Local Presence Global Reach

Compliance-driven Security Requirements
Warzaw 12 Oct 2010

Bengt Berg, M.Sc, CISM, CISSP, QSA, ...
Head of Compliance Management Services
Cybercom Sweden East AB

So... Who's Talking?

Who is Bengt Berg?

What is Cybercom?

- 1800 employees, 11 countries, 28 offices
- Turnover
  - ≈60 M€/2006
  - ≈200 M€/2009
- Cybercom Secure: 80 full-time consultants
  - Compliance Management and PCI DSS
  - IAM
  - Forensics
  - Development of secure software components
  - ...and some other areas of expertise

External Compliance Requirements

PCI DSS, Payment Card Industry Data Security Standard,

Sarbanes-Oxley Act

ISO 14001

ISO/EIC 27001:2006

FDA/Part11

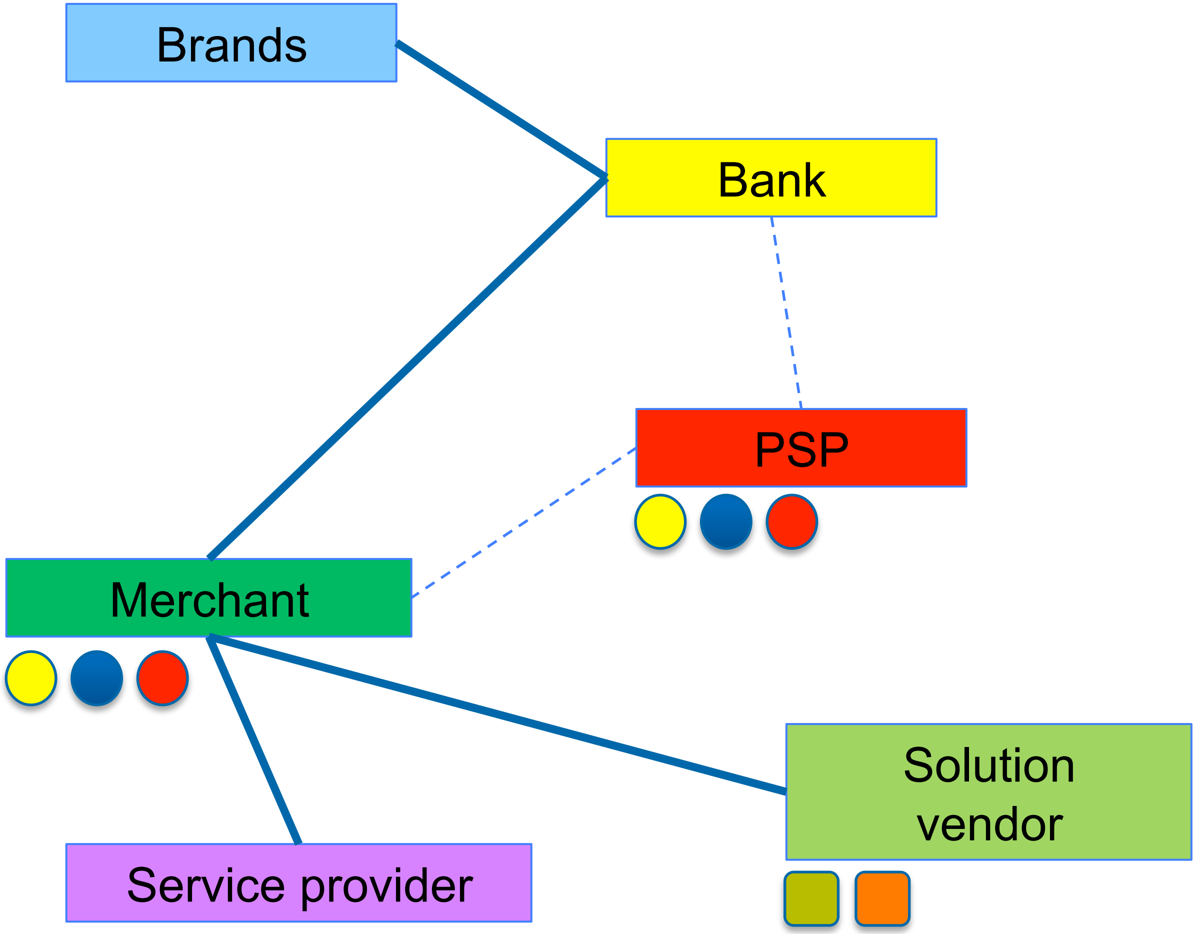
CE certification

Public Sector Procurement Laws

Basel3

How PCI DSS has Transformed the Payment Security Area

PCI DSS



🟡 QSA

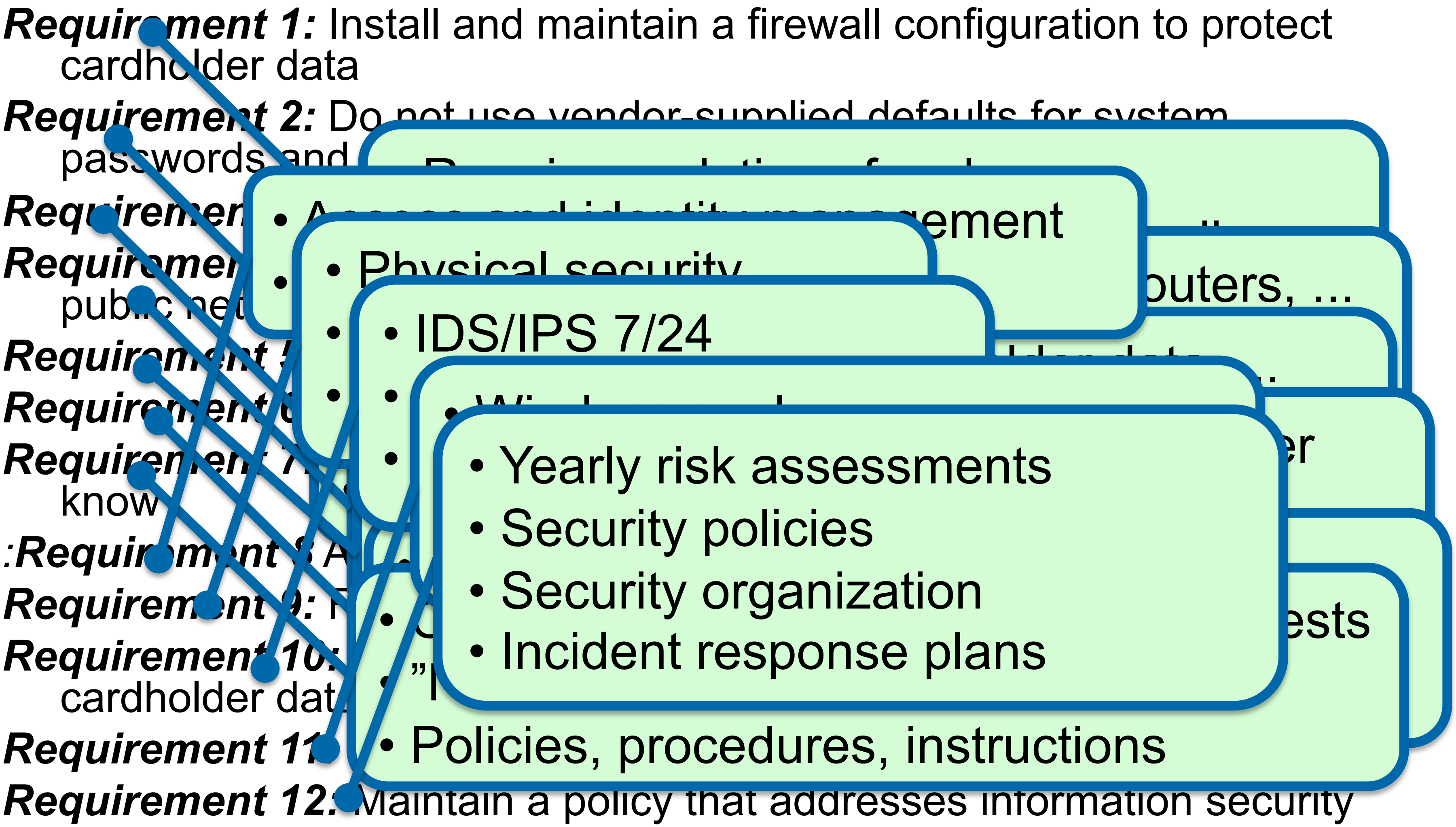
🔵 ASV

🔴 PFI

🟩 PA-QSA

🟧 PTS

But What are These Requirements?



Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and

Requiremen

Requiremen public net

Requirement 5

Requirement 6

Requirement 7: know

:Requirement 8 A

Requirement 9: R

Requirement 10: cardholder dat

Requirement 11

Requirement 12: Maintain a policy that addresses information security

puters, ...
lder data ...
er
ests
• Access and identity management
• Physical security
• IDS/IPS 7/24
• Yearly risk assessments
• Security policies
• Security organization
• Incident response plans
„
• Policies, procedures, instructions

Initial Backlashes

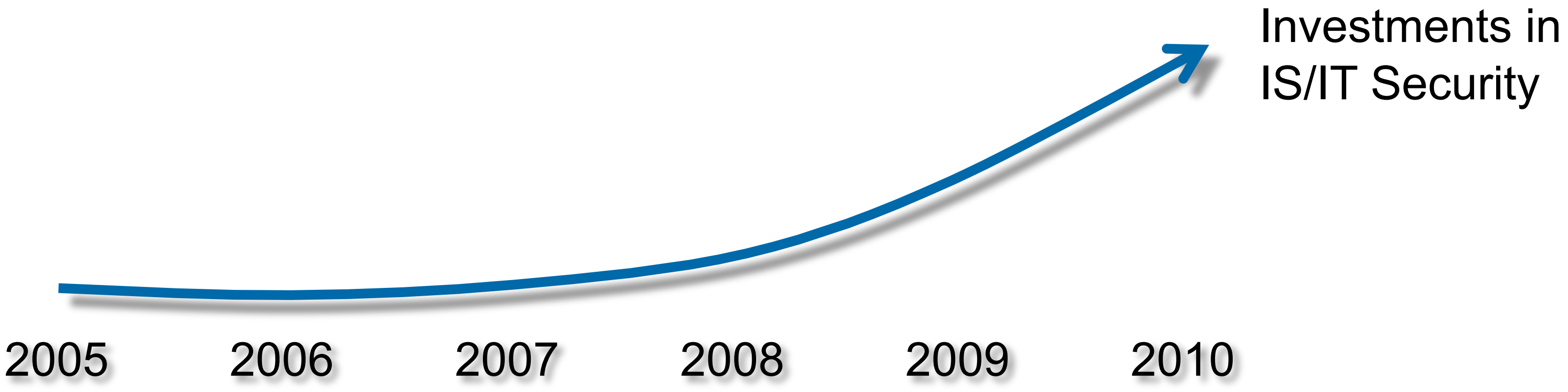
- Conflict of interests
- Banks initially uncoordinated
  - Caused great problems
  - Situation fixed by PAN Nordic
- Self assessments (In Norway: ”self betrayal” ☺)
  - Almost always too nice
- First PA-DSS self-assessment: 45 minutes.

Lesson learned: Patience... Endurance...

Response From Product Suppliers and Consultancy Companies

What Results Have Been Achieved?

