ISSeG

Integrated Site Security for Grids

EU-FP6 Project 026745

ISSeG/EGEE SA1:Site Security Training

David Jackson, STFC

Monday 1 Oct, 16:00 – 17:30
& Thursday 4 Oct, 14:00 – 16:00

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Welcome

- **Welcome!**
- **Protect, detect & respond**
- **Risk assessments**
- **Recommendations**

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Welcome

- **We are continually improving the slides and training materials and would like your feedback:**
  - Feedback form
  - Attendance form
  - Questions

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

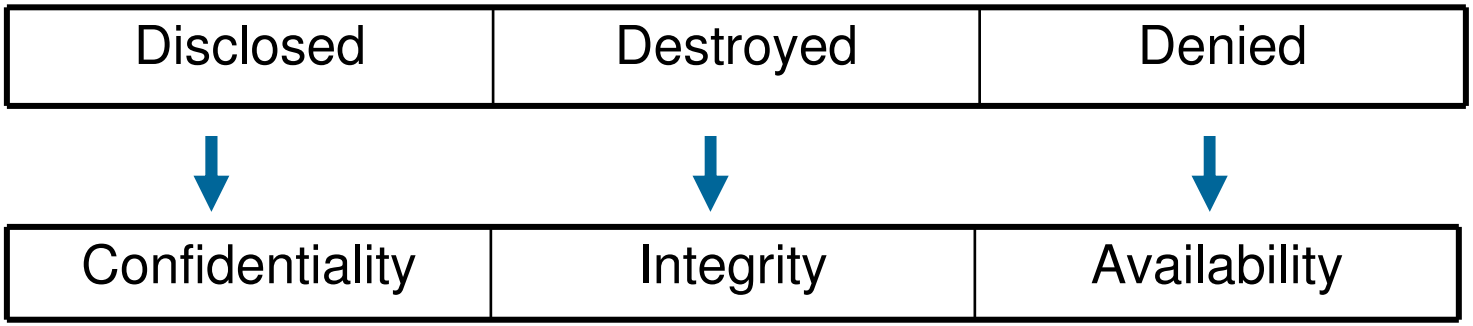
Protect, detect & respond

1. ISS – A very short introduction
2. Three types of site attack
3. Your role during an incident

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

- **Information Security** (Grid and IT world)

  In practice, this is the embodiment of a number of disparate measures (generally technical) that act to prevent information from being:

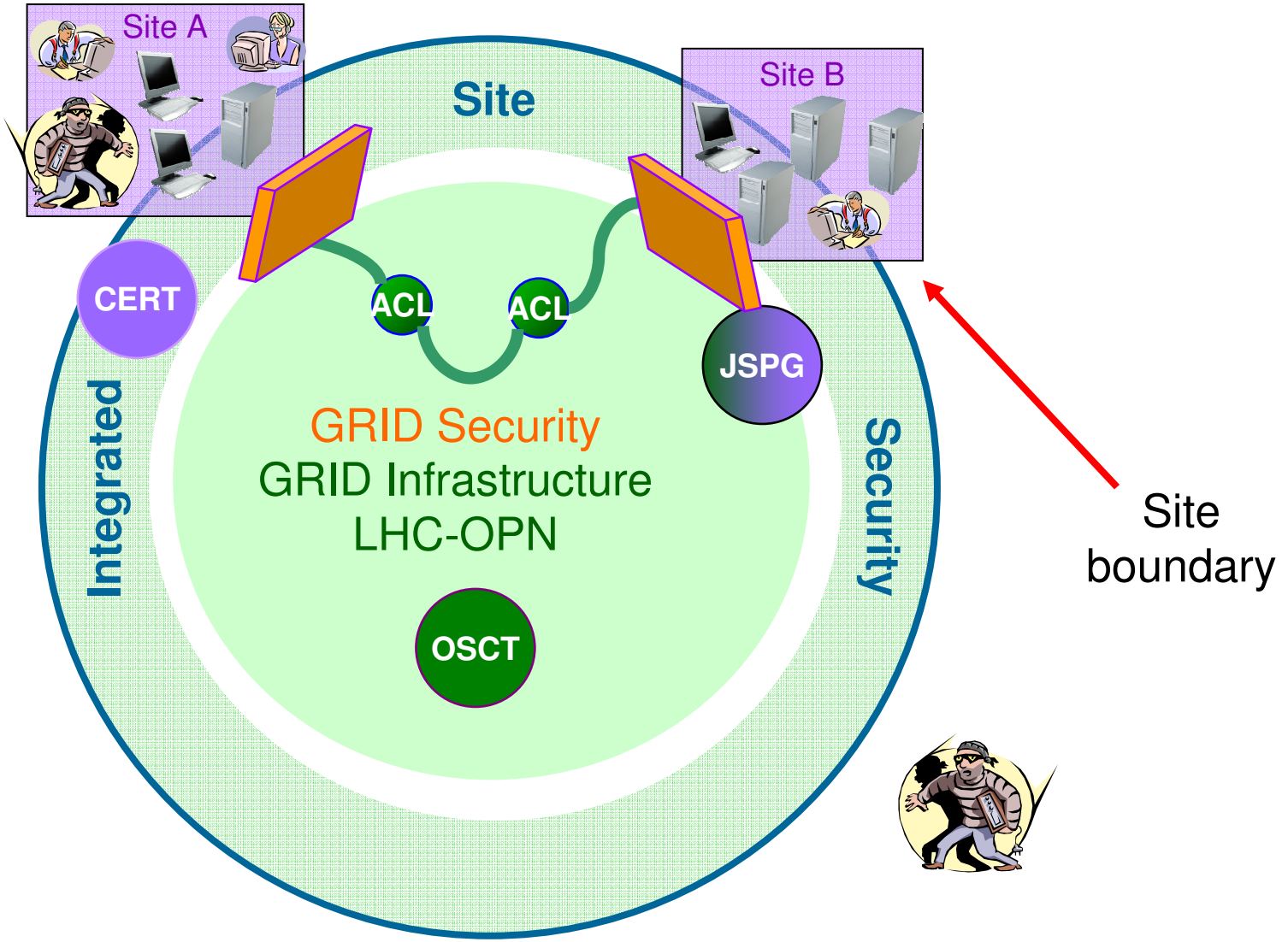


  Any good security system must include non-technical aspects such as **training, policies, procedures** etc**.** Security is:

  - a cultural issue and not just a technical issue
  - protecting against danger and loss

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

ISS - Site



Integrated
Site
Security for
Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

ISS - Integrated

- **Integrated Site Security (ISS)**

  ISS is the concept of integrating the technical, administrative and educational aspects of information security at your site so that they work together to improve your overall site security.

  While this is not specific to Grid environments, it is extremely relevant to all Grid sites as we all work together.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

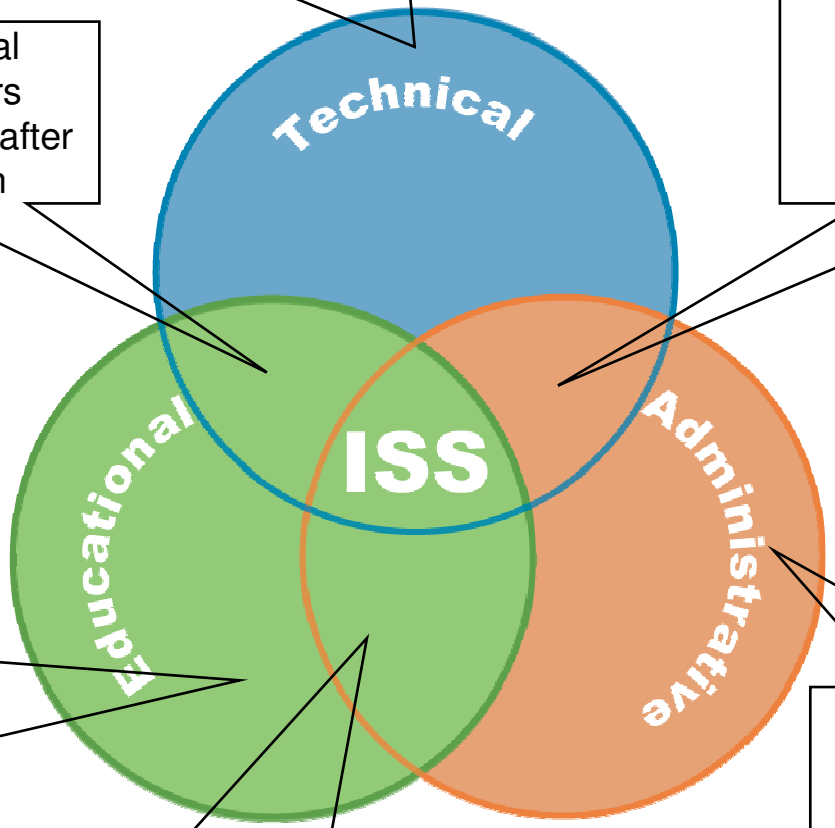
ISS - Integrated Site Security

Example

Use security mechanisms and tools to manage the installation and update of anti-virus products

Explain technical changes to users before, during and after implementation

Know who is using your network



Create and maintain training and awareness campaigns for security polices and best practice.

