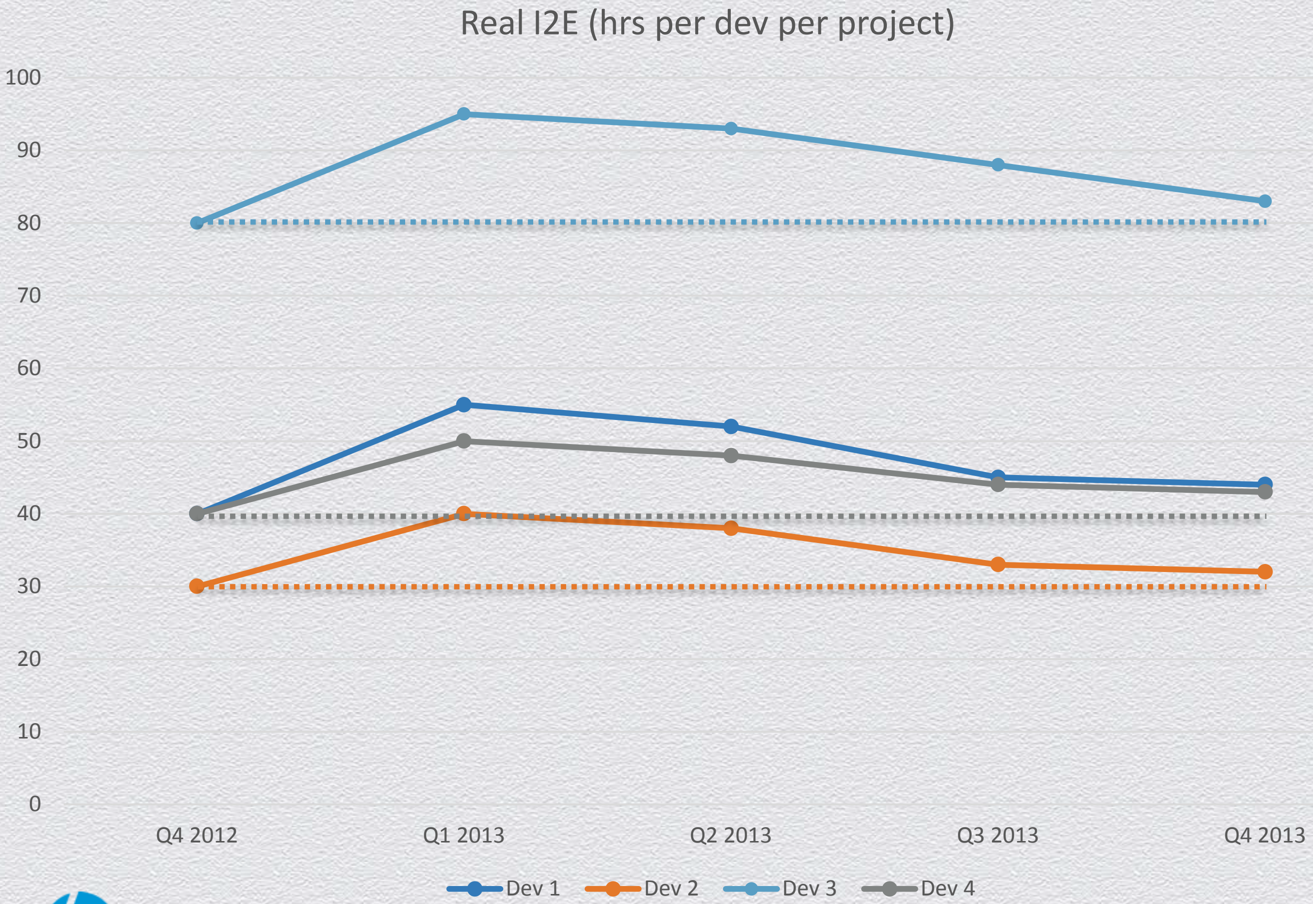
What security did:

Introduced (self-service) static analysis tools into development cycle

Impact it had:

Initially the impact was prohibitive, but with effort became manageable.