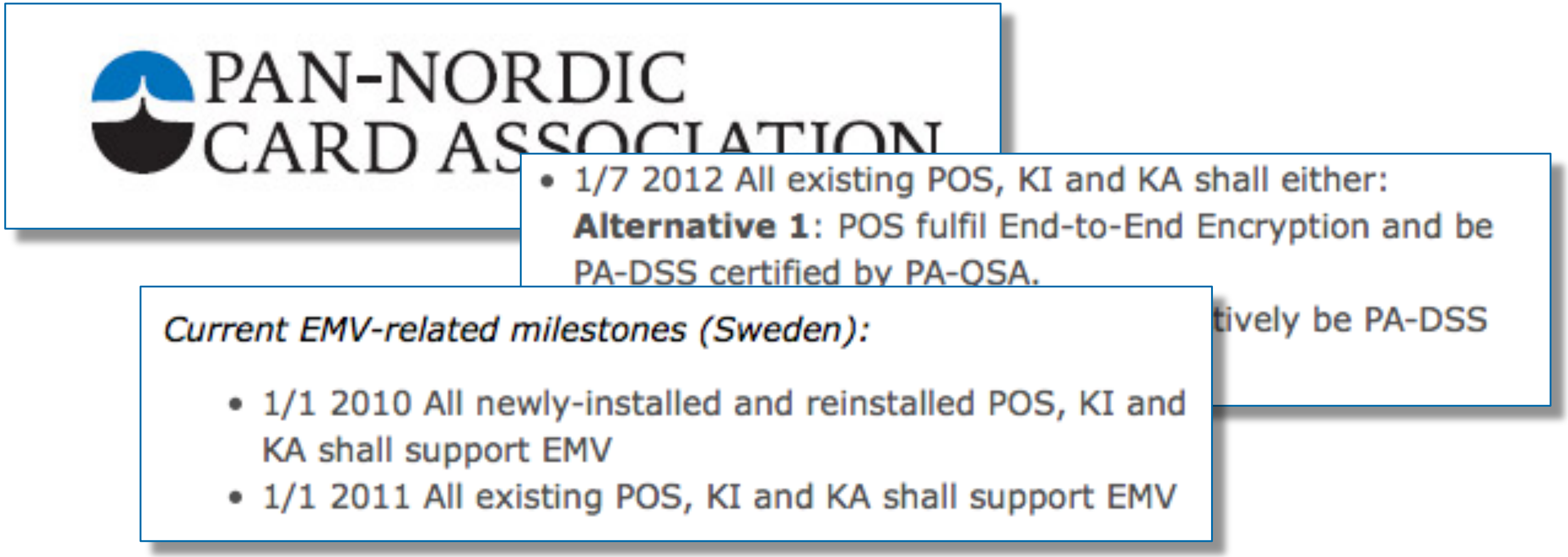
- Retailers now have a very high level of security
- Leveraging the investments into other business areas
  - Using the IDS for the whole company
  - Incident management methods covers the whole company



What Results Have Been Achieved?

CYBERCOM GROUP

- Not possible to sell insecure software to retailers anymore



PAN-NORDIC CARD ASSOCIATION

- 1/7 2012 All existing POS, KI and KA shall either:

  Alternative 1: POS fulfil End-to-End Encryption and be PA-DSS certified by PA-QSA.

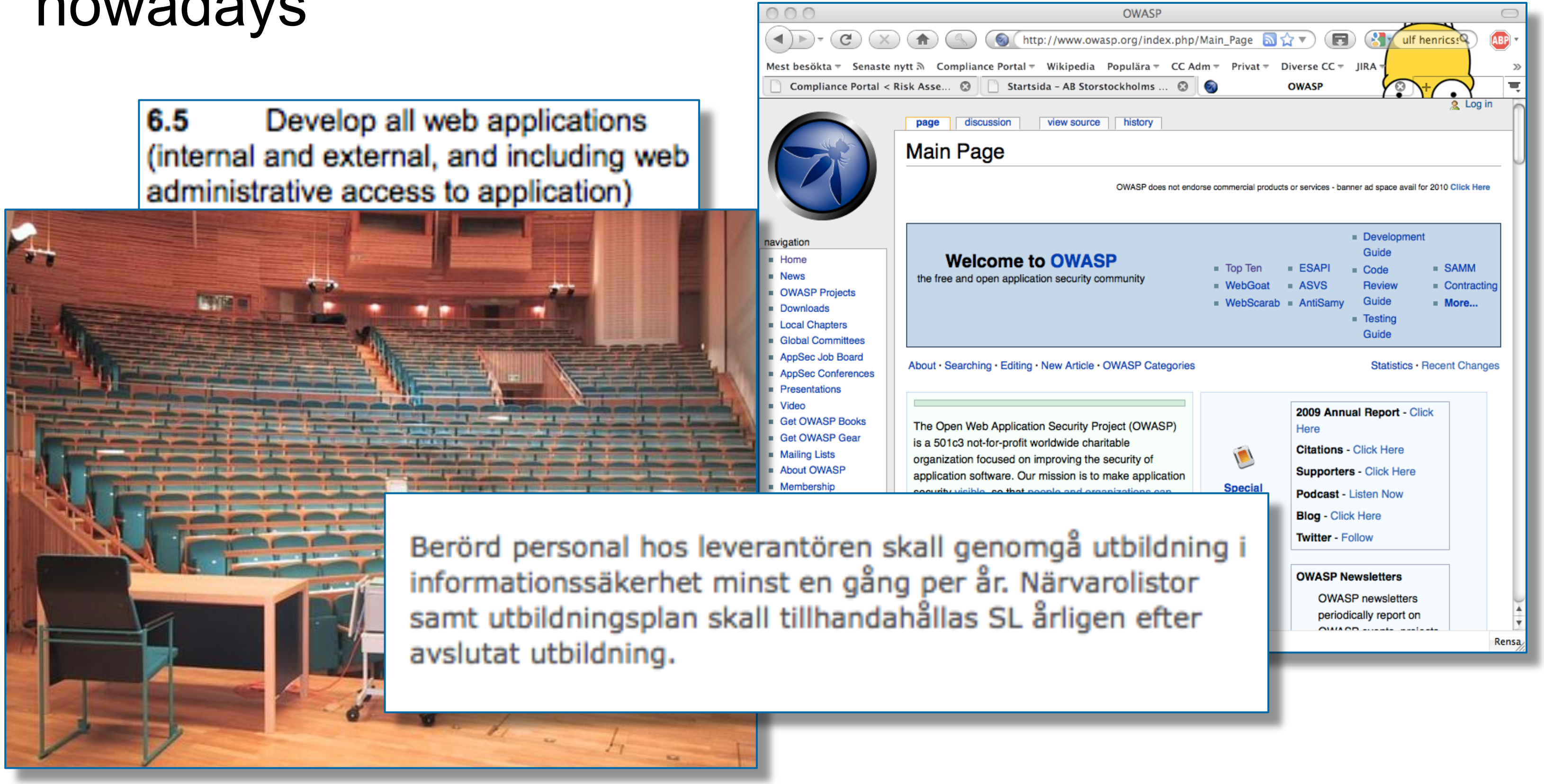
  tively be PA-DSS

Current EMV-related milestones (Sweden):

- 1/1 2010 All newly-installed and reinstalled POS, KI and KA shall support EMV
- 1/1 2011 All existing POS, KI and KA shall support EMV

What Results Have Been Achieved?