Follow incident response procedures when viruses found

Policy: Require all PC to run a valid anti-virus product

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Protect, detect & respond

- **What can you do?**
  - Protect
  - Detect
  - Respond

  → Against security incidents/events

Integrated Site Security for Grids

www.isseg.eu

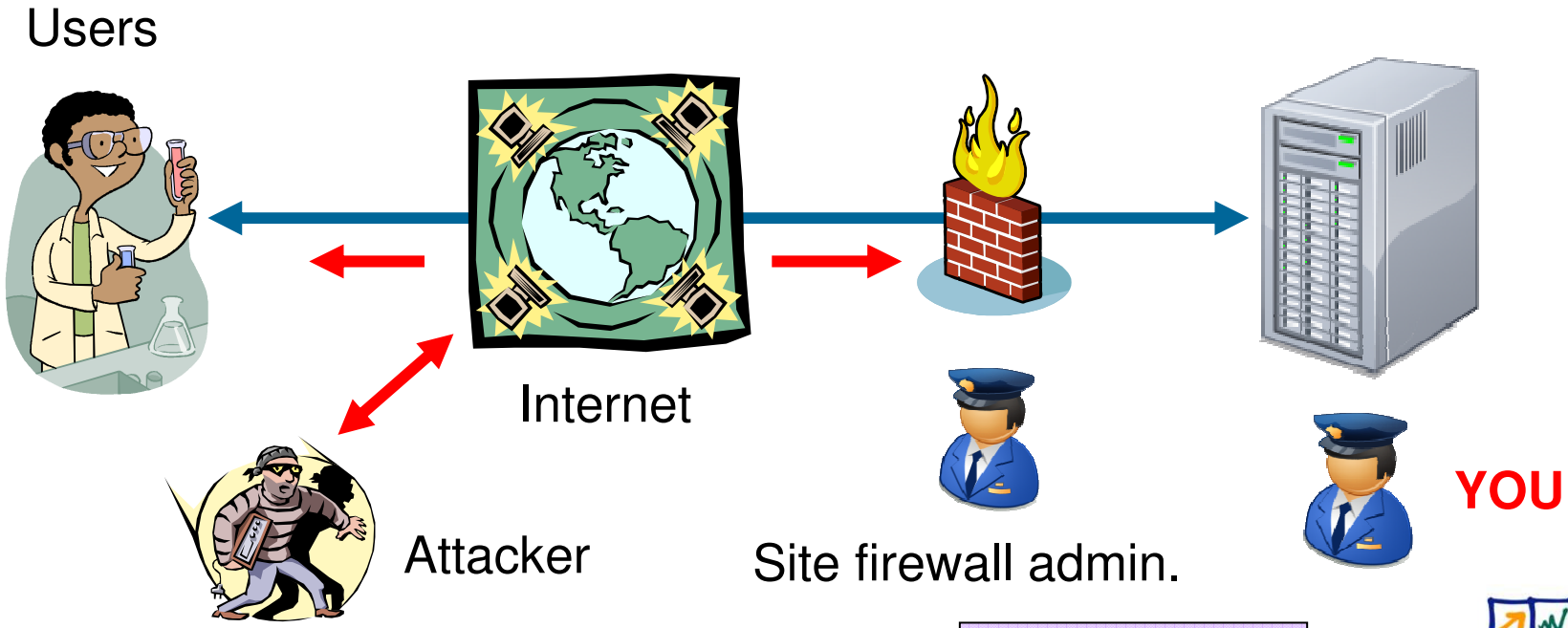
© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- **My site does not get attacked!**

  Sites provide resources to Grid for Science.
  Do they really get attacked?



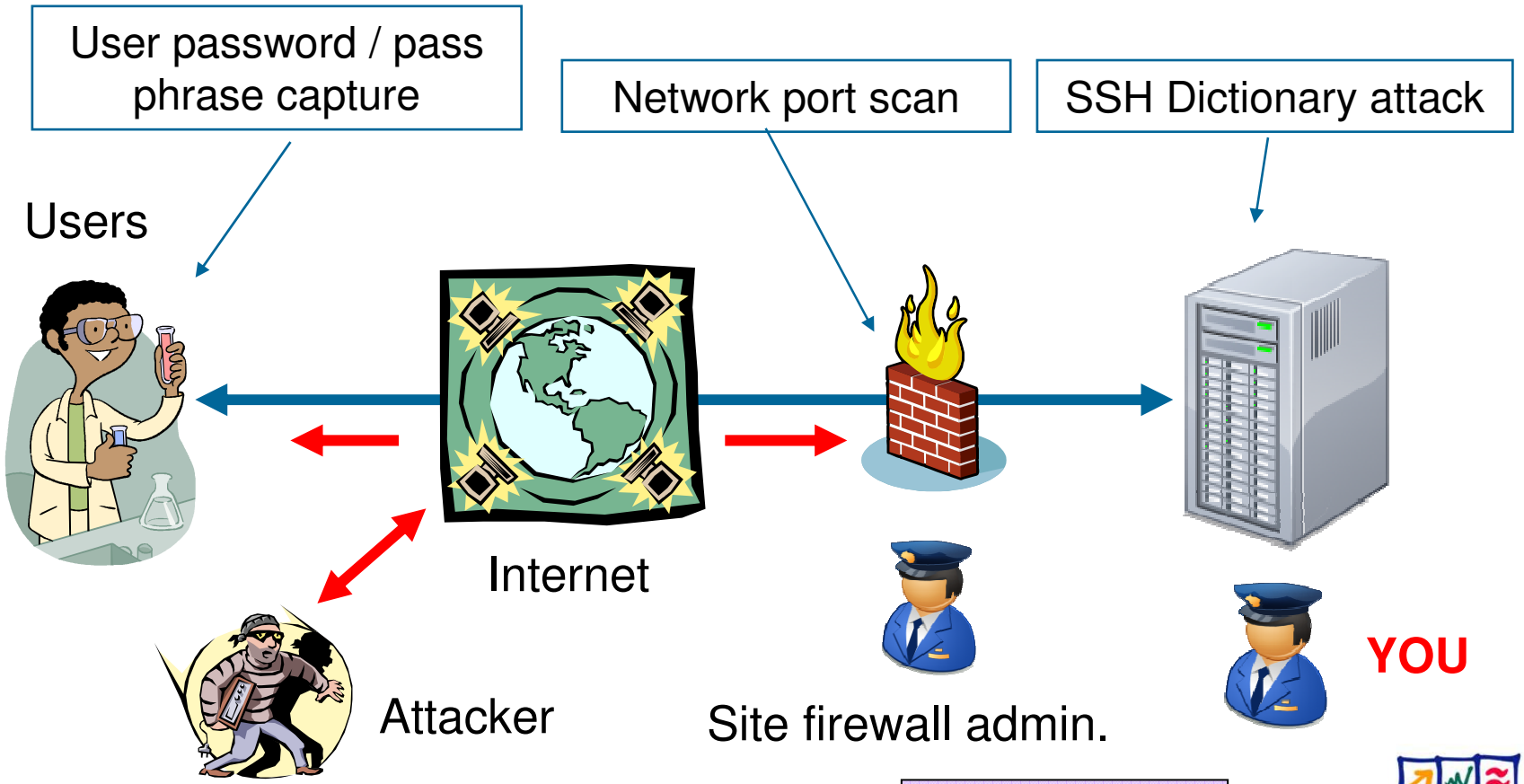
Integrated Site Security for Grids
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu
Information Society and Media

Protect, detect & respond

- **My site does not get attacked! –** Yes it does!



Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

Protect, detect & respond

- **User password/pass phrases can get sniffed**

  In a recent multi-site incident where no harm was done, valid account details were used by an unauthorised person to connect to a number of machines at over 20 sites.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Protect, detect & respond

Source	Destination	Destination Port
src=65.105.x.x	dst=130.246.192.11	dst_port=2967
src=65.105.x.x	dst=130.246.192.11	dst_port=2967
src=65.105.x.x	dst=130.246.192.110	dst_port=2967
src=65.105.x.x	dst=130.[illegible].192.111	[illegible]t_port=2967
src=65.10[illegible]	[illegible]	[illegible]t_port=2967
src=65.10[illegible]	[illegible]	[illegible]t_port=2967
src=65.10[illegible]	[illegible].192.114	dst_port=2967
src=65.105.x.x	dst=130.246.192.115	dst_port=2967
src=65.105.x.x	dst=130.246.192.116	dst_port=2967
src=65.105.x.x	dst=130.246.192.117	dst_port=2967
src=65.105.x.x	dst=130.246.192.118	dst_port=2967
src=65.105.x.x	dst=130.246.192.119	dst_port=2967

Blocked

Source	Destination	Destination port
src=60.168.89.228	dst=130.246.192.110	dst_port=2967
src=121.12.178.173	dst=130.246.192.110	dst_port=1434
src=91.98.89.33	dst=130.246.192.110	[illegible]t_port=1433
src=91.98.89.33	dst=130[illegible]	[illegible]t_port=1433
src=65.10[illegible]	[illegible]	[illegible]t_port=2967
src=65.10[illegible]	[illegible]	dst_port=2967
src=202.[illegible]	dst=130.246.192.110	dst_port=1434
src=121.102.9.148	dst=130.246.192.110	dst_port=445
src=121.102.9.148	dst=130.246.192.110	dst_port=445
src=61.153.194.138	dst=130.246.192.110	dst_port=1434
src=85.248.121.12	dst=130.246.192.110	dst_port=52540

Blocked

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

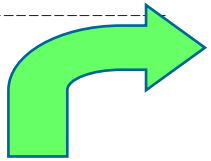
http://www.isseg.eu

Information Society and Media

Protect, detect & respond

```
-------------------- pam_unix Begin ----------------
sshd:
   Invalid Users:
      Unknown Account: 118 Time(s)
   Authentication Failures:
   rpm (125.63.75.131 ): 1 Time(s)
   apache (125.63.75.131 ): 1 Time(s)
   news (125.63.75.131 ):
   operator (125.63.75.131
   sshd (125.63.75.131 ):
   games (125.63.75.131 ):
   mail (125.63.75.131 ): 1 Time(s)
   ftp (125.63.75.131 ): 1 Time(s)
   nobody (125.63.75.131 ): 1 Time(s)

------------------ pam_unix End -----------------------
```



Extract of Failed logins from these:

Aaliyah/password	**aron**/password
Aba/password	**Abel**/password
Exit/password	**Ionut**/password
Jewel/pa word	**Zmeu**/password
ad m word	**add**/password
ord from	**admin**/password
ssword	**adrian**/password
word	**alex**/password
alina/password	**amanda**/password
andrei/password	**angel**/password
apache/password	**aron**/password
backup/password	….. (other 94 not shown)

