Closing the Gap Between Network Policy Creation and Enforcement

- Field Report from a Managed Security Provider -

Sven Bruelisauer

Senior Security Engineer Open Systems

sb@open.ch

mission control™
security services

FIRST
Improving Security Together

Vitals & Insights

Protect Your Assets ...

mission control™
security services
by open systems ag
www.open.ch

→ Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Agenda

Purpose of Network Security Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control – An Example

Closing the Gap

Q & A

Purpose of Network Security Policy

Help to Protect Company Assets

Agenda

→ Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Purpose of Network Security Policy

Ensure Secure Data Transfer

Agenda

→ Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Purpose of Network Security Policy

Ensure Availability & Redundancy Management

- Agenda
- → Purpose of Network Policy
- How & Who
- Pitfalls from Reality
- The Ability to Design
- The Ability to Create
- The Ability to Manage & Execute
- Mission Control
- Closing the Gap
- Q & A

Purpose of Network Security Policy

Ensure Protection of Services & Stop Defacements

Agenda

→ Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Purpose of Network Security Policy

Ensure Secure Network User Identification

Agenda

→ Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Purpose of Network Security Policy

… Distinguish the Good from the Bad

Agenda

→ Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

How & Who
Avoiding the Gap

Agenda

Purpose of Network Policy

→ How & Who

Pitfalls from Reality

The Ability to Design

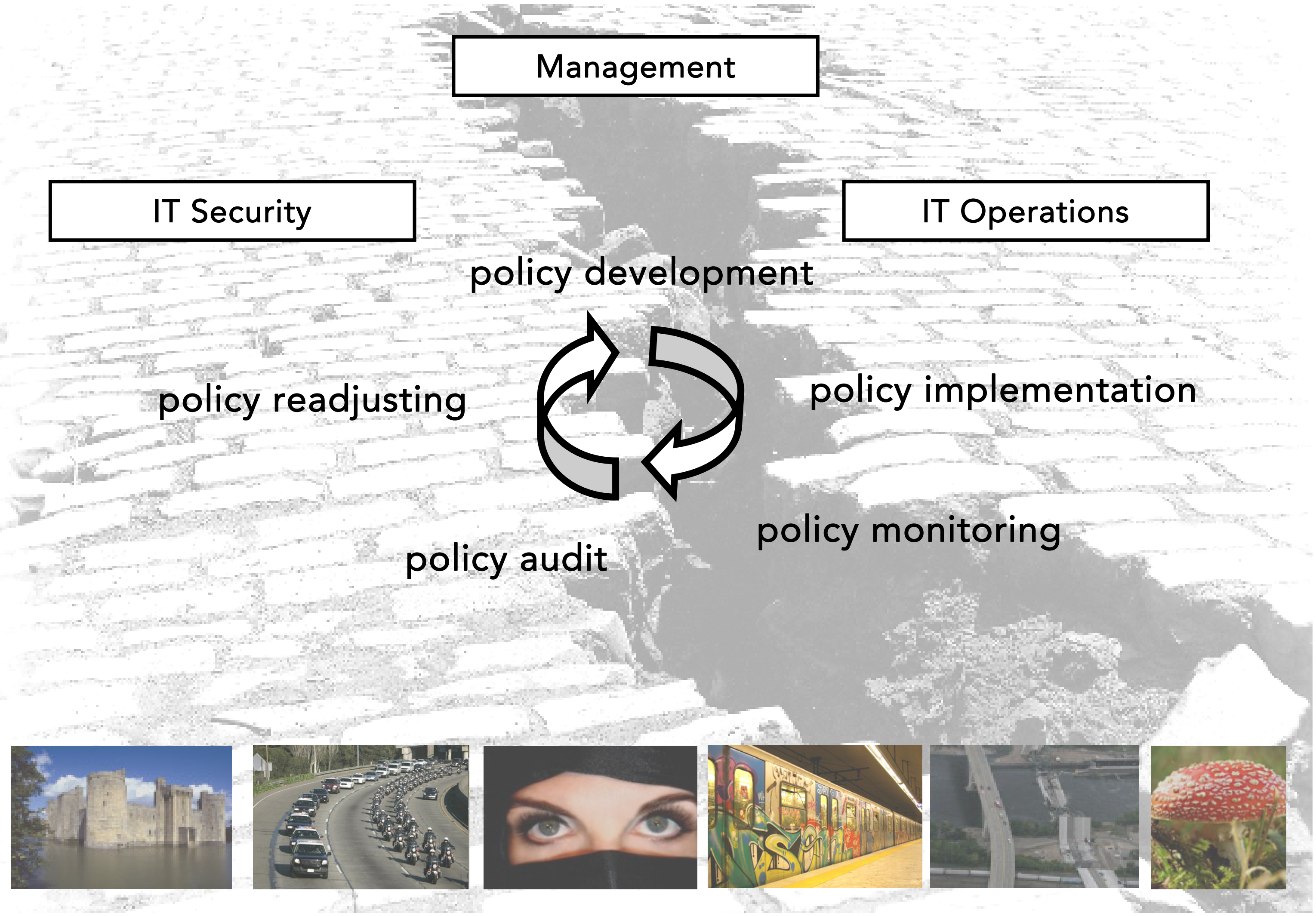
The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A



Management

IT Security

IT Operations

policy development

policy implementation

policy monitoring

policy audit

policy readjusting

Agenda

Purpose of Network Policy

How & Who

→ Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Major Pitfalls from Reality
Clear by Theory but …