- Software developers know about security nowadays



6.5 Develop all web applications (internal and external, and including web administrative access to application)

Berörd personal hos leverantören skall genomgå utbildning i informationssäkerhet minst en gång per år. Närvarolistor samt utbildningsplan skall tillhandahållas SL årligen efter avslutat utbildning.

Main Page

OWASP does not endorse commercial products or services - banner ad space avail for 2010 Click Here

Welcome to OWASP
the free and open application security community

The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can

2009 Annual Report - Click Here

Citations - Click Here

Supporters - Click Here

Podcast - Listen Now

Blog - Click Here

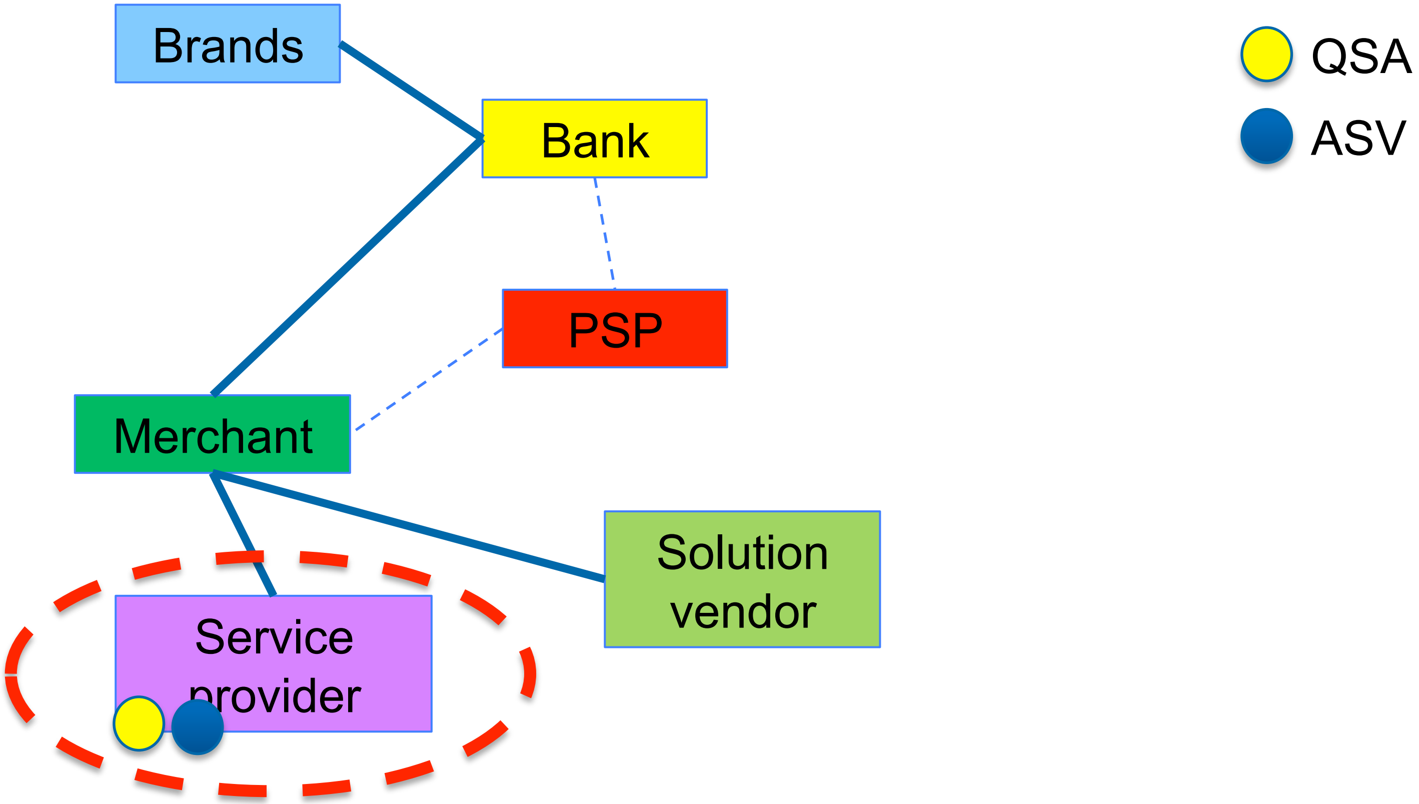
Twitter - Follow

OWASP Newsletters

OWASP newsletters periodically report on OWASP events, projects

What Results Have Been Achieved?

- Increased security amongst outsourcing companies
  - And they make good business out of it!