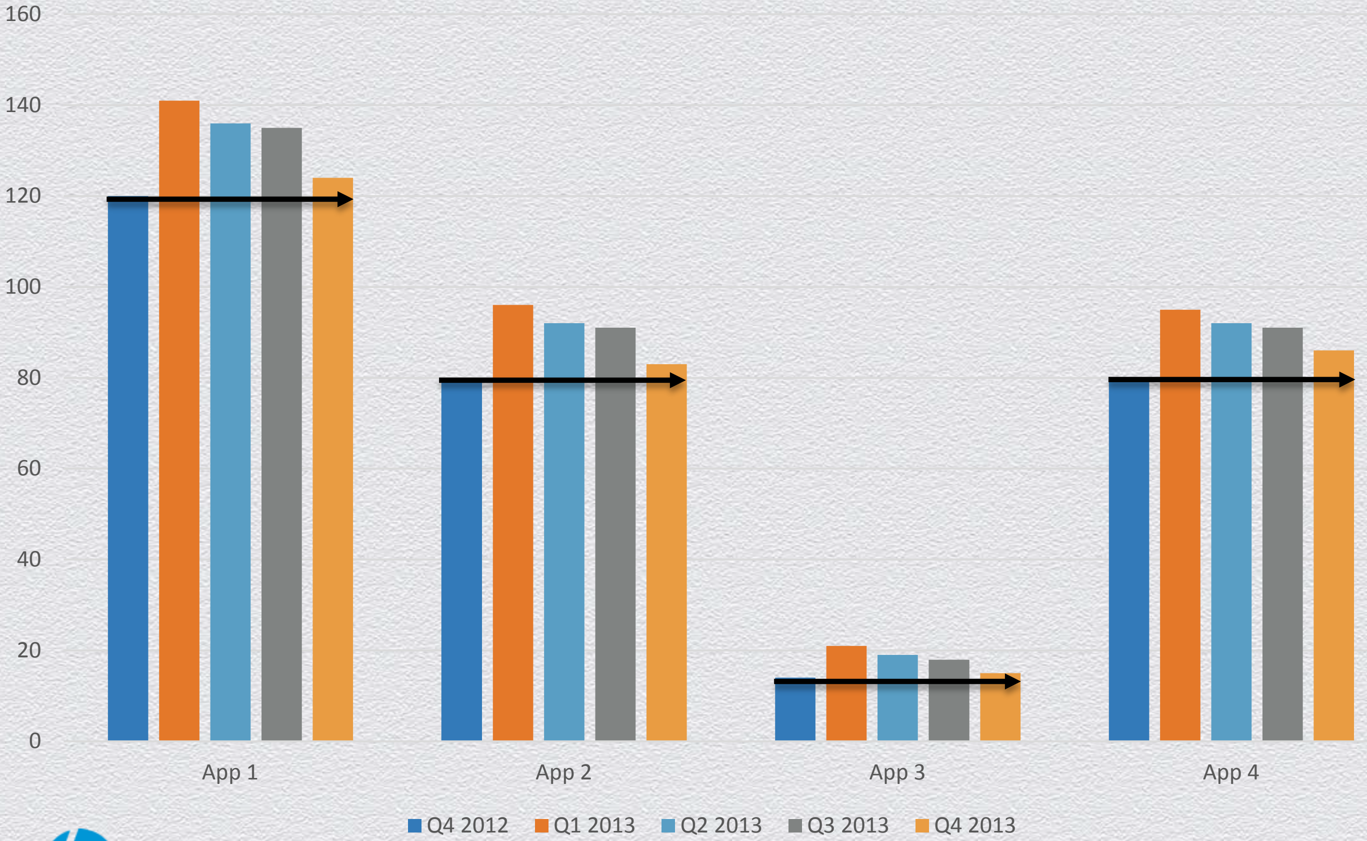
“Impact to effort”



Q4 2012	Baseline
Q1 2013	Initial rollout
Q2 2013	Product training
Q3 2013	IDE Automation
Q4 2013	Workstream integration