Lack of responsibility

Everybody signs – Who enforces?
ISO, SOX, ITIL, inspection

Lack of design

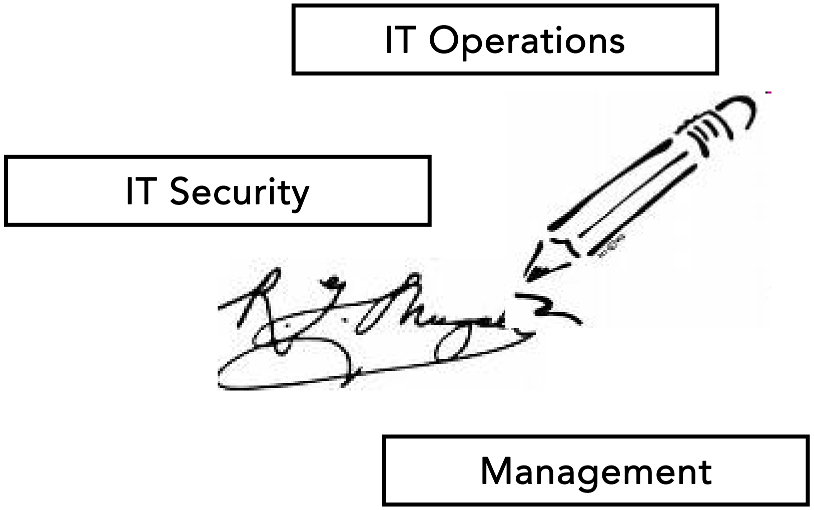
The rule of the weakest link…

Lack of flexibility

Mergers & Acquisitions

Lack of control

Technology risk
Enforcements


IT Operations

IT Security

Management

The Ability to Design
A Living Example…

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

→ The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

A global Swiss supplier of integrated logistics solutions

swisslog

2239 employees
20 countries
4 continents

Customers: Target, Wal-Mart…

The Ability to Design
Starting from Scratch

Service identification

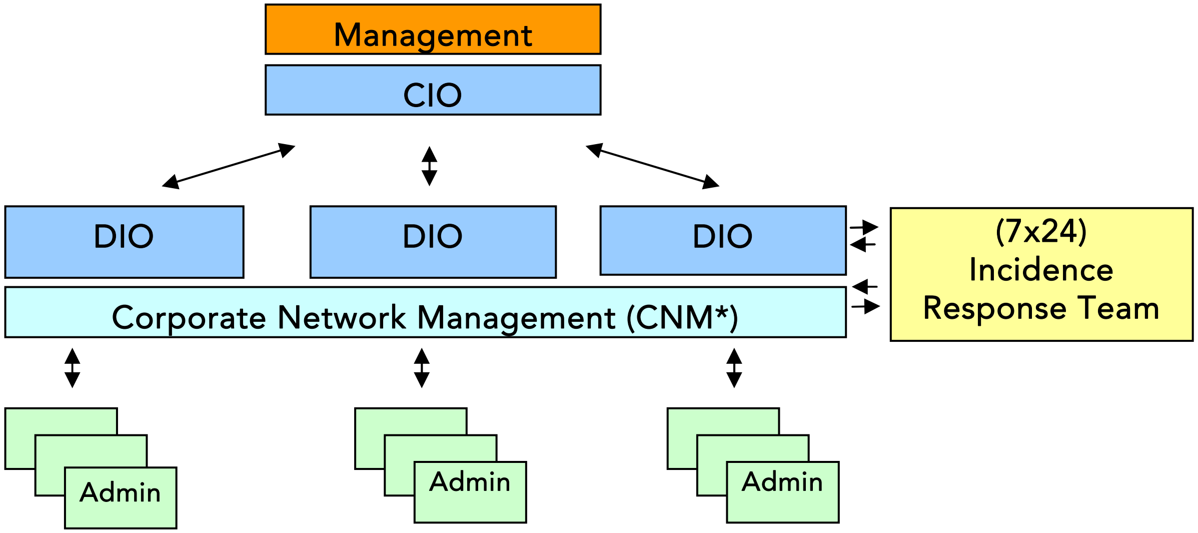
Service classification

Site classification (questionnaire, confirmed by management)

Design global network policy

Ensure management support

Enforce



DIO: Divisional Information Officer

The Ability to Design

Asset Identification - Service Classification

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

→ The Ability to Design

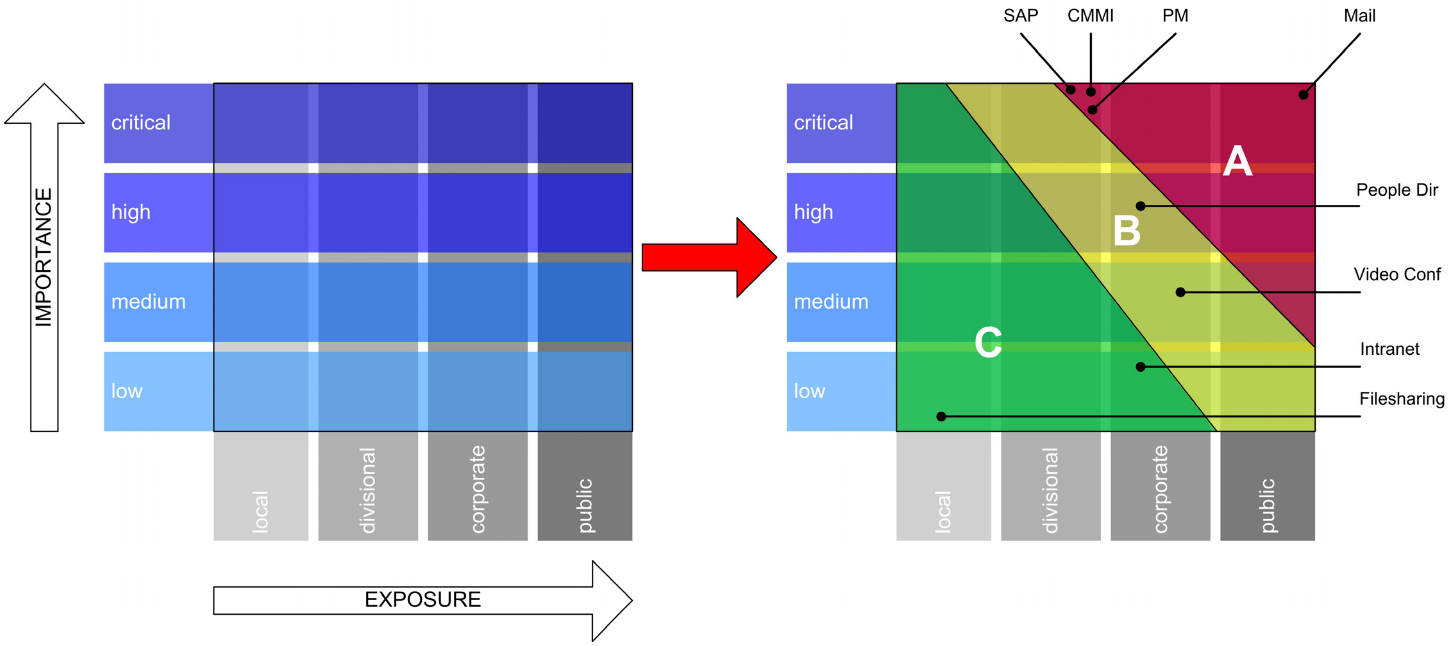
The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A



A **Examples:** *CMMI, PM, SAP, Email (*)*

B **Examples:** *Video Conference, People Directory(*)*

C **Examples:** *Intranet, local filesharing(*)*

The Ability to Design
Site Classification

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

→ The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

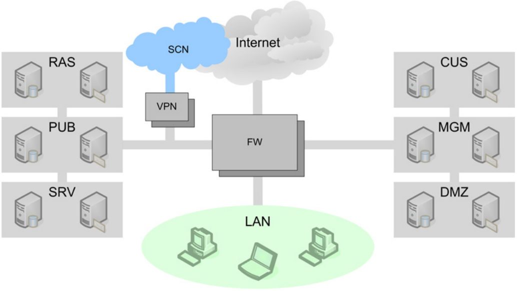
Closing the Gap

Q & A

Security Hub Site (SHS)

receives service classes A,B,C

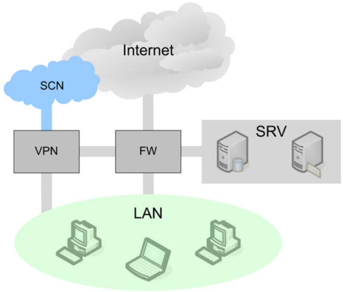
provides services classes A,B,C



Hosting Site (HS)

receives service classes A,B,C

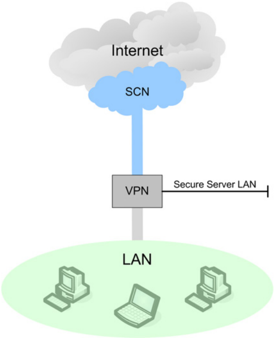
provides services classes B-C



Standard Site (SS)

receives service classes A,B,C

provides services classes none (SSL)