Emerging Methods for Managing External Compliance Requirements

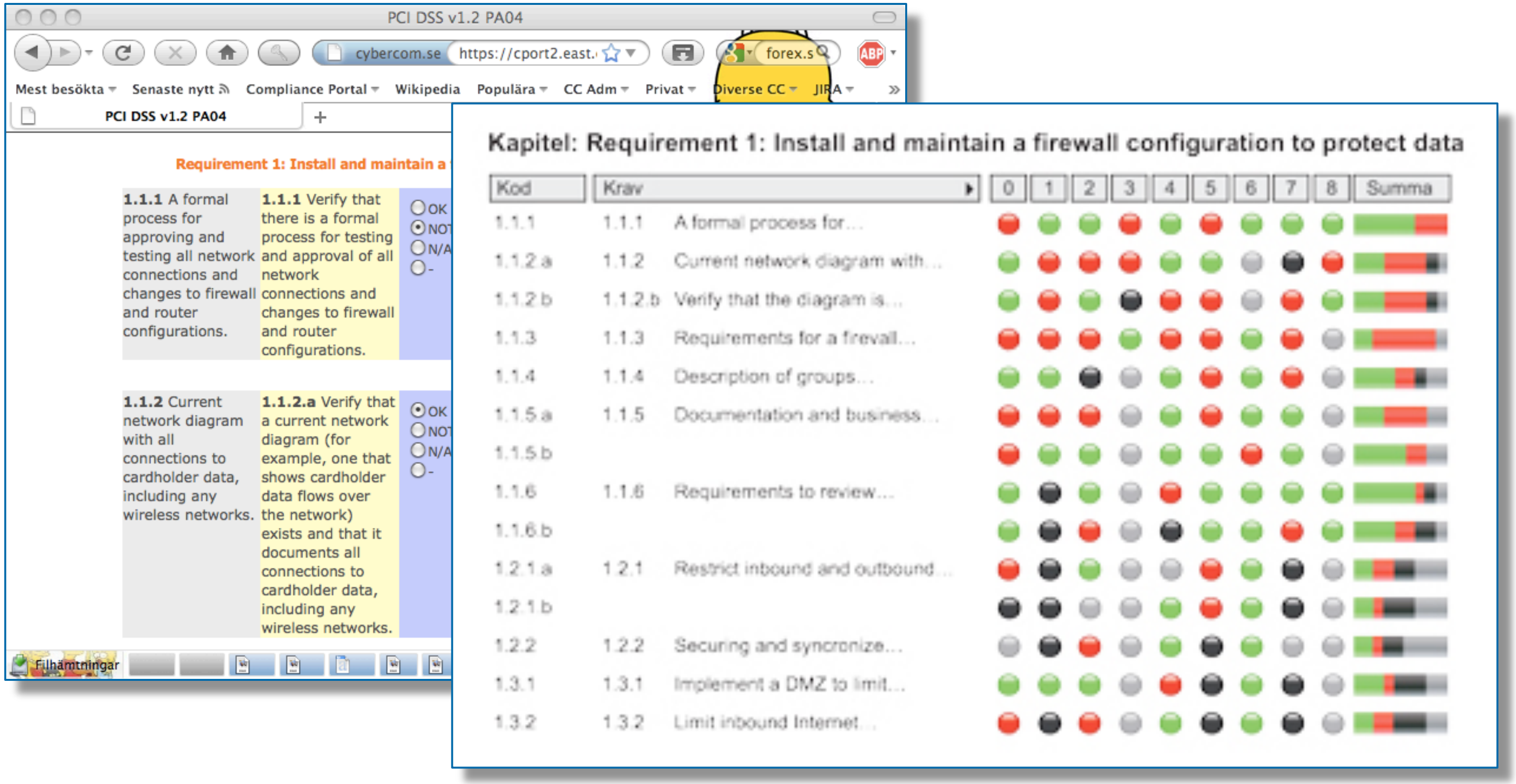
Emerging methods

A few trends growing more solid every day:

1. Portal solutions for compliance management
2. Extreme use of issue management solutions
3. Using wikis for policies and other documentation..
4. Trend-oriented tests of compliance status

Portal Solutions for Compliance Management

- Cybercom, Acrea, ARIS, and numerous others
  - Binders in a bookshelf isn’t enough



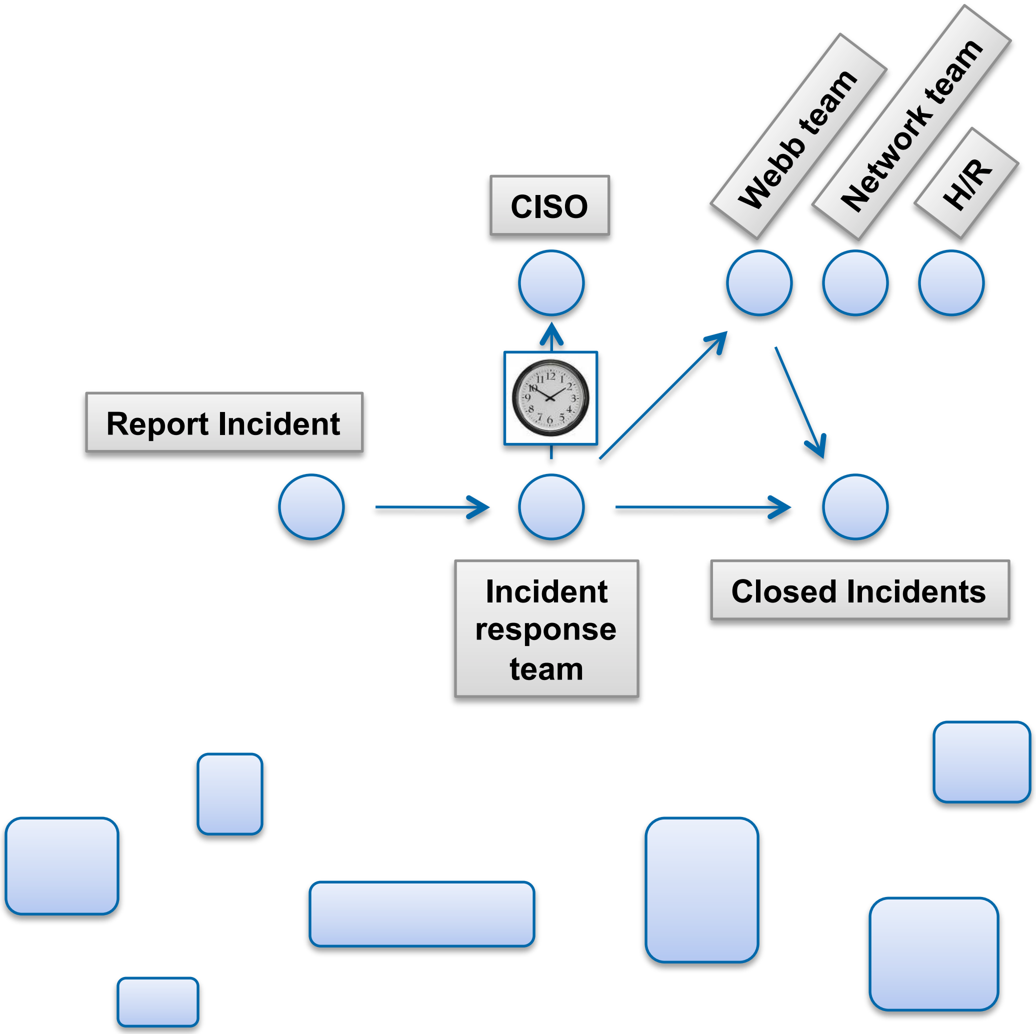
Requirement 1: Install and maintain a

1.1.1 A formal process for approving and testing all network connections and changes to firewall and router configurations.	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	○ OK ● NOT ○ N/A ○ -
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	● OK ○ NOT ○ N/A ○ -

Kapitel: Requirement 1: Install and maintain a firewall configuration to protect data