“Impact to release”

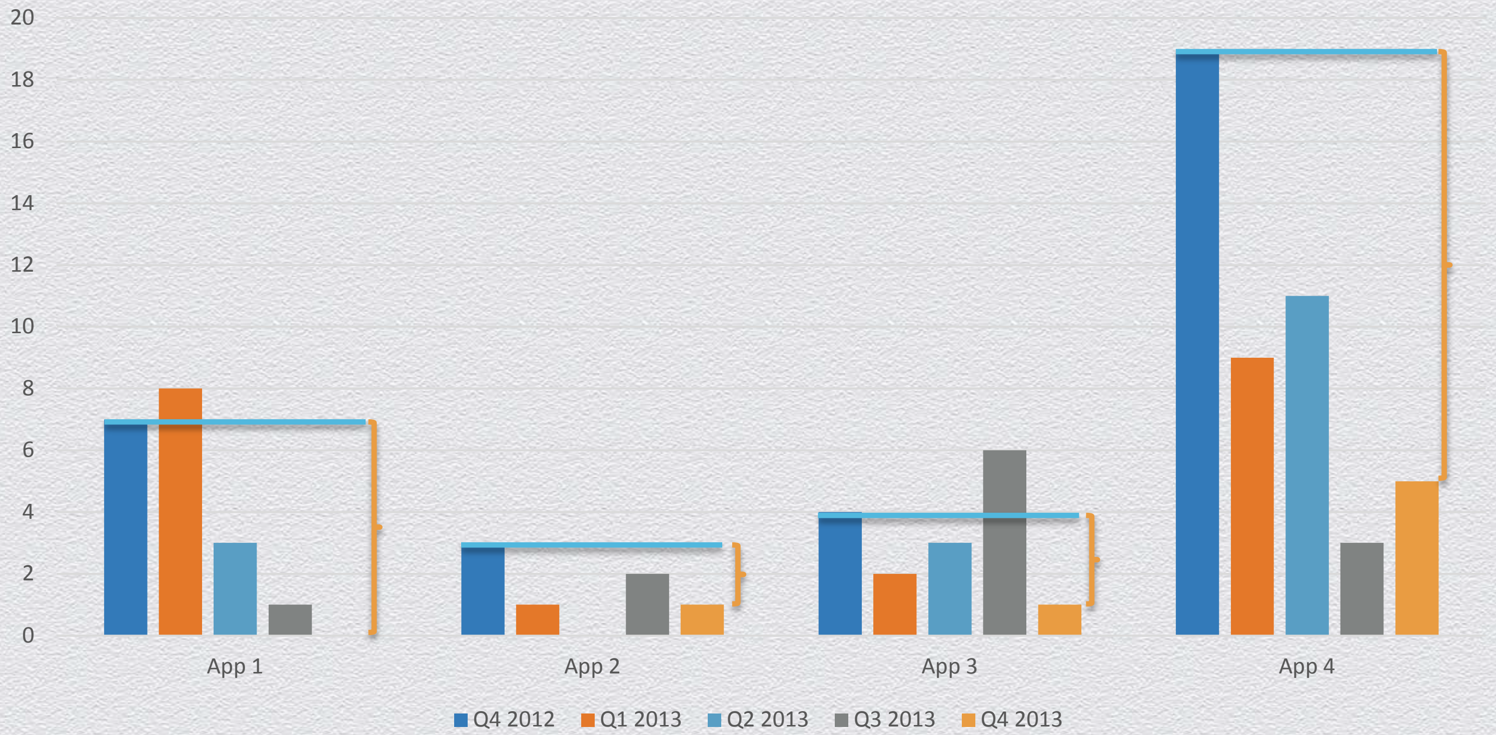
Real I2E (hrs per dev per project)



Q4 2012	Baseline
Q1 2013	Initial rollout
Q2 2013	Product training
Q3 2013	IDE Automation
Q4 2013	Workstream integration

“Impact to uptime”