The Ability to Create

Going “all Green” – Enforcement Matrix

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

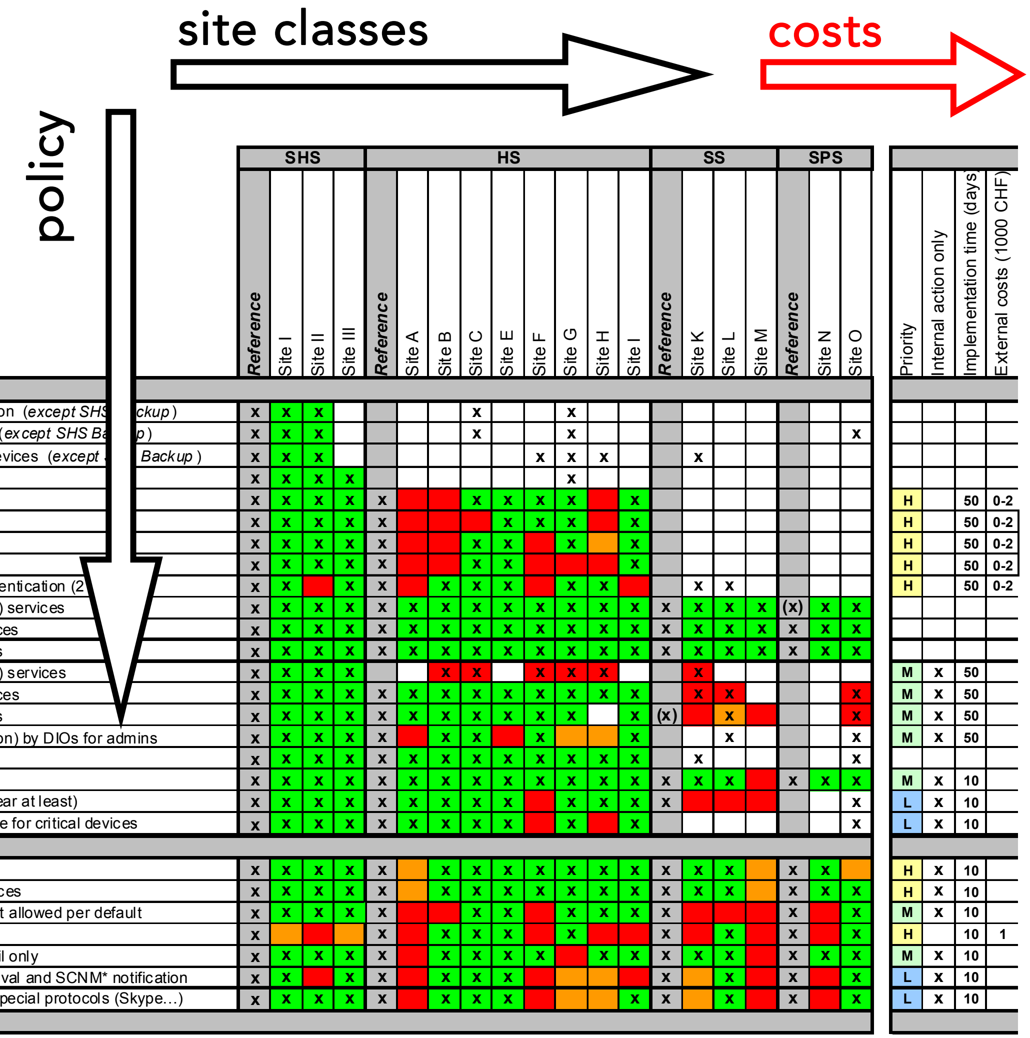
→ The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A



site classes

costs

policy

		SHS				HS									SS				SPS						
		Reference	Site I	Site II	Site III	*Reference*	Site A	Site B	Site C	Site E	Site F	Site G	Site H	Site I	*Reference*	Site K	Site L	Site M	*Reference*	Site N	Site O	Priority	Internal action only	Implementation time (days	External costs (1000 CHF)
Network Policy																									
5.1.5.1	Redundant and independent ISP connection (*except SHS* *ckup*)	x	🟩 x	🟩 x					x			x													
5.1.5.2	Redundant Firewall and SCN connectors (*except SHS Ba* *p*)	x	🟩 x	🟩 x					x			x									x				
5.1.5.3	Additional console connection of critical devices (*except* *Backup*)	x	🟩 x	🟩 x							x	x	x			x									
5.1.5.4	Requires Dedicated Management LAN	x	🟩 x	🟩 x	🟩 x							x													
5.1.5.5	Provides Remote Access DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x								H		50	0-2
5.1.5.6	Provides Public DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟥	🟩 x	🟩 x	🟩 x	🟥	🟩 x								H		50	0-2
5.1.5.7	Provides Service/Wan DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟩 x	🟩 x	🟥	🟩 x	🟧	🟩 x								H		50	0-2
5.1.5.8	Provides Customer DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟩 x	🟩 x	🟥	🟥	🟥	🟩 x								H		50	0-2
5.1.5.9	Administrative access through strong authentication (2	x	🟩 x	🟥	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟩 x	🟥		x	x					H		50	0-2
5.1.5.10	Site may receive class A (business critical) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	(x)	🟩 x	🟩 x				
5.1.5.11	Site may receive class B (important) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x				
5.1.5.12	Site may receive class C (normal) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x				
5.1.5.13	Site may provide class A (business critical) services	x	🟩 x	🟩 x	🟩 x			🟥 x	🟥 x		🟥 x	🟥 x	🟥 x			🟥 x						M	x	50	
5.1.5.14	Site may provide class B (important) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		🟥 x	🟥 x				🟥 x	M	x	50	
5.1.5.15	Site may provide class C (normal) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		🟩 x	(x)	🟥	🟧 x	🟥			🟥 x	M	x	50	
5.1.5.16	Proof of competence (Experience/Education) by DIOs for admins	x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟥	🟩 x	🟧	🟧	🟩 x			x				x	M	x	50	
5.1.5.17	Administrator Deputy/Backup required	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		x					x				
5.1.5.18	Detailed documentation and topology	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x	M	x	10	
5.1.5.19	Frequent documentation review (once a year at least)	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟥			x	L	x	10	
5.1.5.20	Defined emergency replacement procedure for critical devices	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥	🟩 x							x	L	x	10	
Firewall Policy																									
5.1.5.21	“Default Deny” approach for Firewall	x	🟩 x	🟩 x	🟩 x	x	🟧	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟧	x	🟩 x	🟧	H	x	10	
5.1.5.22	Incoming: Only ports open of offered services	x	🟩 x	🟩 x	🟩 x	x	🟧	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟧	x	🟩 x	🟩 x	H	x	10	
5.1.5.23	Outgoing: No direct connections to Internet allowed per default	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟩 x	🟩 x	🟥	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟥	x	🟥	🟩 x	M	x	10	
5.1.5.24	Outgoing: Web traffic via proxy only	x	🟧	🟥	🟧	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥	🟥	x	🟥	🟩 x	🟥	x	🟥	🟩 x	H		10	1
5.1.5.25	Outgoing: Mail via Swisslog Corporate mail only	x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟩 x	x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x	M	x	10	
5.1.5.26	Direct Internet connection need DIO approval and SCNM* notification	x	🟩 x	🟥	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟧	🟥	x	🟧	🟩 x	🟥	x	🟥	🟩 x	L	x	10	
5.1.5.27	DIO approval and SCNM* notification for special protocols (Skype…)	x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟧	🟩 x	x	🟧	🟩 x	🟥	x	🟥	🟩 x	L	x	10	
Monitoring, Reporting Policy																									