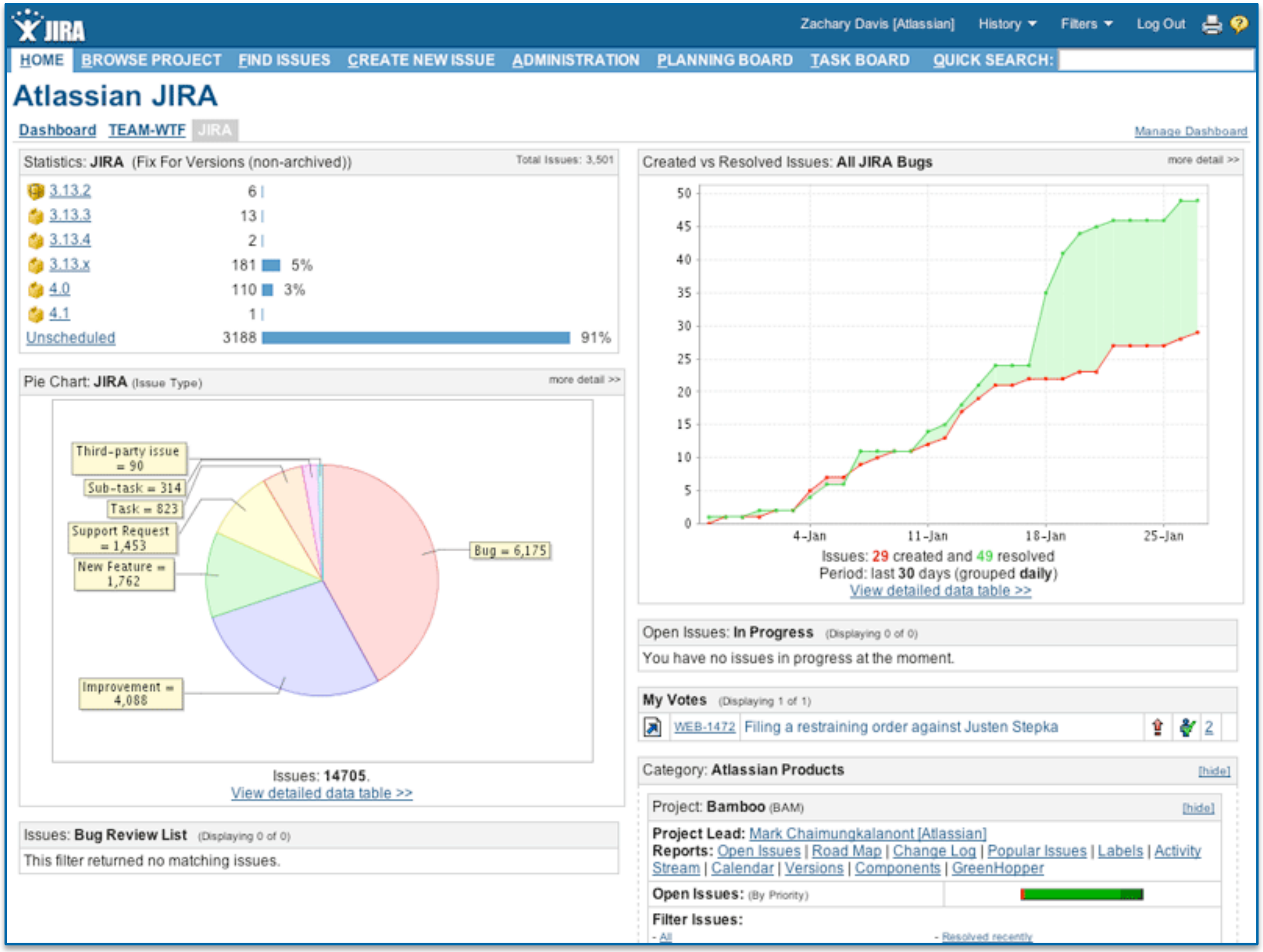
Kod	Krav		0	1	2	3	4	5	6	7	8	Summa
1.1.1	1.1.1	A formal process for...	🔴	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🟢	
1.1.2 a	1.1.2	Current network diagram with...	🟢	🔴	🔴	🔴	🟢	🟢	⚪	⚫	🔴	
1.1.2 b	1.1.2.b	Verify that the diagram is...	🟢	🔴	🟢	⚫	🔴	🔴	⚪	🔴	🟢	
1.1.3	1.1.3	Requirements for a firewall...	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	⚪	
1.1.4	1.1.4	Description of groups...	🟢	🟢	⚫	⚪	🟢	🔴	🟢	🔴	⚪	
1.1.5 a	1.1.5	Documentation and business...	🔴	🔴	🔴	⚪	🟢	🔴	🟢	🟢	⚪	
1.1.5 b			🔴	🟢	🟢	⚪	🟢	🟢	🔴	🟢	⚪	
1.1.6	1.1.6	Requirements to review...	🟢	⚫	🟢	⚪	🔴	🟢	🟢	🟢	🟢	
1.1.6 b			🟢	⚫	🔴	⚪	⚫	🟢	🟢	🔴	🟢	
1.2.1 a	1.2.1	Restrict inbound and outbound...	🔴	⚫	🟢	⚪	⚪	🔴	🟢	⚫	⚪	
1.2.1 b			⚫	⚫	⚪	⚪	🟢	🔴	🟢	⚫	⚪	
1.2.2	1.2.2	Securing and syncronize...	⚪	⚫	🔴	⚪	🟢	⚫	🟢	⚪	⚪	
1.3.1	1.3.1	Implement a DMZ to limit...	🟢	🟢	🟢	⚪	🔴	⚫	🟢	⚫	⚪	
1.3.2	1.3.2	Limit inbound Internet...	🔴	⚫	🔴	⚪	🟢	⚫	🟢	⚫	⚪	

Use of Issue Management Systems



27 workflows neccessary to implement ISO 27001

Use of Issue Management Systems



JIRA

Zachary Davis [Atlassian] History ▾ Filters ▾ Log Out

HOME BROWSE PROJECT FIND ISSUES CREATE NEW ISSUE ADMINISTRATION PLANNING BOARD TASK BOARD QUICK SEARCH:

Atlassian JIRA

Dashboard TEAM-WTF JIRA Manage Dashboard

Statistics: **JIRA** (Fix For Versions (non-archived)) Total Issues: 3,501

3.13.2	6	
3.13.3	13	
3.13.4	2	
3.13.x	181	5%
4.0	110	3%
4.1	1	
Unscheduled	3188	91%

Pie Chart: **JIRA** (Issue Type) more detail >>

Issues: **14705**.
View detailed data table >>

Issues: **Bug Review List** (Displaying 0 of 0)

This filter returned no matching issues.