Integrated Site Security for Grids

www.isseg.eu

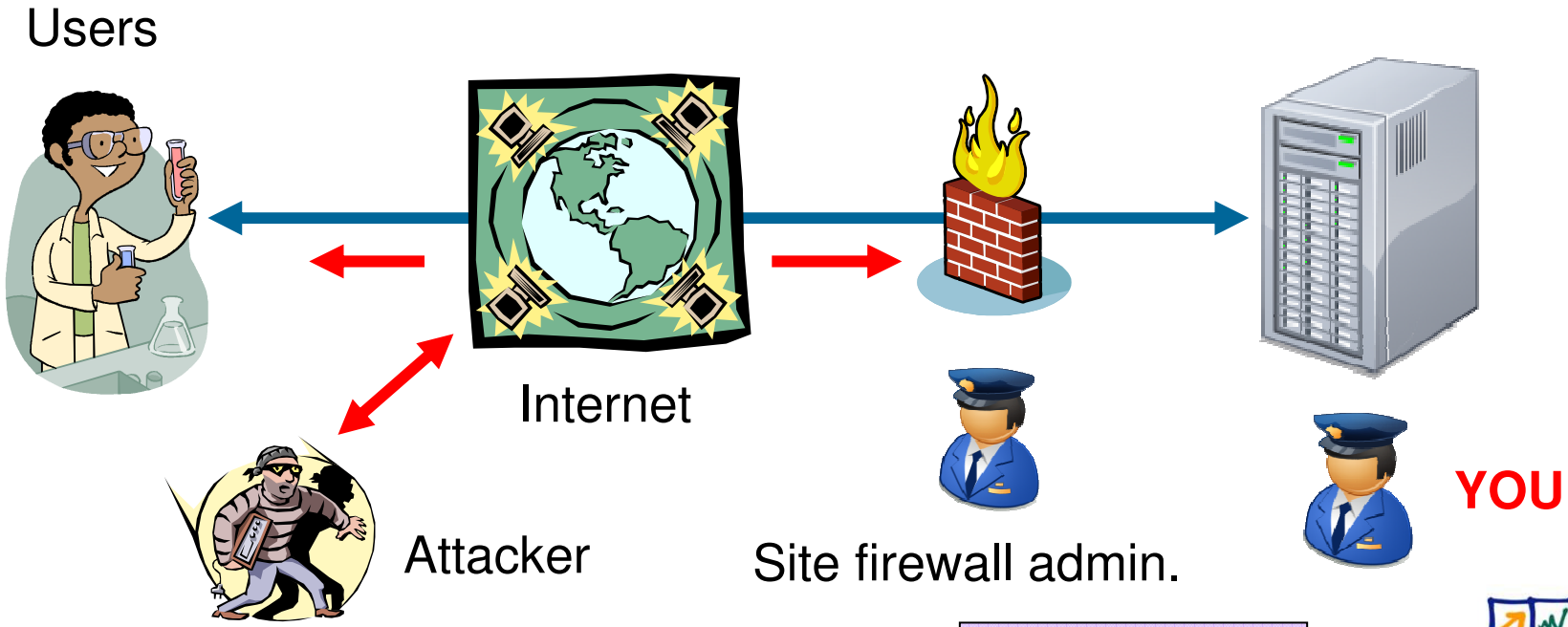
© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- **My site does not get attacked! –** Yes it does!

  You *might not* see all the attacks, but they are out there.



Integrated Site Security for Grids
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu
Information Society and Media

Protect, detect & respond

- **My site does not get attacked!**

What do you think?

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- **Harden** the operating system
- Keep the operating system and application **up-to-date**
- Use a **local firewall**
  - *Do not keep default passwords*
  - *Do not run unnecessary applications*

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- Take advantage of the **logs**
- Use relevant **security products** (e.g. IDS)
- Ensure that **passwords** are secure

  - *Know what is "normal"*
  - *Watch out for "strange" or "unexpected" activity*
  - *Know where the logs are kept*
  - *Know how to read them:*

    2007-08-15 00:00:00 130.246.XXX.XXX GET /Communications/Default.aspx - 80 - 172.16.XXX.X Mozilla/4.0+ (compatible; +MSIE +6.0; +Windows +NT; +MS +Search +4.0 +Robot) ***302*** *0 0* *e.g. successful redirect*

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- You are not alone! Know who can help you. Check with your local site and identify:
  - Your local/national/regional CSIRT (Computer Security Incident Response Team)
  - What your local site process is (if there is one)
  - Your role in an incident and what you can do.

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- You are not alone! Know who can help you. Check with your local site and identify:
  - 80/20 rule
  - “Forensics”

It is better to plan and prepare for incidents before they happen.

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- **Visit the ISSeG web site (www.isseg.eu) for the**
  - Checklist for system administrators

Details of the ISSeG recommendations will be given in session 3.

Integrated Site Security for Grids

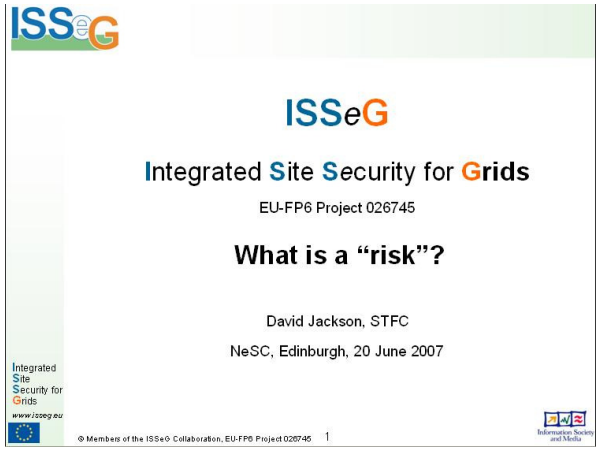
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- You are not alone! Know who can help you.
  - You need to talk to managers to gain support. An example presentation for “senior management” asking for extra resources can be found on www.isseg.eu



http://www.isseg.eu

Integrated Site Security for Grids
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Protect, detect & respond

- **Summary**

  - You are not alone – identify who can help you
  - **Protect** your systems from attack
  - **Detect** the attacks
  - **Respond** to the attacks appropriately
  - Use the checklists and resources on www.isseg.eu to help you.

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

- **Welcome!**
- **Protect, detect & respond**
- **Risk assessments**
- **Recommendations**

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Risk assessments

Security is not a “thing” you do, it is more a process of gradual improvement. You need some way of working out where to start and measure progress.

A **risk assessment process** can help, so

- What are they and why bother?
- Establish a common understanding of risk
- ISSeG risk assessment questionnaire

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

Risk assessments – What are they and why bother?

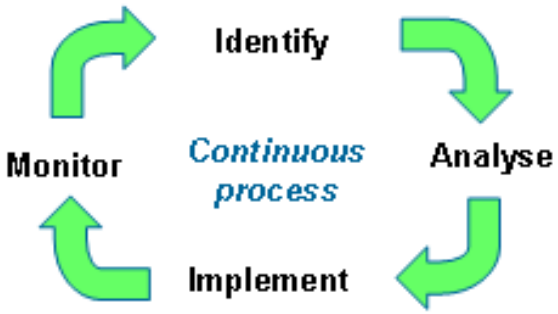
All organizations contain assets that they wish to protect from harm. The harm may be the result of an accidental or deliberate act by an individual or the result of some external event, e.g.

Accidental - A user deletes all their data files
Deliberate - An external attacker tries to access finance information
External event - Flooding of a data centre or loss of power

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Risk assessments – What are they and why bother?

The senior managers within organizations are often required to establish a process to manage risks within the organization as part of a corporate governance strategy. Often a **risk assessment process** is established to support this understanding of risk so that it can:



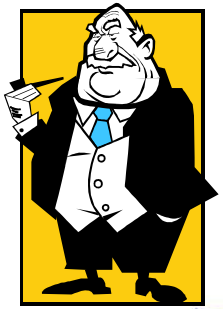
- Identify the assets and risks
- Analyse the existing security controls
- Implement any identified and resourced improvement plan
- Monitor the existing controls to see that they are effective

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Risk assessments

- **Common understanding of "risk" and how to understand some of the many confusing terms.**
  - What is a "risk"? (V5)

Example presentation to help set a common understanding of risk for both the "management" and "technical" people. Should help to understand advice from external sources such as auditors, security experts and web sites.



Integrated Site Security for Grids

www.isseg.eu

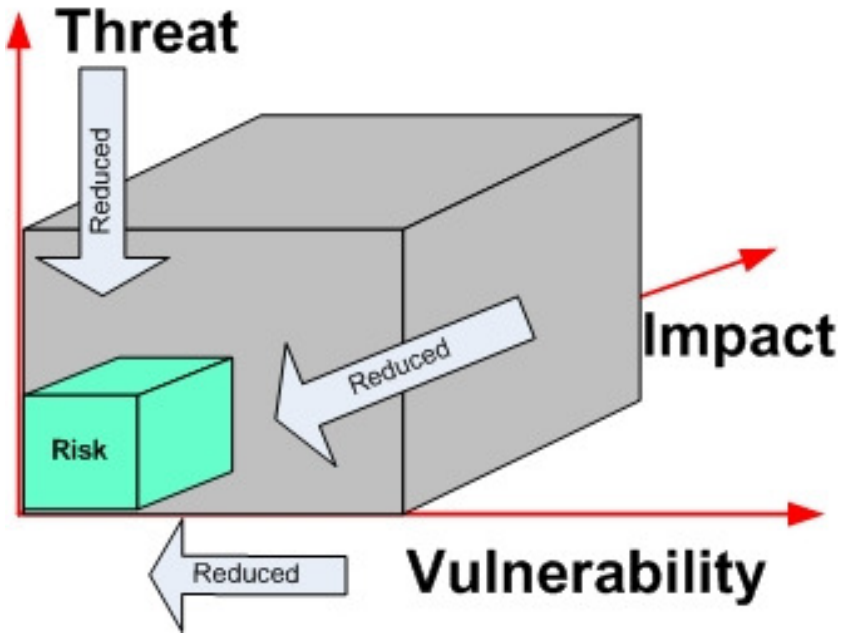
© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

What is a risk?

You can reduce risk down to an acceptable limit (residual risk) and then you just need to deal with it.



***Example**:*

Have more that one connection to the Internet.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Grid specific risks?

- **Vulnerabilities:** There are new Grid specific vulnerabilities.