The Ability to Create

Going "all Green" – Enforcement Matrix

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

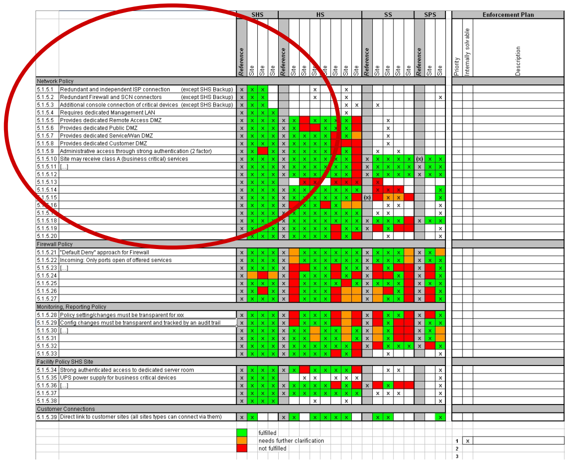
→ The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A



		SHS				HS								SS					SPS			Enforcement Plan		
		Reference	Site	Site	Site	*Reference*	Site	Site	Site	Site	Site	Site	Site	*Reference*	Site	Site	Site	Site	*Reference*	Site	Site	Priority	Internally solvable	Description
Network Policy																								
5.1.5.1	Redundant and independent ISP connection (except SHS Backup)	x	🟩 x	🟩 x					x			x												
5.1.5.2	Redundant Firewall and SCN connectors (except SHS Backup)	x	🟩 x	🟩 x					x			x									x			
5.1.5.3	Additional console connection of critical devices (except SHS Backup)	x	🟩 x	🟩 x								x	x		x									
5.1.5.4	Requires dedicated Management LAN	x	🟩 x	🟩 x	🟩 x							x												
5.1.5.5	Provides dedicated Remote Access DMZ	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟥	🟩 x	🟩 x	🟩 x	🟩 x	🟥			x								
5.1.5.6	Provides dedicated Public DMZ	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟥	🟥	🟩 x	🟩 x	🟩 x	🟥			x								
5.1.5.7	Provides dedicated Service/Wan DMZ	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟧			x								
5.1.5.8	Provides dedicated Customer DMZ	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟥	🟥			x								
5.1.5.9	Administrative access through strong authentication (2 factor)	x	🟩 x	🟥	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥		x		x							
5.1.5.10	Site may receive class A (business critical) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x	🟩 x	🟩 x	(x)	🟩 x	🟩 x			
5.1.5.11	[...]	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x			
5.1.5.12		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x			
5.1.5.13		x	🟩 x	🟩 x	🟩 x			🟥 x	🟥 x		🟥 x	🟥 x	🟥 x		🟥 x									
5.1.5.14		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		🟥 x	🟥 x	🟥 x				🟩 x			
5.1.5.15		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	(x)	🟥	🟧 x	🟧 x	🟥			🟩 x			
5.1.5.16		x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟥	🟩 x	🟧	🟧			x	x				x			
5.1.5.17		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		x	x					x			
5.1.5.18		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x			
5.1.5.19		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟩 x	x	🟥	🟩 x	🟥	🟥			x			
5.1.5.20		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥			x					x			
Firewall Policy																								
5.1.5.21	"Default Deny" approach for Firewall	x	🟩 x	🟩 x	🟩 x	x	🟧	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟧	x	🟩 x	🟧			
5.1.5.22	Incoming: Only ports open of offered services	x	🟩 x	🟩 x	🟩 x	x	🟧	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟧	x	🟩 x	🟩 x			
5.1.5.23	[...]	x	🟩 x	🟩 x	🟩 x	x	🟥	🟥	🟩 x	🟩 x	🟥	🟩 x	🟩 x	x	🟥	🟩 x	🟥	🟥	x	🟥	🟩 x			
5.1.5.24		x	🟧	🟥	🟧	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥	x	🟥	🟥	🟩 x	🟥	x	🟥	🟩 x			
5.1.5.25		x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	x	🟩 x	🟩 x	🟩 x	🟥	x	🟩 x	🟩 x			
5.1.5.26		x	🟩 x	🟥	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟧	x	🟧	🟥	🟩 x	🟥	x	🟥	🟩 x			
5.1.5.27		x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟧	x	🟧	🟩 x	🟩 x	🟥	x	🟥	🟩 x			
Monitoring, Reporting Policy																								
5.1.5.28	Policy setting/changes must be transparent for xxx	x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟥	x	🟥	🟩 x	🟩 x	🟥	x	🟥	🟩 x			
5.1.5.29	Config changes must be transparent and tracked by an audit trail	x	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x	🟩 x	🟩 x	🟥	🟧	🟥	x	🟥	🟩 x	🟥	🟥	x	🟩 x	🟩 x			
5.1.5.30	[...]	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟧	🟩 x	🟩 x	🟧	🟩 x	x	🟧	🟩 x	🟥	🟥	x	🟩 x	🟧			
5.1.5.31		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟧	🟩 x	🟩 x	🟧	🟩 x	x	🟧	🟩 x	🟥	🟥	x	🟩 x	🟧			
5.1.5.32		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	x	🟥	🟩 x	🟩 x	🟩 x	x	🟥	🟩 x			
5.1.5.33		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥			x					x			
Facility Policy SHS Site																								
5.1.5.34	Strong authenticated access to dedicated server room	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟥	🟩 x	🟩 x	🟩 x	🟩 x	🟥			x	x				x			
5.1.5.35	UPS power supply for business critical devices	x	🟩 x	🟩 x	🟩 x			x	x		x	x	x								x			
5.1.5.36	[...]	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟥	🟩 x	🟥	x	🟥	🟩 x	🟥	🟥			x			
5.1.5.37		x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x		x	x	x				x			
5.1.5.38		x	🟩 x	🟩 x	🟩 x				x			x									x			
Customer Connections																								
5.1.5.39	Direct link to customer sites (all sites types can connect via them)	x	🟩 x			x	🟩 x		🟩 x	🟩 x	🟩 x	🟩 x			🟩 x	🟩 x					🟩 x			