Created vs Resolved Issues: **All JIRA Bugs** more detail >>

Issues: 29 created and 49 resolved
Period: last **30** days (grouped **daily**)
View detailed data table >>

Open Issues: **In Progress** (Displaying 0 of 0)

You have no issues in progress at the moment.

My Votes (Displaying 1 of 1)

WEB-1472 Filing a restraining order against Justen Stepka 2

Category: **Atlassian Products** [hide]

Project: **Bamboo** (BAM) [hide]

Project Lead: Mark Chaimungkalanont [Atlassian]
Reports: Open Issues | Road Map | Change Log | Popular Issues | Labels | Activity Stream | Calendar | Versions | Components | GreenHopper

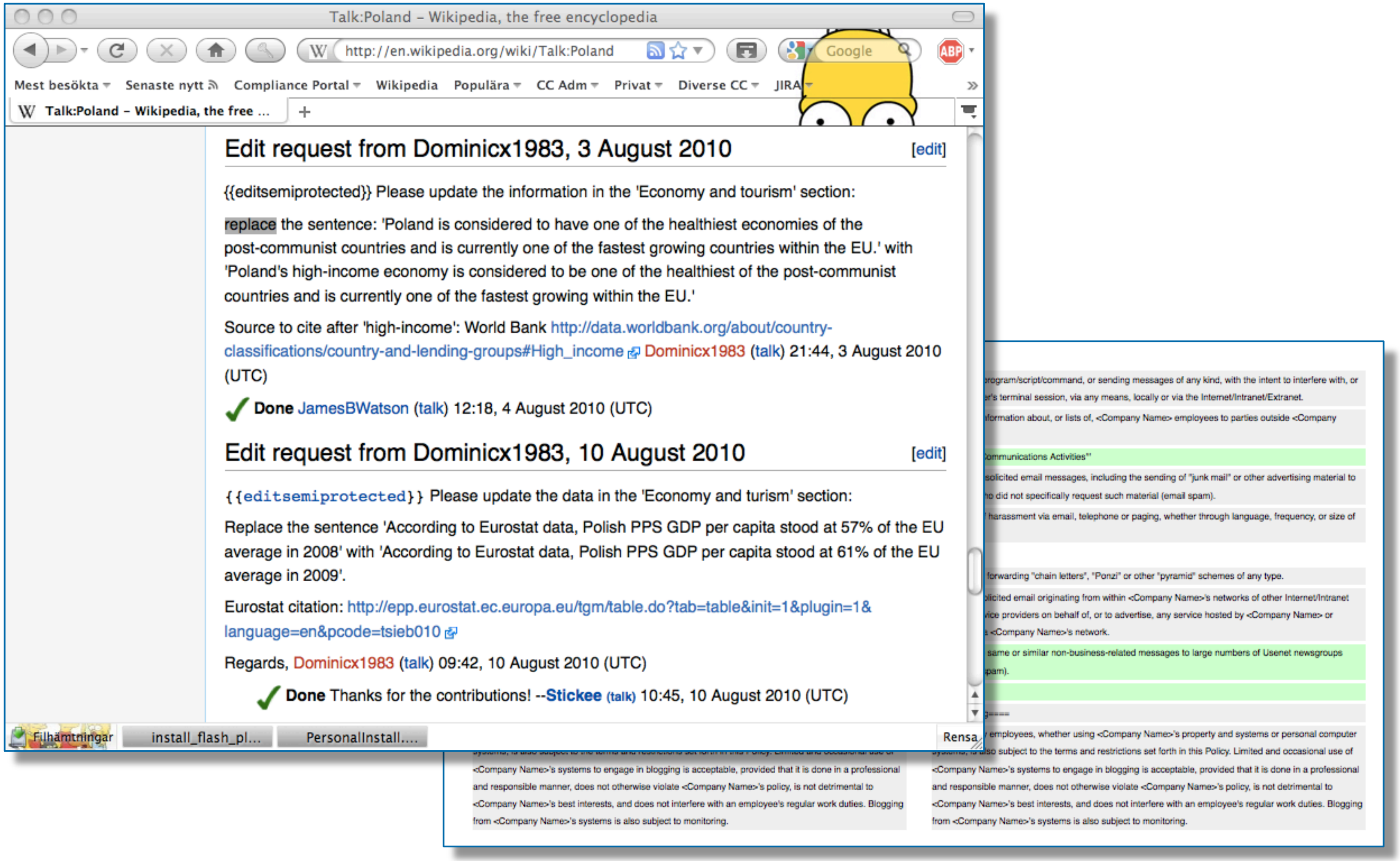
Open Issues: (By Priority)

Filter Issues:
- All - Resolved recently

All Documentation in Wiki format

- All documents easily accessible (read)
  - Policy documents
  - Instructions
- Edit only by document owner
  - Easy to allow ”free for all” in draft mode
- Built-in discussion forum!
  - Let people help each other...
- Built-in functionality for version control

All Documentation in Wiki format



Edit request from Dominicx1983, 3 August 2010

[edit]

{{editsemiprotected}} Please update the information in the 'Economy and tourism' section:

replace the sentence: 'Poland is considered to have one of the healthiest economies of the post-communist countries and is currently one of the fastest growing countries within the EU.' with 'Poland's high-income economy is considered to be one of the healthiest of the post-communist countries and is currently one of the fastest growing within the EU.'

Source to cite after 'high-income': World Bank http://data.worldbank.org/about/country-classifications/country-and-lending-groups#High_income Dominicx1983 (talk) 21:44, 3 August 2010 (UTC)

✓ **Done** JamesBWatson (talk) 12:18, 4 August 2010 (UTC)

Edit request from Dominicx1983, 10 August 2010

[edit]

`{{editsemiprotected}}` Please update the data in the 'Economy and turism' section:

Replace the sentence 'According to Eurostat data, Polish PPS GDP per capita stood at 57% of the EU average in 2008' with 'According to Eurostat data, Polish PPS GDP per capita stood at 61% of the EU average in 2009'.