Sites use homogenous IT resources

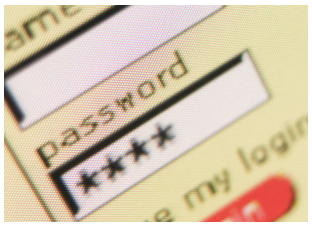
Break in to one site => break in to many sites
One flaw on one node = X flaws on X similar nodes

Middleware

Any new component of a system introduces new vulnerabilities

Users and Activity

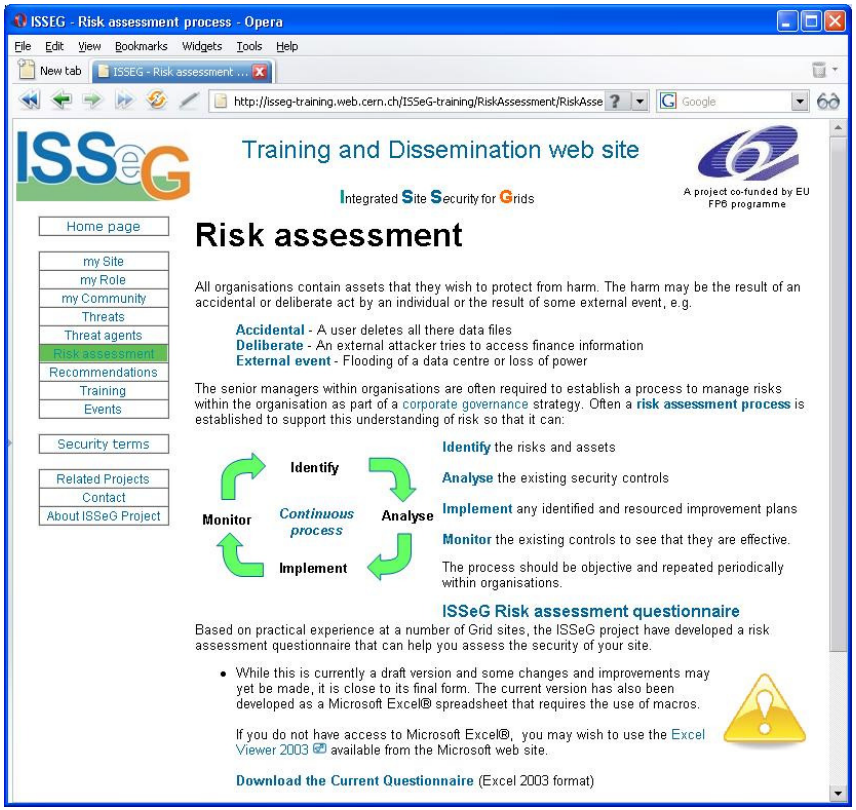
The numbers of both are up. This is increases the probability of an password/pass phrase compromise.



© Members of the ISSeG Collaboration, EU-FP6 Project 026745

ISSeG risk assessment questionnaire

Based on practical experience at a number of Grid sites, the ISSeG project have developed a risk assessment questionnaire that can help you assess the security of your site.



Integrated Site Security for Grids

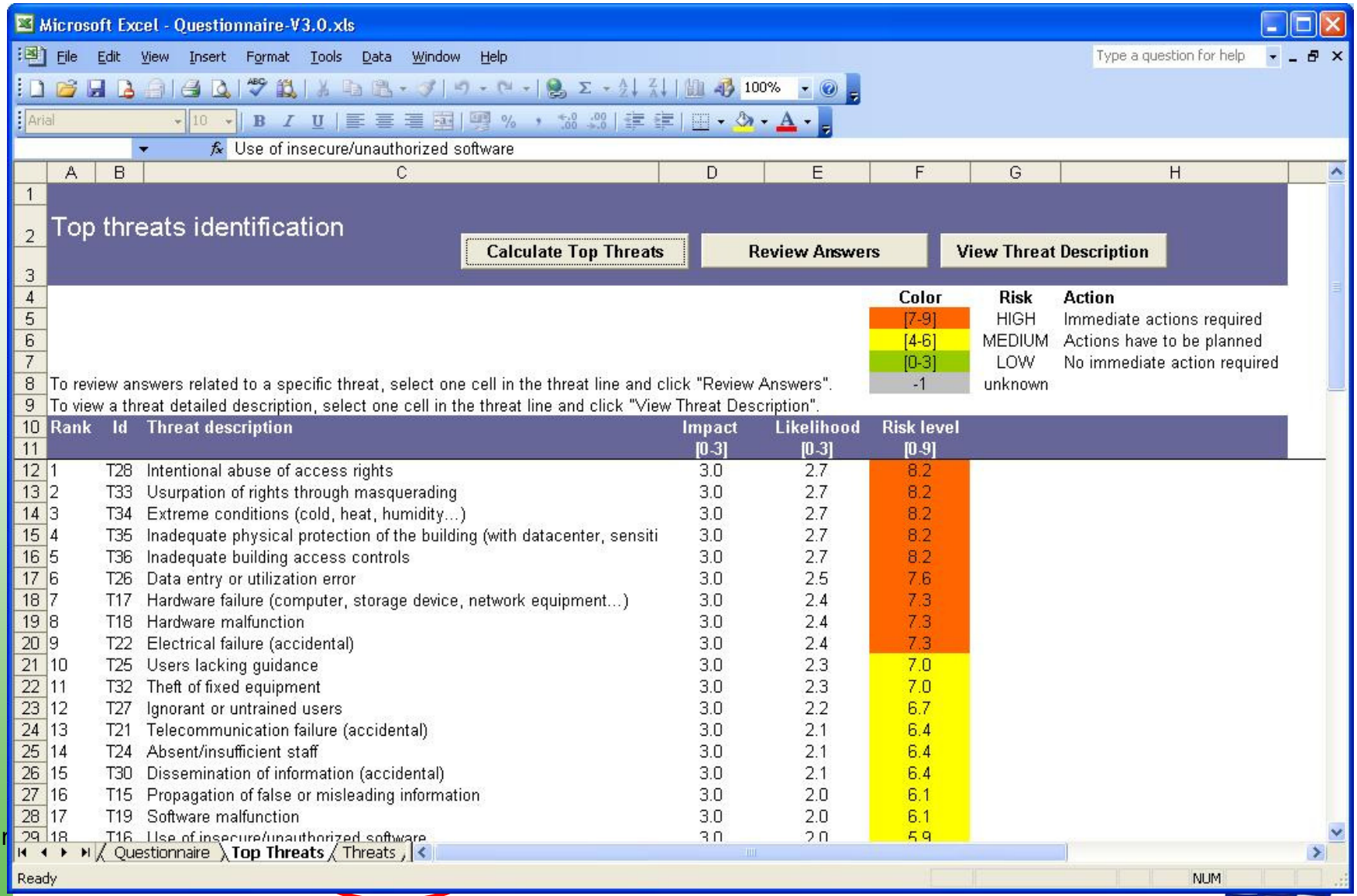
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

ISSeG questionnaire



Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

ISSeG – Top 12 threats

ISSeG

Training and Dissemination web site

Integrated Site Security for Grids

A project co-funded by EU FP6 programme

Home page

my Site
my Role
my Community
Threats
Threat agents
Risk assessment
Recommendations
Training
Events

Security terms

Related Projects
Contact
About ISSeG Project

Threats - Top 12 threats

Based on the implementation of the ISS concept at two Grid sites, feedback from Site security officers within operational Grid environments and the development of the ISSeG risk assessment questionnaire, we believe the top 12 threats to grid sites to be:

Top 12 list of threats

- T1: Faulty access rights management
- T2: Password compromise
- T3: Intrusion (by scanning techniques)
- T5: Data interception techniques (sniffing/man in the middle attack)
- T6: Fraudulent connection
- T7: Exploiting software vulnerabilities
- T8: Fraudulent use of systems
- T9: Repudiation (system usage)
- T13: Software alteration (time bomb, worm, Trojan, virus etc.)
- T16: Use of insecure/unauthorized software
- T24: Absent/insufficient staff
- T27: Lack of security awareness or job training

Clearly, creating a list of the top 12 threats for all Grid sites world wide is controversial as each site and Grid infrastructure (e.g. OSG, EGEE etc.) is difference. This **is an illustrative list** and should not be regarded as a universal list for all sites world wide. Please contact us if you would like this list to be updated in some way.

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

ISSeG risk assessment questionnaire

- This can help you **start** the risk assessment process and identify what assets you have and some of the risks.
- You still need to develop the rest of the risk assessment and management processes for your site.
- Based on ISO/IEC 17799:2005 standard

  (e.g. the long list of technical controls)

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Risk assessments help you

- Establish a common understanding of risk across the organisation
- Identify and prioritise what security controls need to be implemented first

The risk assessment process should be repeated regularly to maintain the effectiveness of your security controls.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

- **Welcome!**
- **Protect, detect & respond**
- **Risk assessments**
- **Recommendations**

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Recommendations

The ISSeG project has identified 69 potential recommendations for sites so far. We will

- Discuss where to find the recommendations
- How they were developed (in brief!)
- Look at some examples in detail
- Recommendations and training are linked.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Where to find the recommendations