🟩 fulfilled

🟧 needs further clarification

🟥 not fulfilled

1	x
2	
3	

		SHS				HS									SS				SPS		
		Reference	Site I	Site II	Site III	***Reference***	Site A	Site B	Site C	Site E	Site F	Site G	Site H	Site I	***Reference***	Site K	Site L	Site M	***Reference***	Site N	Site O
Network Policy																					
5.1.5.1	Redundant and independent ISP connection (*except SHS Backup*)	x	🟩 x	🟩 x																	
5.1.5.2	Redundant Firewall and SCN connectors (*except SHS Backup*)	x	🟩 x	🟩 x																	
5.1.5.3	Additional console connection of critical devices (*except SHS Backup*)	x	🟩 x	🟩 x																	
5.1.5.4	Requires Dedicated Management LAN	x	🟩 x	🟩 x	🟩 x																
5.1.5.5	Provides Remote Access DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x							
5.1.5.6	Provides Public DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x							
5.1.5.7	Provides Service/Wan DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x							
5.1.5.8	Provides Customer DMZ *	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x							
5.1.5.9	Administrative access through strong authentication (2 factor)	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x							
5.1.5.10	Site may receive class A (business critical) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	(x)	🟩 x	🟩 x
5.1.5.11	Site may receive class B (important) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x
5.1.5.12	Site may receive class C (normal) services	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x	🟩 x	x	🟩 x	🟩 x

The Ability to Manage & Execute

Keep it “all Green” - This Includes …

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

→ The Ability to Manage & Execute

Mission Control

Closing the Gap

Q & A

Seamless integration of new acquisitions

Guaranteeing availability of logistic management

Outgoing content enforcement …

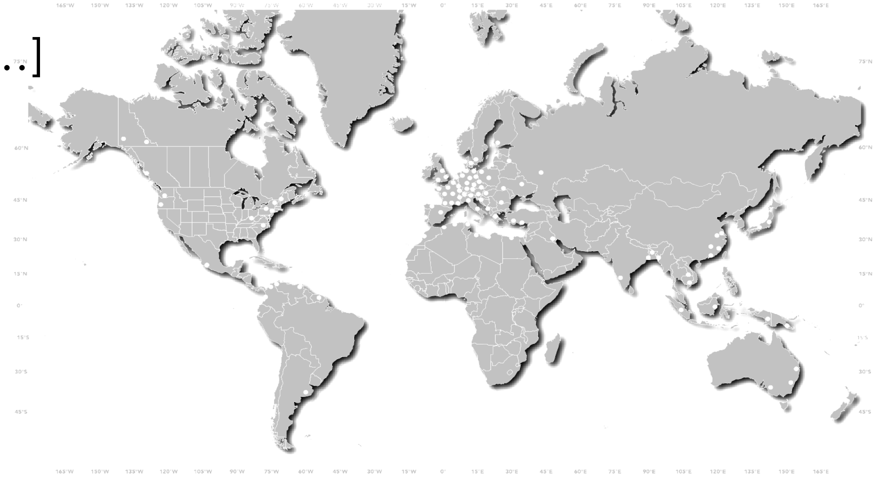
The danger of getting blacklisted …

Worm / Viruses - Conficker E, F, G …

Bandwidth traps (rich media)

Partner connections

[…]



Mission Control – A glance behind the Curtain

The Matrix Approach for All …

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

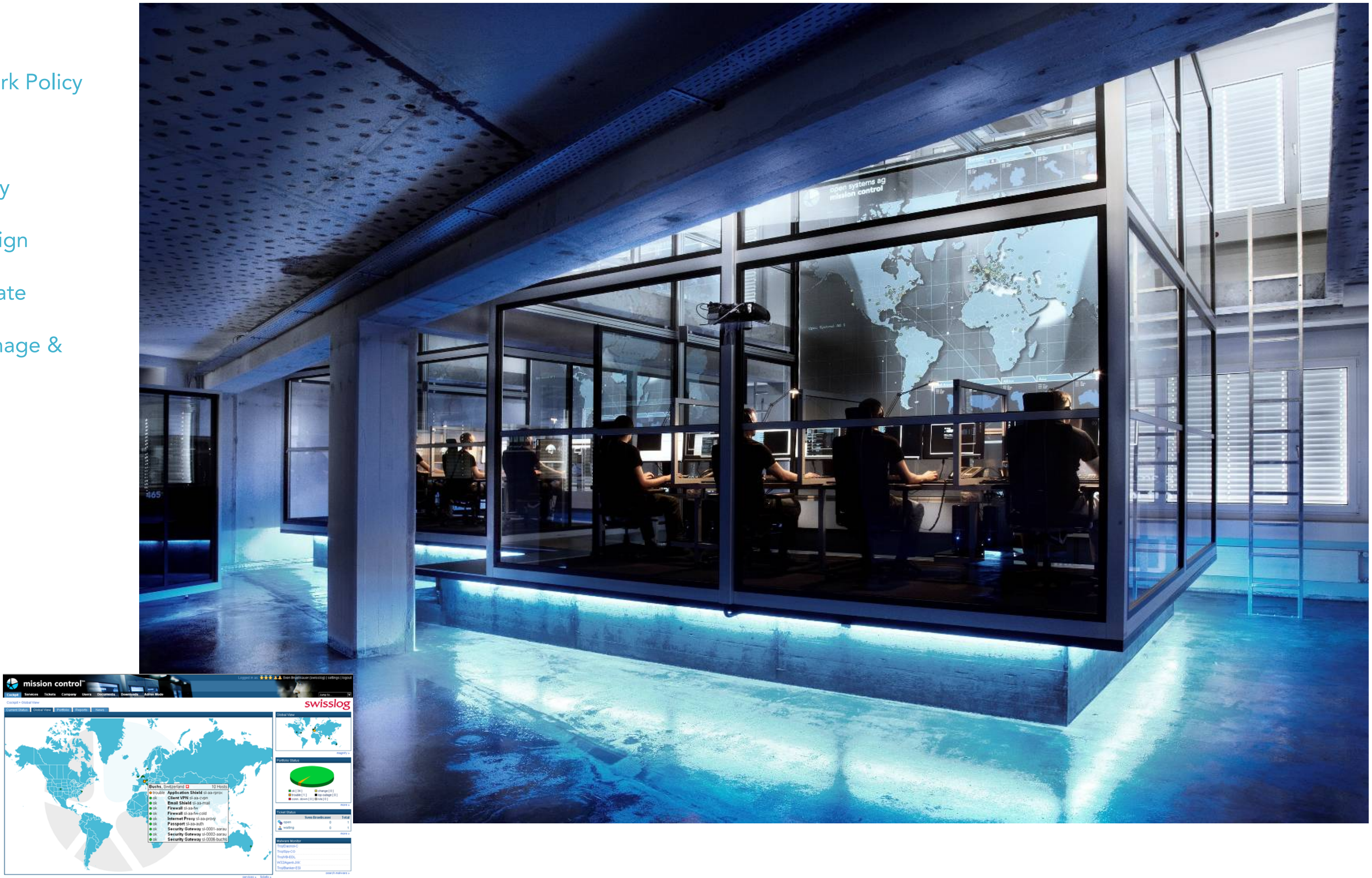
The Ability to Create

The Ability to Manage & Execute

→ Mission Control

Closing the Gap

Q & A



Logged in as: Sven Bruelisauer (swisslog) | settings | logout

Cockpit > Global View

Buchs, Switzerland 10 Hosts

```
trouble  Application Shield sl-aa-rprox
ok       Client VPN sl-aa-cvpn
ok       Email Shield sl-aa-mail
ok       Firewall sl-aa-fw
ok       Firewall sl-aa-fw-cold
ok       Internet Proxy sl-aa-proxy
ok       Passport sl-aa-auth
ok       Security Gateway sl-0001-aarau
ok       Security Gateway sl-0002-aarau
ok       Security Gateway sl-0008-buchs
```

ok [34]　change [0]　trouble [1]　isp outage [0]　conn. down [0]　n/a [0]