Eurostat citation: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tsieb010

Regards, Dominicx1983 (talk) 09:42, 10 August 2010 (UTC)

✓ **Done** Thanks for the contributions! --**Stickee** (talk) 10:45, 10 August 2010 (UTC)

rogram/script/command, or sending messages of any kind, with the intent to interfere with, or
r's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

formation about, or lists of, <Company Name> employees to parties outside <Company

ommunications Activities"'

solicited email messages, including the sending of "junk mail" or other advertising material to
o did not specifically request such material (email spam).

harassment via email, telephone or paging, whether through language, frequency, or size of

forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

licited email originating from within <Company Name>'s networks of other Internet/Intranet
ice providers on behalf of, or to advertise, any service hosted by <Company Name> or
<Company Name>'s network.

same or similar non-business-related messages to large numbers of Usenet newsgroups
pam).

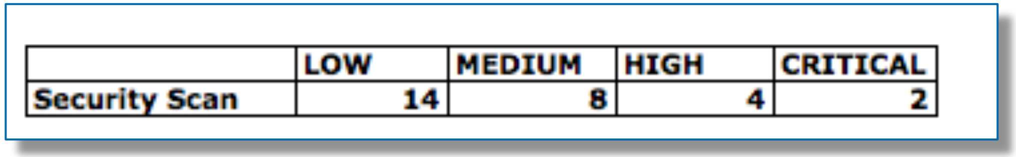
g====

employees, whether using <Company Name>'s property and systems or personal computer
so subject to the terms and restrictions set forth in this Policy. Limited and occasional use of
<Company Name>'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>'s systems is also subject to monitoring.

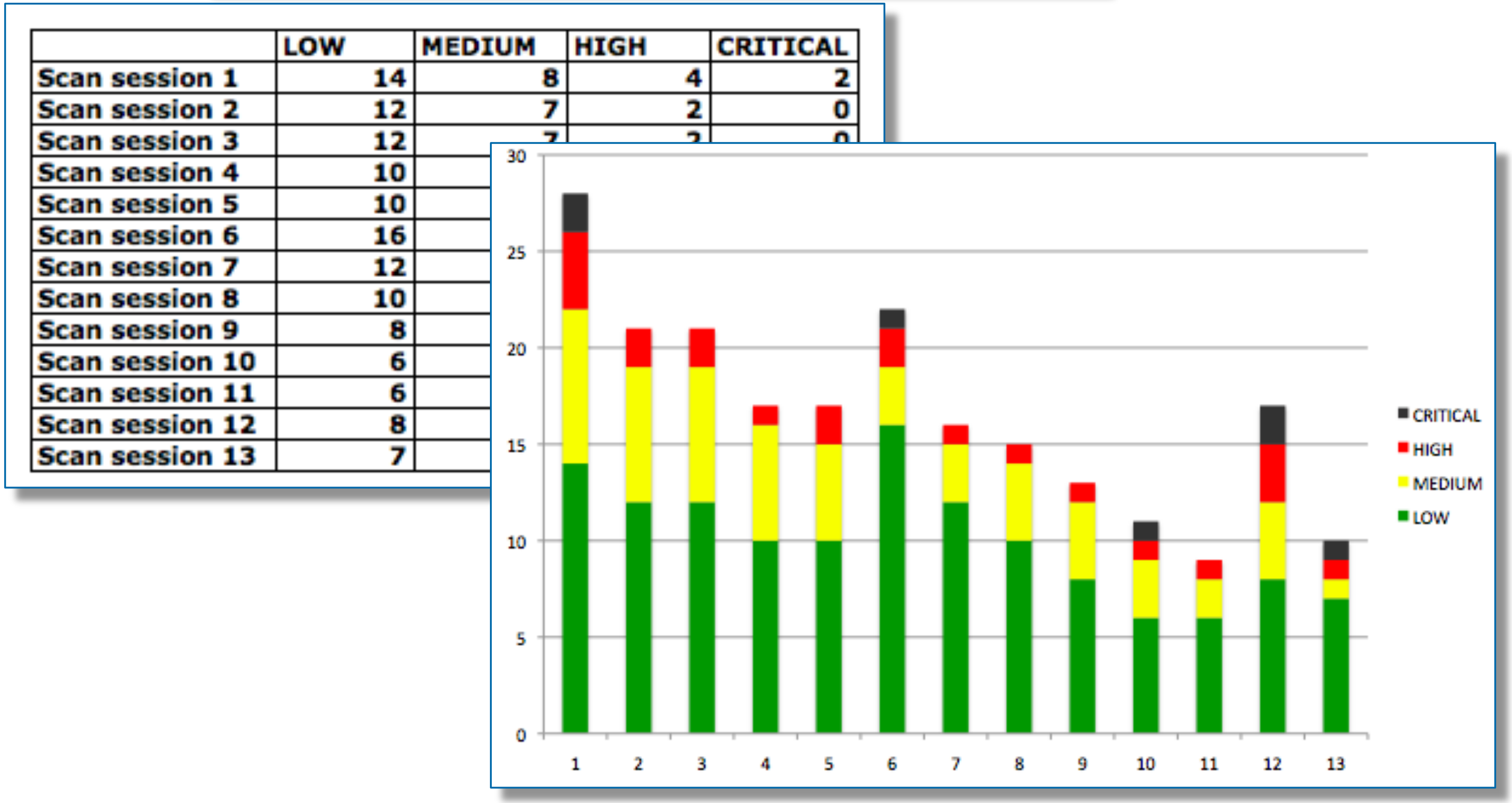
<Company Name>'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>'s systems is also subject to monitoring.

Trend-oriented tests

CYBERCOM GROUP



	LOW	MEDIUM	HIGH	CRITICAL
Security Scan	14	8	4	2



	LOW	MEDIUM	HIGH	CRITICAL
Scan session 1	14	8	4	2
Scan session 2	12	7	2	0
Scan session 3	12	7	2	0
Scan session 4	10			
Scan session 5	10			
Scan session 6	16			
Scan session 7	12			
Scan session 8	10			
Scan session 9	8			
Scan session 10	6			
Scan session 11	6			
Scan session 12	8			
Scan session 13	7			

Conclusions

- What are the effects of external compliance requirements?

New compliance-oriented business models

Will always benefit the outsourcing providers

Rational methods decrease investment

The leader gets a competitive advantage

Success depends on the governance framework

Nobody wants to be a problem for their customer