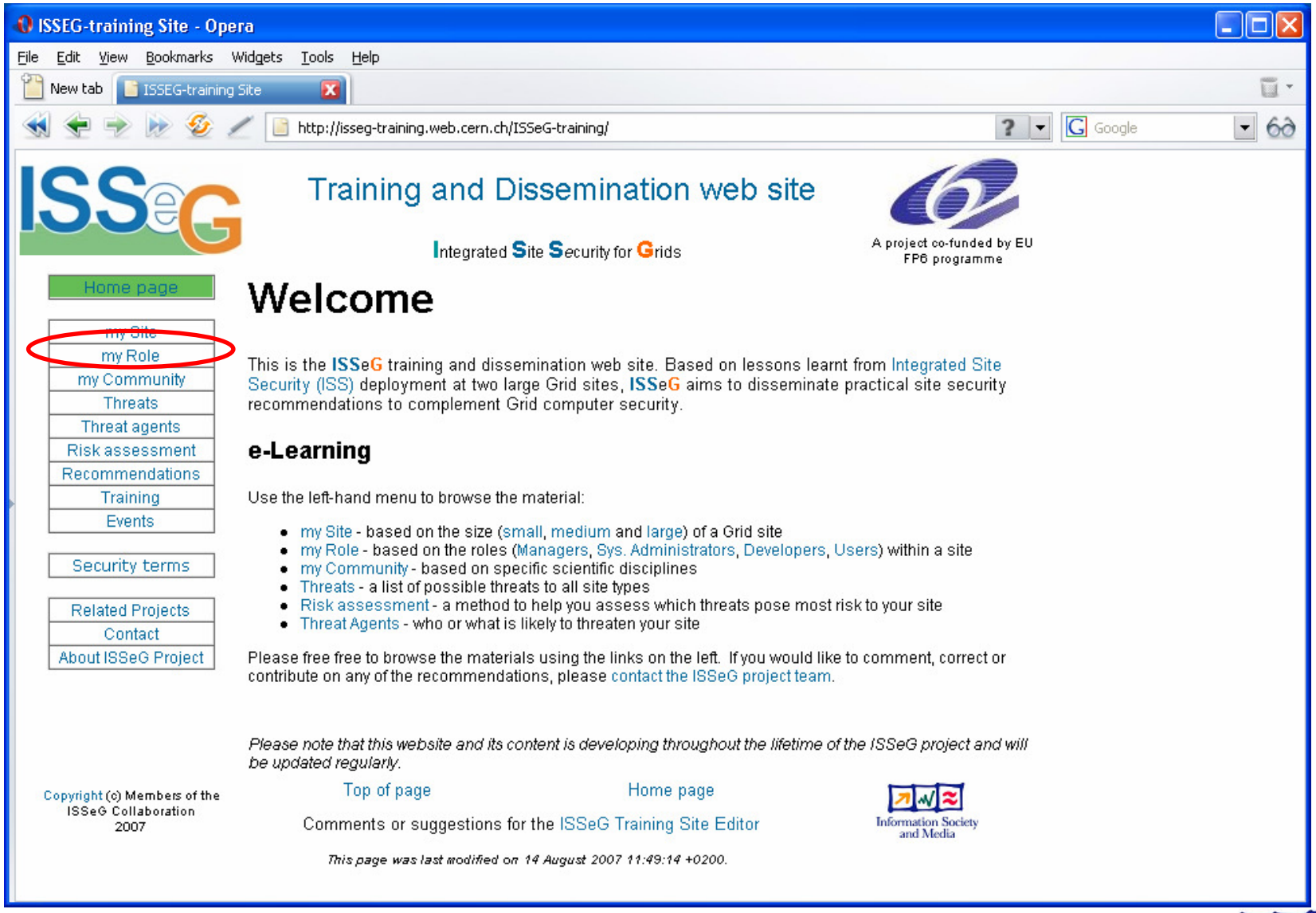
Based on practical experience, the ISSeG project has identified 69 potential recommendations for sites, each with implementation details. For example:

- R2: Centrally manage patches and system configurations
  - Linux based method
  - Windows based method

Visit www.isseg.eu to see the full list as it develops.