	Sven Bruelisauer	Total
open	0	1
waiting	0	1

Troj/Daonol-C
Troj/Spy-CO
Troj/VB-EDL
W32/Agent-JXK
Troj/Banker-ESI

mission control™
security services
by open systems ag
www.open.ch

Mission Control

Built-in Process – 4-Eye Principle

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

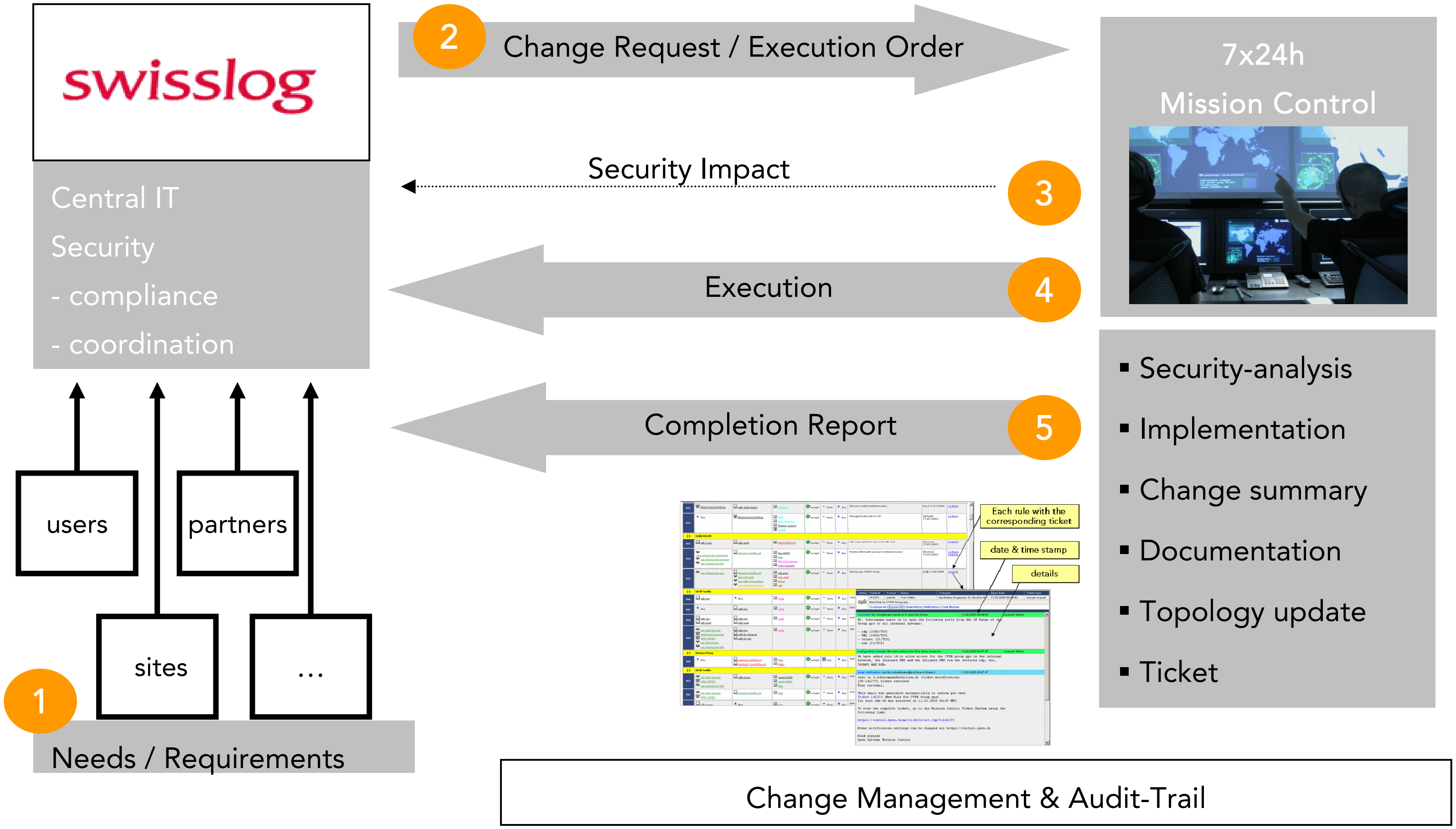
The Ability to Create

The Ability to Manage & Execute

→ Mission Control

Closing the Gap

Q & A



- Security-analysis
- Implementation
- Change summary
- Documentation
- Topology update
- Ticket