Security related downtime events

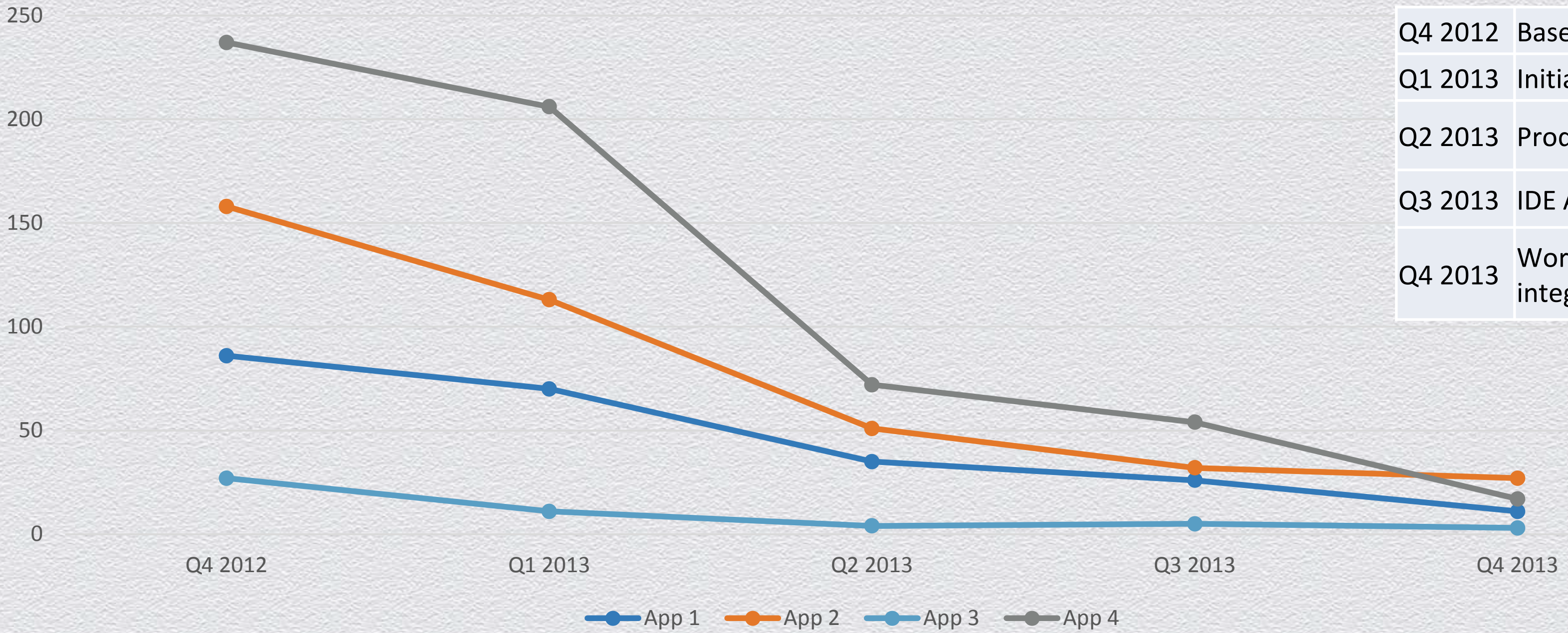


Q4 2012	Baseline
Q1 2013	Initial rollout
Q2 2013	Product training
Q3 2013	IDE Automation
Q4 2013	Workstream integration

“Impact to residual risk”

Impact to residual risk

*Only A1 + A2 (OWASP Top 10)



Q4 2012	Baseline
Q1 2013	Initial rollout
Q2 2013	Product training
Q3 2013	IDE Automation
Q4 2013	Workstream integration

*based on organization's basic IT risk' calculation

For the adventurous:

“Impact to business”

Is this approach perfect?

No.

Do these KPIs work everywhere?

No.

Better than existing metrics?

Absolutely.

Strive to do better.

Demonstrate meaningful progress

Follow the wh1t3rabbit.

https://twitter.com/Wh1t3Rabbit