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

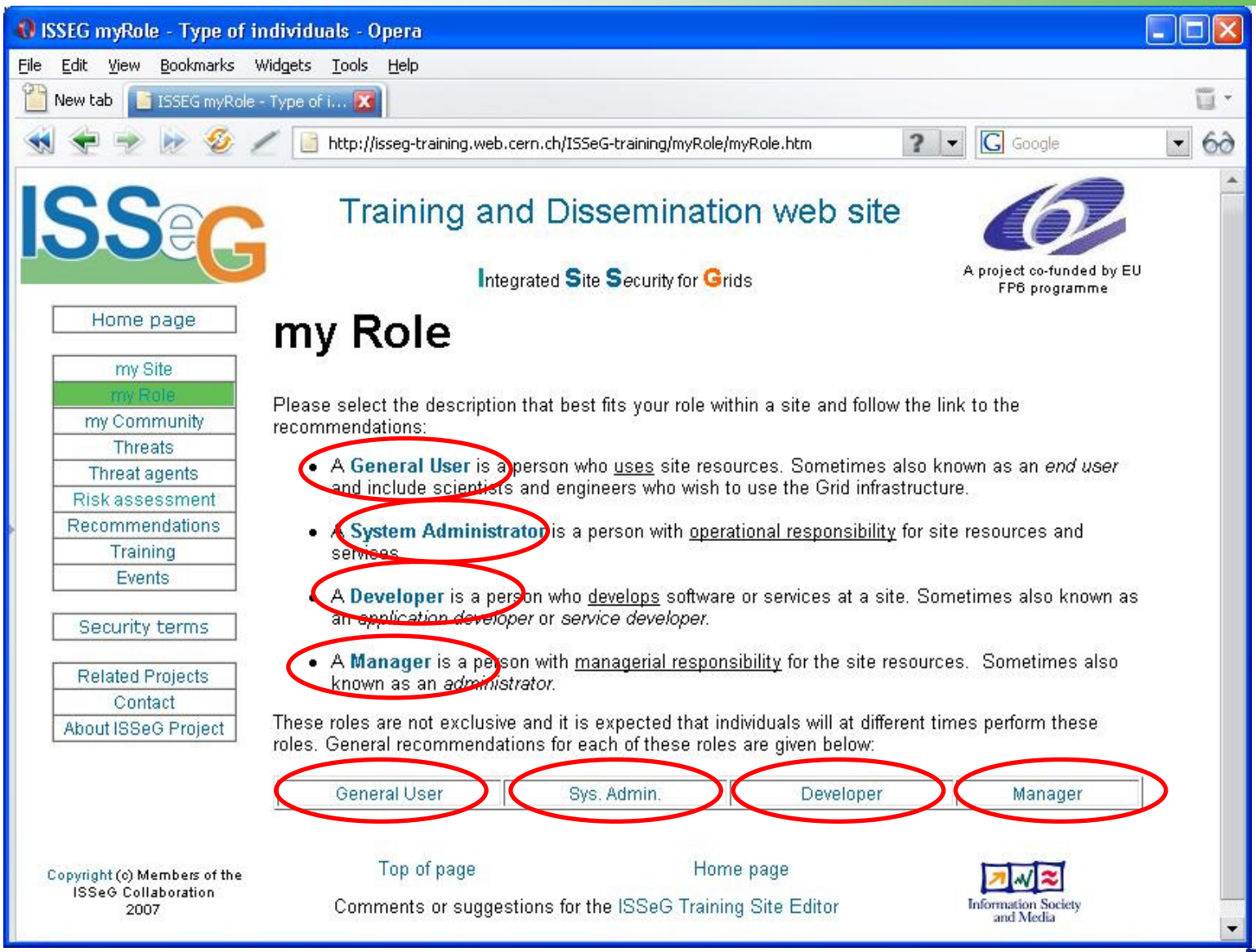
Recommendations



Integrated Site Security for Grids

www.isseg.eu

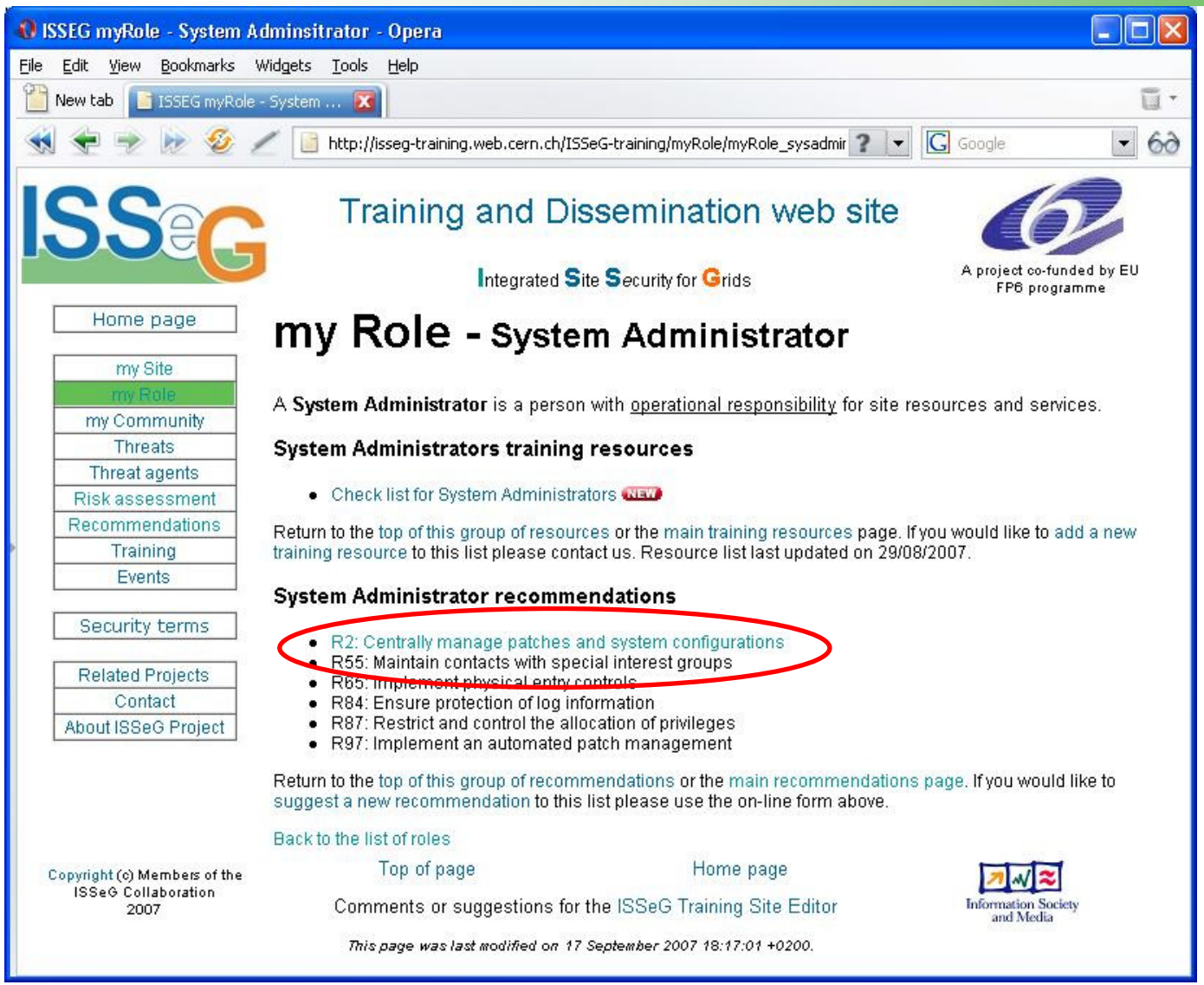
Recommendations



Integrated Site Security for Grids

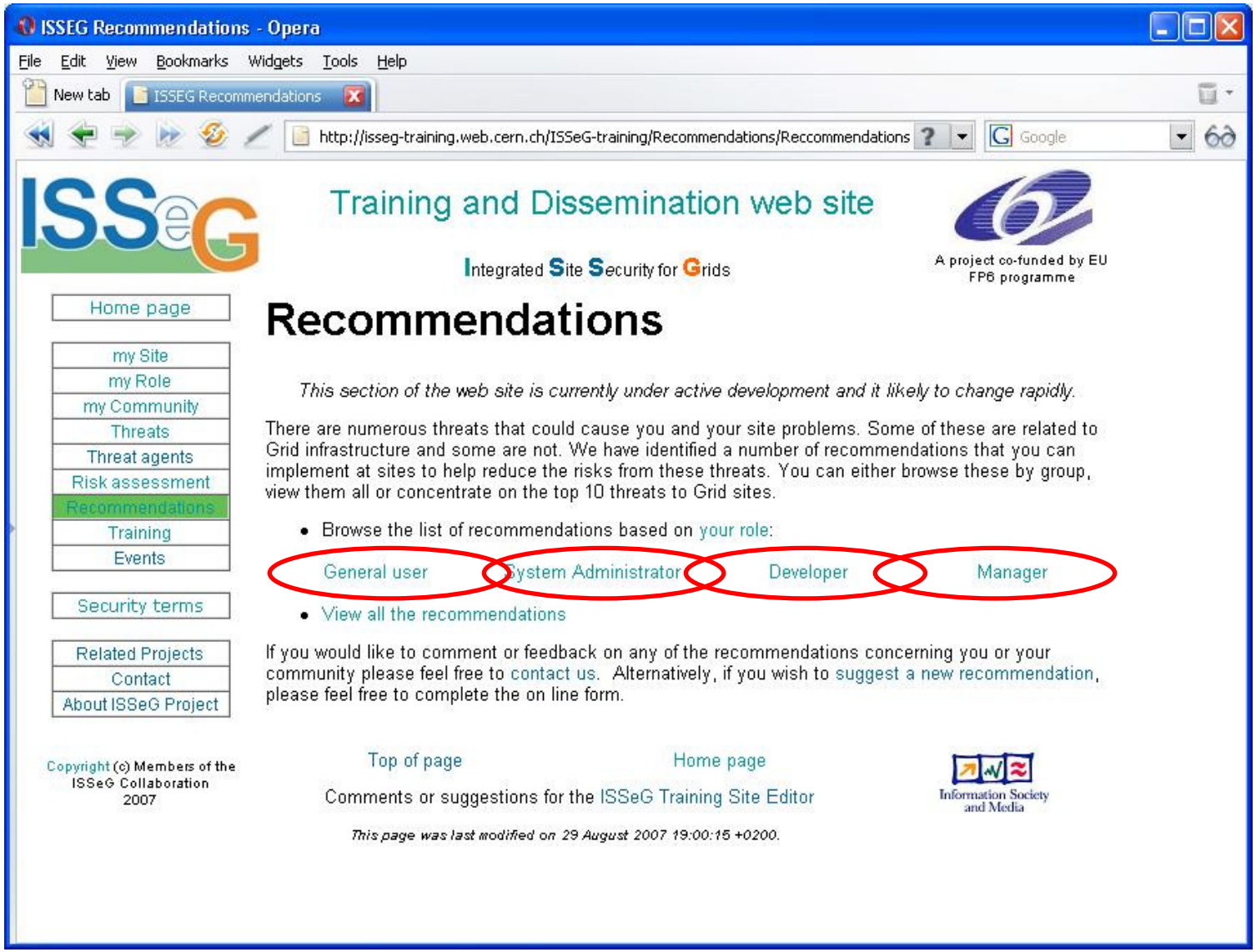
www.isseg.eu

Recommendations



Integrated Site Security for Grids

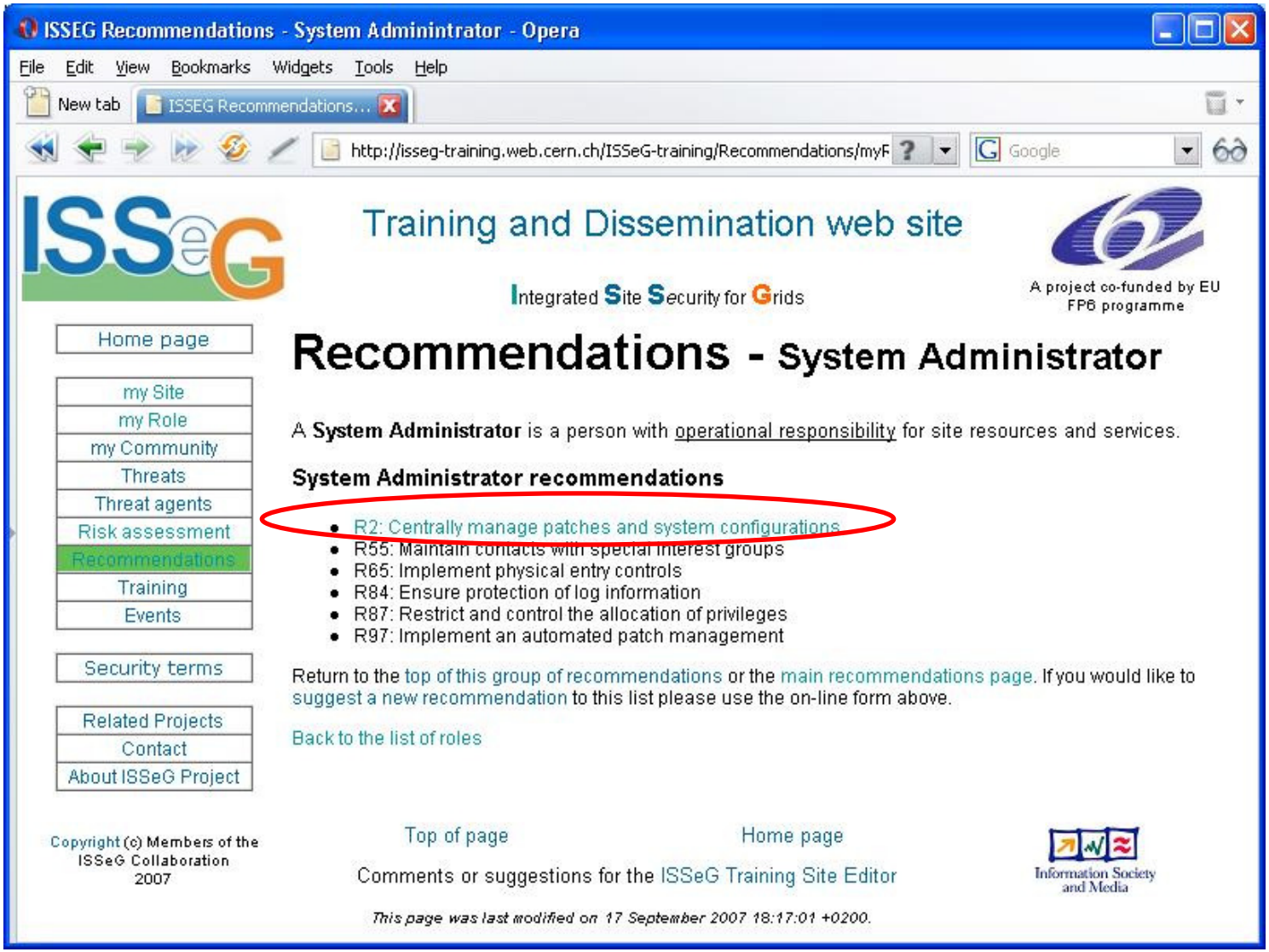
www.isseg.eu



Integrated Site Security for Grids

www.isseg.eu

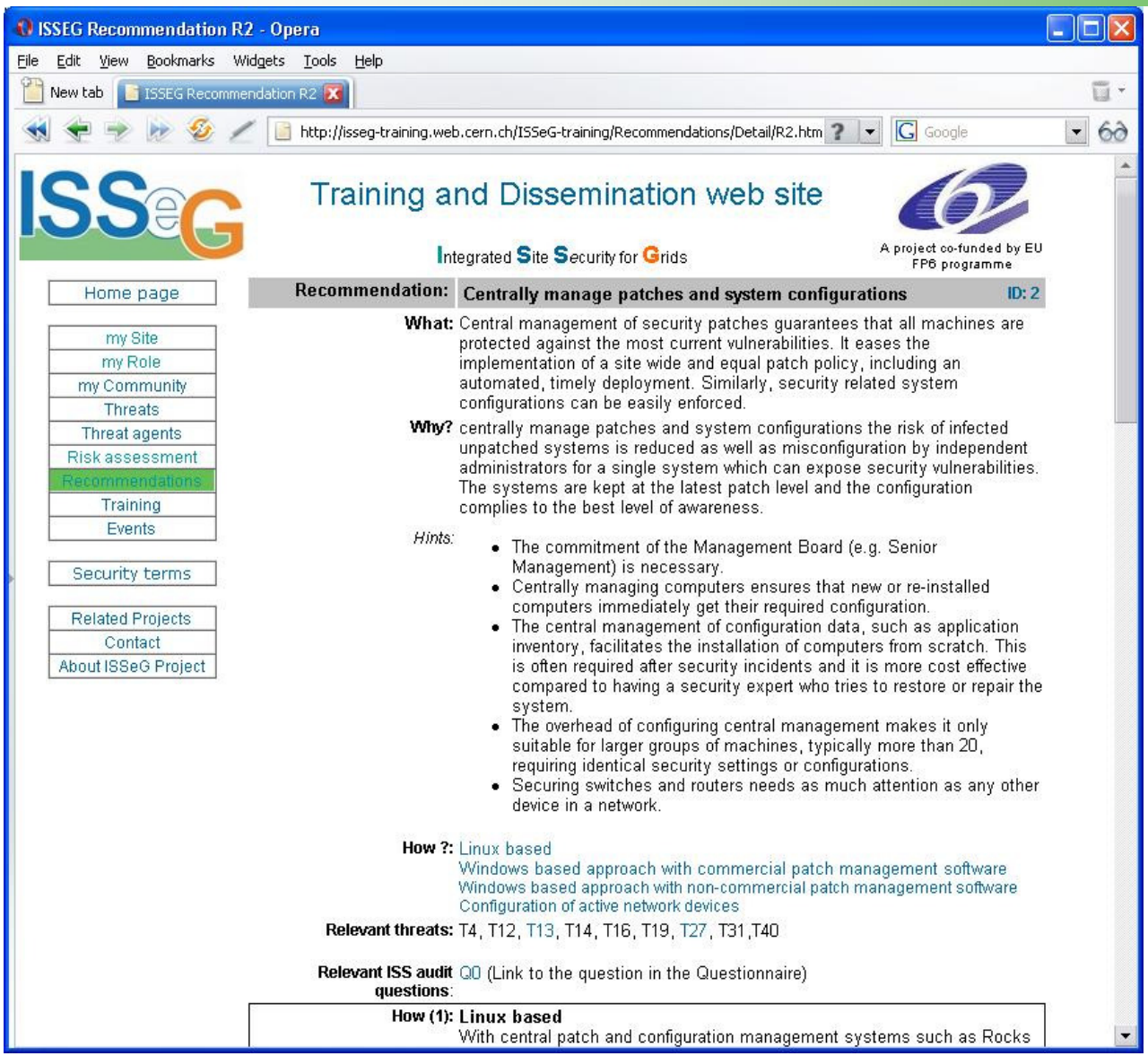
Recommendations



Integrated Site Security for Grids

www.isseg.eu

Recommendations



Integrated Site Security for Grids

www.isseg.eu

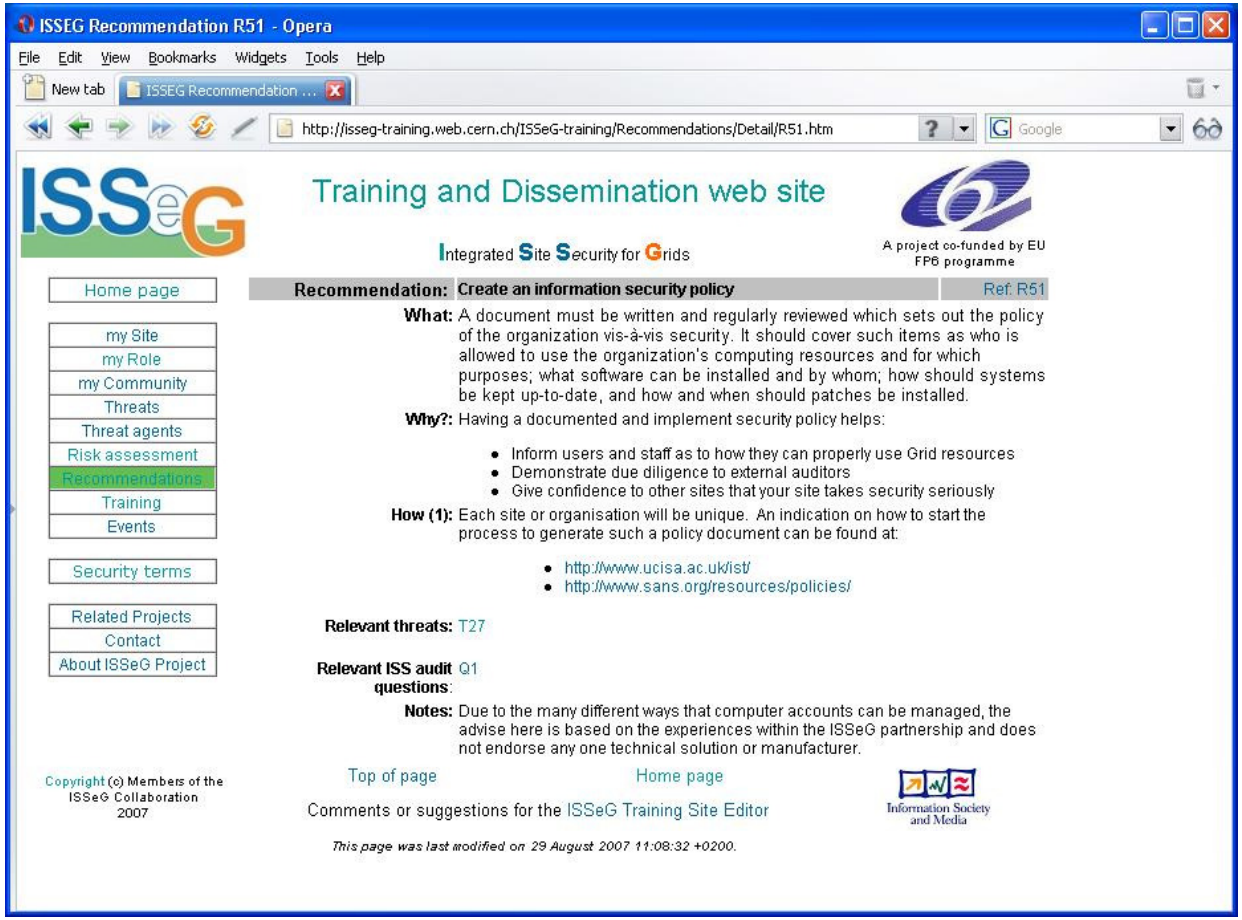
© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Recommendations

- **Common structure:**
  - What
  - Why
  - How
  - Links



Integrated Site Security for Grids

www.isseg.eu

Recommendations

Broaden the use of centralised management

- R1: Centrally manage accounts
- R2: Centrally manage patches and system configurations
- R3: Centrally manage Internet Services

Integrate identity and resource management

- R4: Provide integrated identity management
- R5: Ensure resources link to the people in charge of them
- R6: Define responsibilities using roles and groups

Manage your network connectivity

- R7: Restrict Intranet access to authorised devices
- R8: Restrict Internet access to authorised connections
- R9: Segregate networks dedicated to sensitive devices
- R10: Expand the use of application gateways

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Recommendations

Use security mechanisms and tools

- R11: Strengthen authentication and authorisation
- R12: Increase the use of vulnerability assessment tools
- R13: Adapt incident detection to meet evolving trends
- R14: Strengthen and promote network monitoring tools
- R15: Enhance span filter tools and mailing security
- R16: Extend policy enforcement

Strengthen administrative procedures and training

- R17: Adapt training to requirements of users, developers and system administrators
- R18:Integrate security training and best practice into organisational structures
- R19:Maintain administrative procedures in step with evolving security needs
- R20: Extend policy regulations
- R21: Regulate the use and coexistence of legacy Operating Systems