Mission Control

Built-in Process

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

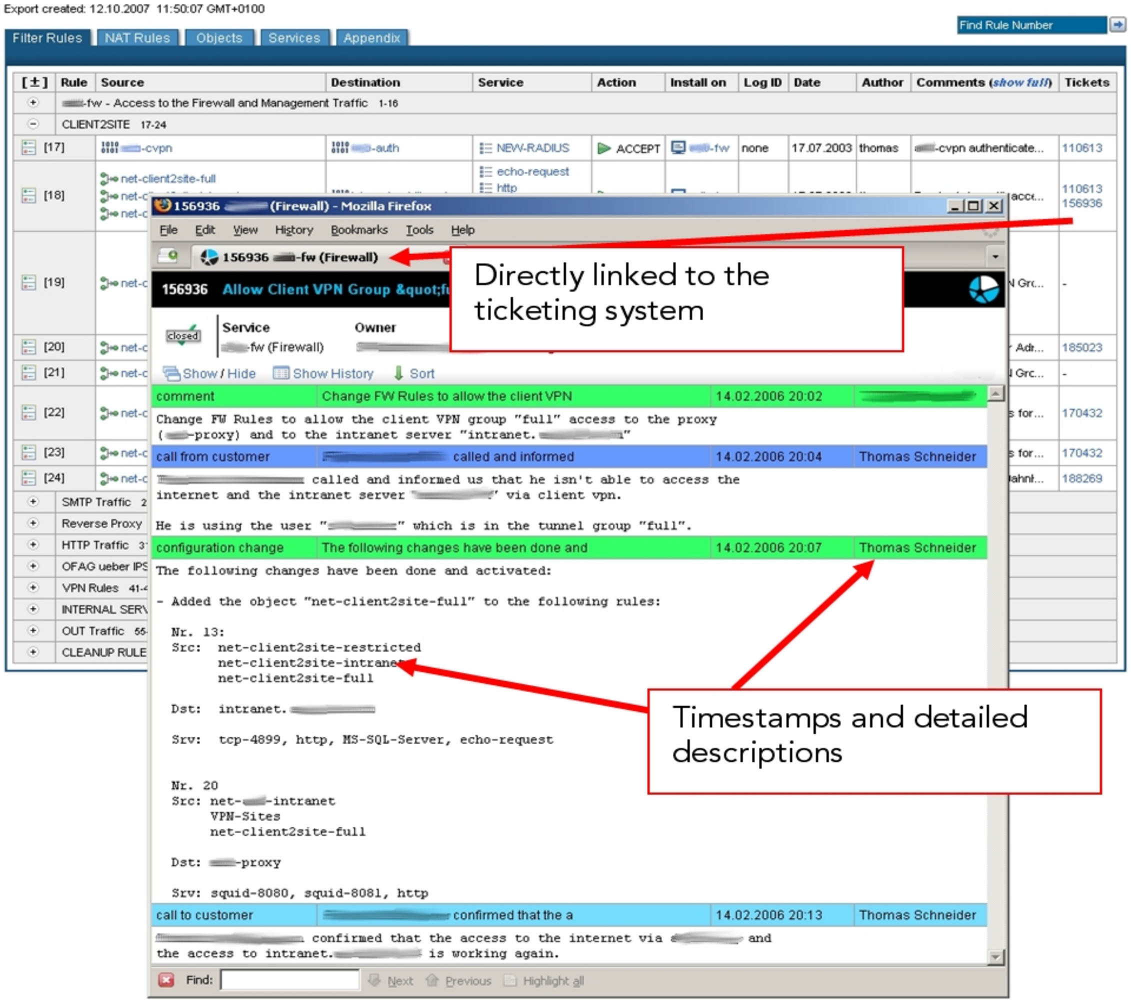
The Ability to Create

The Ability to Manage & Execute

→ Mission Control

Closing the Gap

Q & A



Export created: 12.10.2007 11:50:07 GMT+0100

[±]	Rule	Source	Destination	Service	Action	Install on	Log ID	Date	Author	Comments (show full)	Tickets
+	[redacted]-fw - Access to the Firewall and Management Traffic 1-16										
−	CLIENT2SITE 17-24										
	[17]	[redacted]-cvpn	[redacted]-auth	NEW-RADIUS	ACCEPT	[redacted]-fw	none	17.07.2003	thomas	[redacted]-cvpn authenticate...	110613
	[18]	net-client2site-full net-c net-c		echo-request http						acc...	110613 156936
	[19]	net-c								N Grc...	-
	[20]	net-c								r Adr...	185023
	[21]	net-c								l Grc...	-
	[22]	net-c								s for...	170432
	[23]	net-c								s for...	170432
	[24]	net-c								lahnl...	188269
+	SMTP Traffic 2										
+	Reverse Proxy										
+	HTTP Traffic 3										
+	OFAG ueber IPS										
+	VPN Rules 41-										
+	INTERNAL SERV										
+	OUT Traffic 55-										
+	CLEANUP RULE										

156936 [redacted] (Firewall) - Mozilla Firefox

156936 [redacted]-fw (Firewall)

156936 Allow Client VPN Group &quot;fu

closed

Service: [redacted]-fw (Firewall)

Owner: [redacted]

comment | Change FW Rules to allow the client VPN | 14.02.2006 20:02 | [redacted]

```
Change FW Rules to allow the client VPN group "full" access to the proxy
([redacted]-proxy) and to the intranet server "intranet.[redacted]"
```

call from customer | [redacted] called and informed | 14.02.2006 20:04 | Thomas Schneider

```
[redacted] called and informed us that he isn't able to access the
internet and the intranet server "[redacted]" via client vpn.

He is using the user "[redacted]" which is in the tunnel group "full".
```

configuration change | The following changes have been done and | 14.02.2006 20:07 | Thomas Schneider

```
The following changes have been done and activated:

- Added the object "net-client2site-full" to the following rules:

  Nr. 13:
  Src:  net-client2site-restricted
        net-client2site-intranet
        net-client2site-full

  Dst:  intranet.[redacted]

  Srv:  tcp-4899, http, MS-SQL-Server, echo-request


  Nr. 20
  Src: net-[redacted]-intranet
       VPN-Sites
       net-client2site-full

  Dst: [redacted]-proxy

  Srv: squid-8080, squid-8081, http
```

call to customer | [redacted] confirmed that the a | 14.02.2006 20:13 | Thomas Schneider

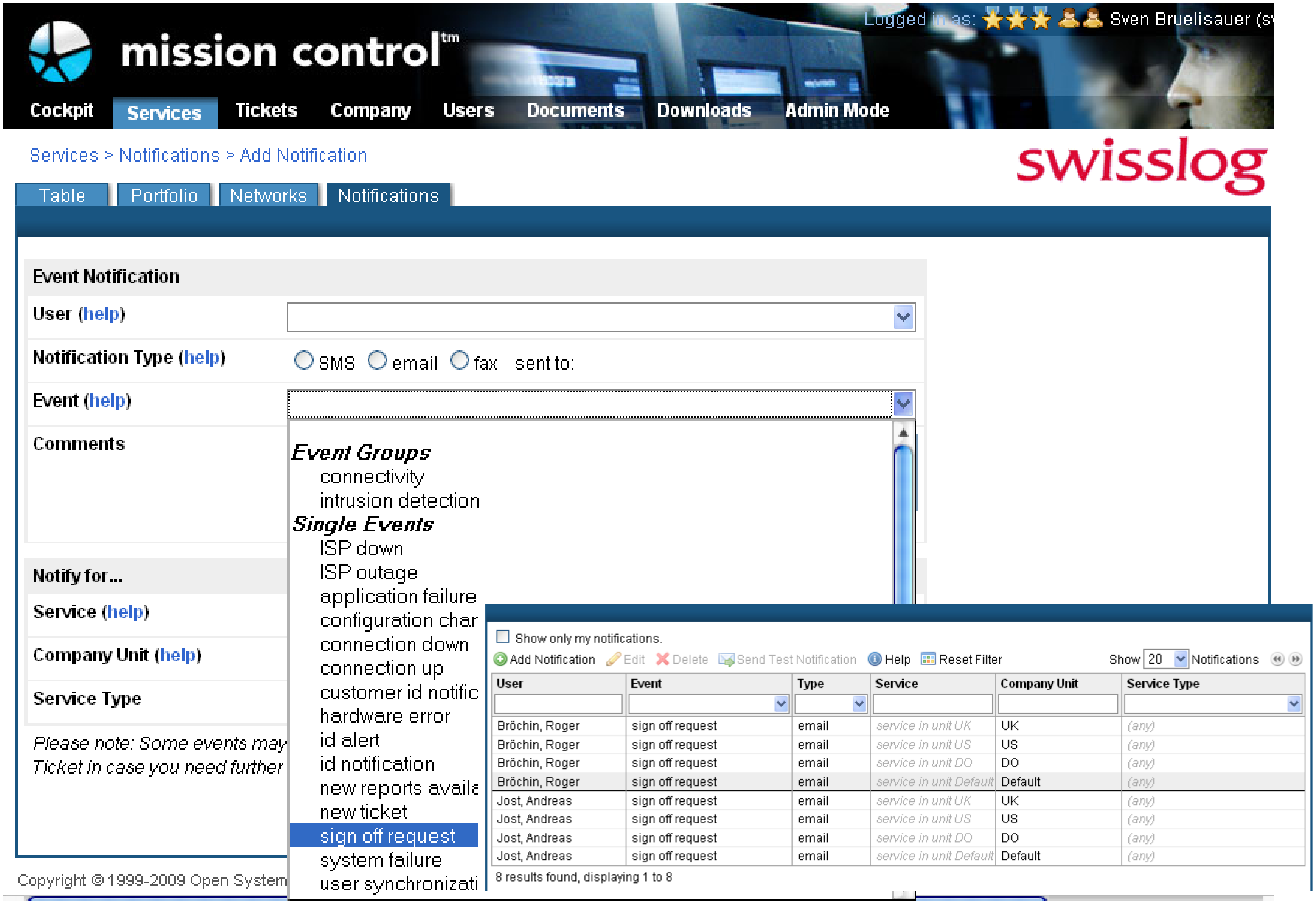
```
[redacted] confirmed that the access to the internet via [redacted] and
the access to intranet.[redacted] is working again.
```

Directly linked to the ticketing system

Timestamps and detailed descriptions

Mission Control

Built-in Process



Services > Notifications > Add Notification

Event Notification

User (help)	
Notification Type (help)	○ SMS ○ email ○ fax sent to:
Event (help)	
Comments	

Event Groups
connectivity
intrusion detection
Single Events
ISP down
ISP outage
application failure
configuration char
connection down
connection up
customer id notific
hardware error
id alert
id notification
new reports availa
new ticket
sign off request
system failure
user synchronizati

Notify for...

Service (help)	
Company Unit (help)	
Service Type	

Please note: Some events may
Ticket in case you need further

Copyright © 1999-2009 Open System

□ Show only my notifications.

Add Notification Edit Delete Send Test Notification Help Reset Filter Show 20 Notifications

User	Event	Type	Service	Company Unit	Service Type
Bröchin, Roger	sign off request	email	*service in unit UK*	UK	*(any)*
Bröchin, Roger	sign off request	email	*service in unit US*	US	*(any)*
Bröchin, Roger	sign off request	email	*service in unit DO*	DO	*(any)*
Bröchin, Roger	sign off request	email	*service in unit Default*	Default	*(any)*
Jost, Andreas	sign off request	email	*service in unit UK*	UK	*(any)*
Jost, Andreas	sign off request	email	*service in unit US*	US	*(any)*
Jost, Andreas	sign off request	email	*service in unit DO*	DO	*(any)*
Jost, Andreas	sign off request	email	*service in unit Default*	Default	*(any)*

8 results found, displaying 1 to 8

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

→ Mission Control

Closing the Gap

Q & A

Mission Control

Full Involvement

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

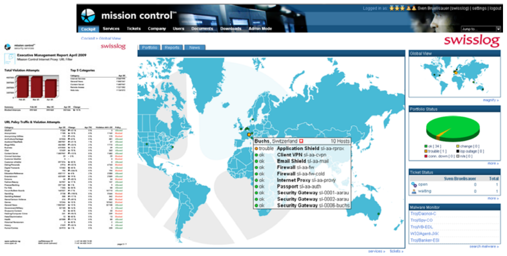
→ Mission Control

Closing the Gap

Q & A

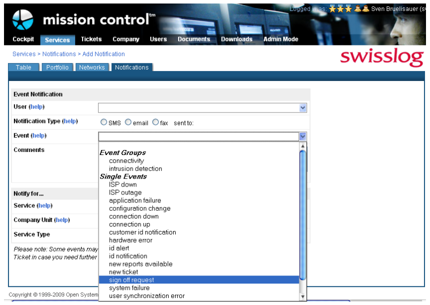
Management / CIO

- Receive executive reports, ROIs
- See global IT-perimeter status, 7x24



IT Security / Security Officer

- Receive automatic change report
- Notifications on sign-off requirement



Services > Notifications > Add Notification

Event Notification

User (help)

Notification Type (help) ○ SMS ○ email ○ fax sent to:

Event (help)

Comments

Event Groups
connectivity
intrusion detection
Single Events
ISP down
ISP outage
application failure
configuration change
connection down
connection up
customer id notification
hardware error
id alert
id notification
new reports available
new ticket
sign off request
system failure
user synchronization error

Notify for...

Service (help)

Company Unit (help)

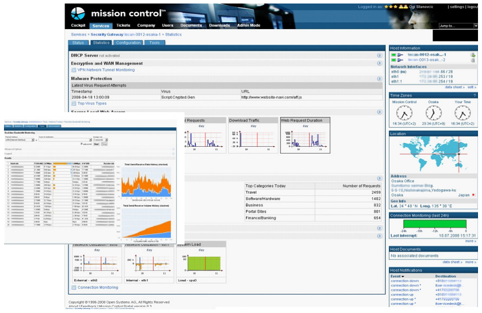
Service Type

Please note: Some events may
Ticket in case you need further

Copyright © 1999-2009 Open System

IT Operations / Administrator, Regional IT

- Get all security, availability information and technical details in real-time
- Change requests via sign-off-process



All have the **same information source** (cockpit) with appropriate levels of information based on their clearance

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

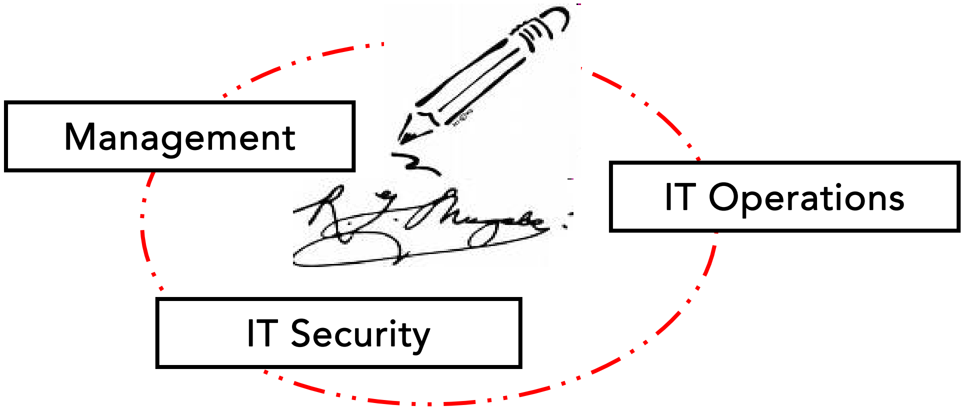
Mission Control

→ Closing the Gap

Q & A

Closing the Gap

Key Factors



Management

IT Operations

IT Security

CLARITY	Clear goals, interfaces and steps shared by all in charge
VISIBILITY	Ability to verify policy and status any time globally
INVOLVEMENT	Full involvement, same source of information for all
ENFORCEMENT	Built-in process

… avoids pitfalls & closes the gap

Q & A

Agenda

Purpose of Network Policy

How & Who

Pitfalls from Reality

The Ability to Design

The Ability to Create

The Ability to Manage & Execute

Mission Control

Closing the Gap

→ Q & A