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

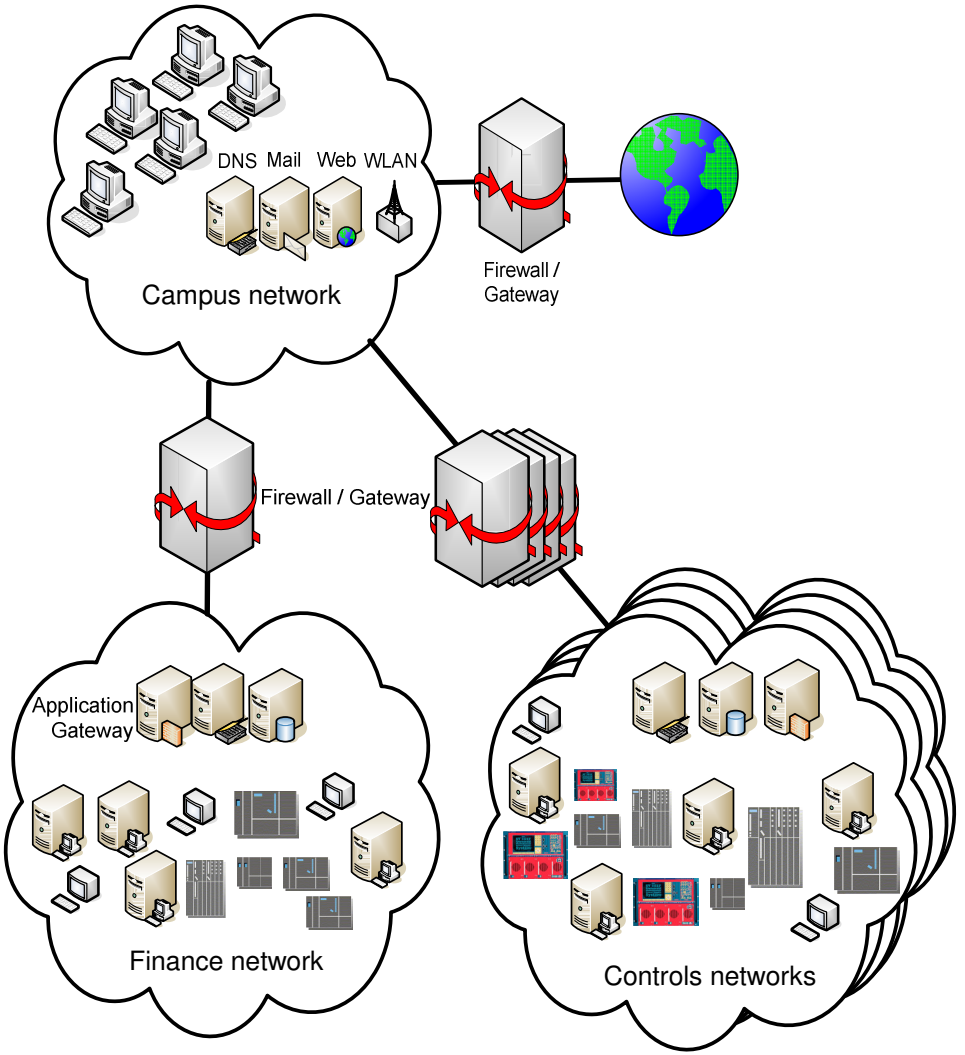
Recommendations

- R51: Create an information security policy
- R52: Review your information security policy
- R53: Allocate information security responsibilities
- R54: Establish confidentiality agreements
- R55: Maintain contacts with special interest groups
- R56: Maintain an inventory of assets
- R57: Establish ownership of assets
- R58: Define acceptable use for assets
- R59: Establish information classification guidelines
- R60: Develop information labeling and handling procedures
- R61: Define terms and conditions of employment
- R62: Encourage information security awareness, education and training
- R63: Ensure access rights are up to date
- R64: Establish a physical security perimeter
- R65: Implement physical entry controls
- R66: Provide physical protection and guidelines for working in secure areas
- R67: Protect equipment from disruptions in supporting facilities
- R68: Assure secure disposal or reuse of equipment
- R69: Document your operating procedures
- R70: Manage changes to information processing facilities and systems
- R71: Separate you development, test, and operational facilities
- R72: Implement capacity management
- R73: Install and regularly update malicious code detection and repair software
- R74: Manage the execution of mobile code
- R75: Establish backup and restoration procedures
- R76: Implement intrusion detection and prevention mechanisms
- R77: Control access to your network
- R78: Use cryptographic techniques for information confidentiality and integrity
- R79: Establish agreements for exchange of information and software with external parties
- R80: Enhance the security of your e-mail communications
- R81: Protect the integrity of publicly available information
- R82: Enable audit logging of user activities, exceptions and security events
- R83: Establish procedures for monitoring system use and reviewing results
- R84: Ensure protection of log information
- R85: Establish an access control policy based on security requirements
- R86: Establish a formal procedure to control the allocation of access rights
- R87: Restrict and control the allocation of privileges
- R88: Implement a formal management process for password allocation
- R89: Enforce good practices in the selection and use of passwords
- R90: Ensure that unattended equipment is appropriately protected
- R91: Prevent unauthorized access to network services
- R92: Implement strong authentication for external connections
- R93: Adopt appropriate security measures for mobile computing
- R94: Implement appropriate policy, procedures, and guidelines for teleworking
- R95: Establish training and guidelines for secure programming
- R96: Establish a formal application integration/qualification process
- R97: Implement an automated patch managementS5: Strengthen administrative procedures and training *(cont.)*

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Example recommendations

- **Restrict Internet access to authorized connections**
  - Closing firewall access impacts used applications
  - Update mechanism is required
- **Segregate networks dedicated to sensitive devices**
  - Requires careful analysis of requirements and impact
- **Expand the use of application gateways**
  - Reduces spread of incidents
  - Useful for *untrusted* devices
- **Restrict Intranet access to authorized devices**
  - 802.1x functionality
  - A mapping to the device owner is recommended



Integrated Site Security for Grids

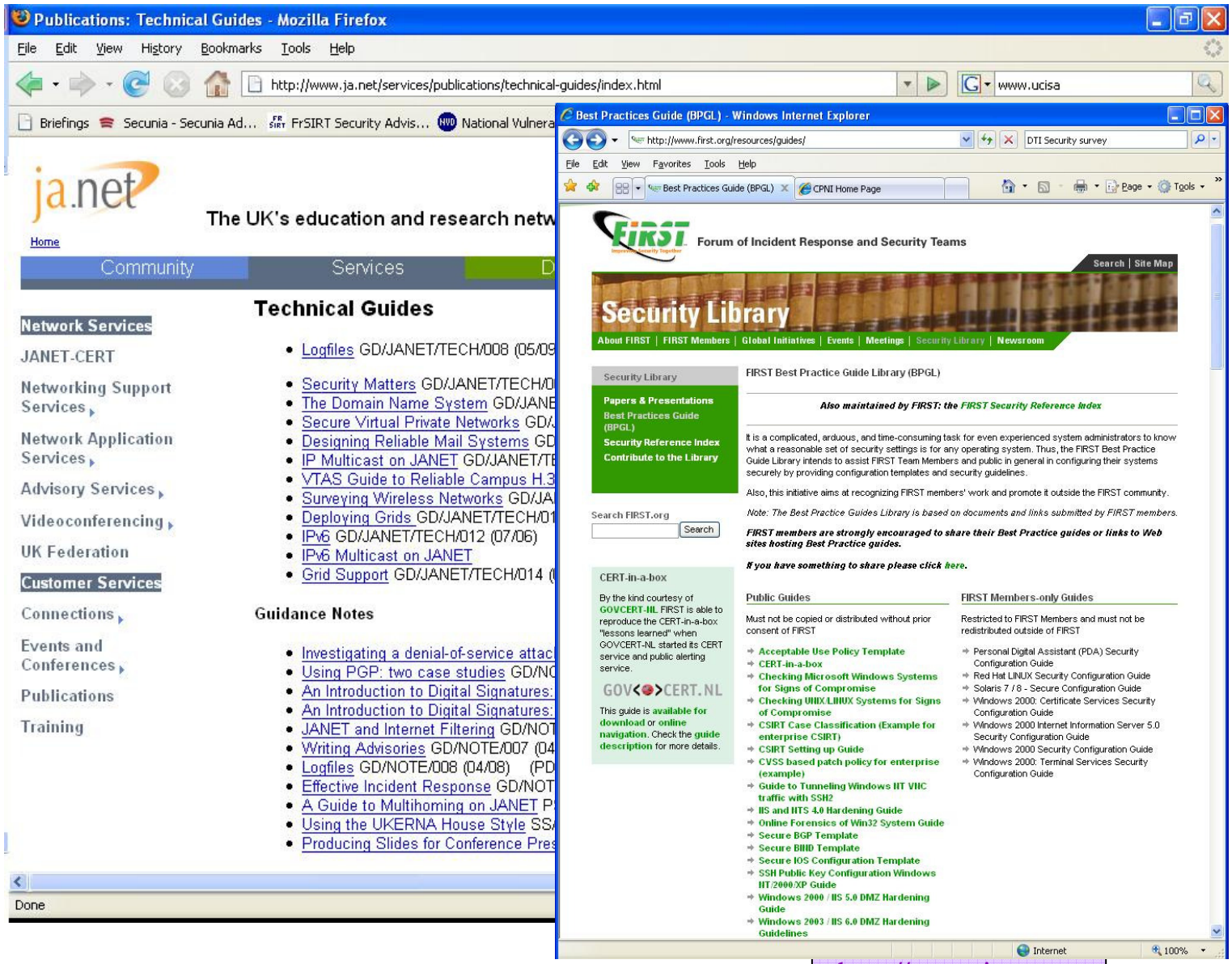
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Example recommendations



Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Example recommendations

- **General users**
  - Computer users just want to get on and use the systems. Security needs to invisible.
  - They need to know why security is relevant to them.

this is not good security…

Integrated Site Security for Grids

www.isseg.eu

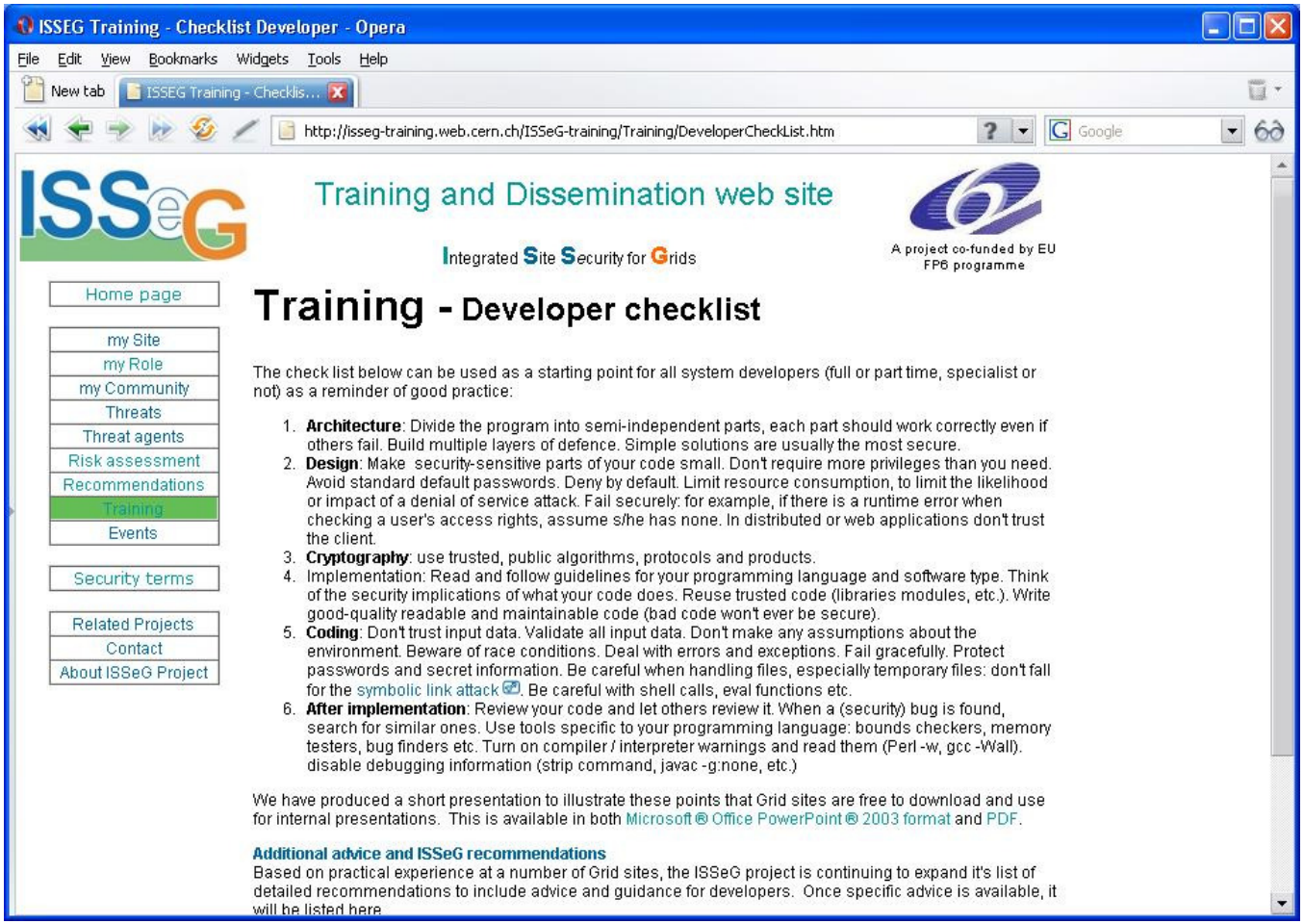
© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Example recommendations

- **Application developers**
  - Check lists can be useful aids to secure software.

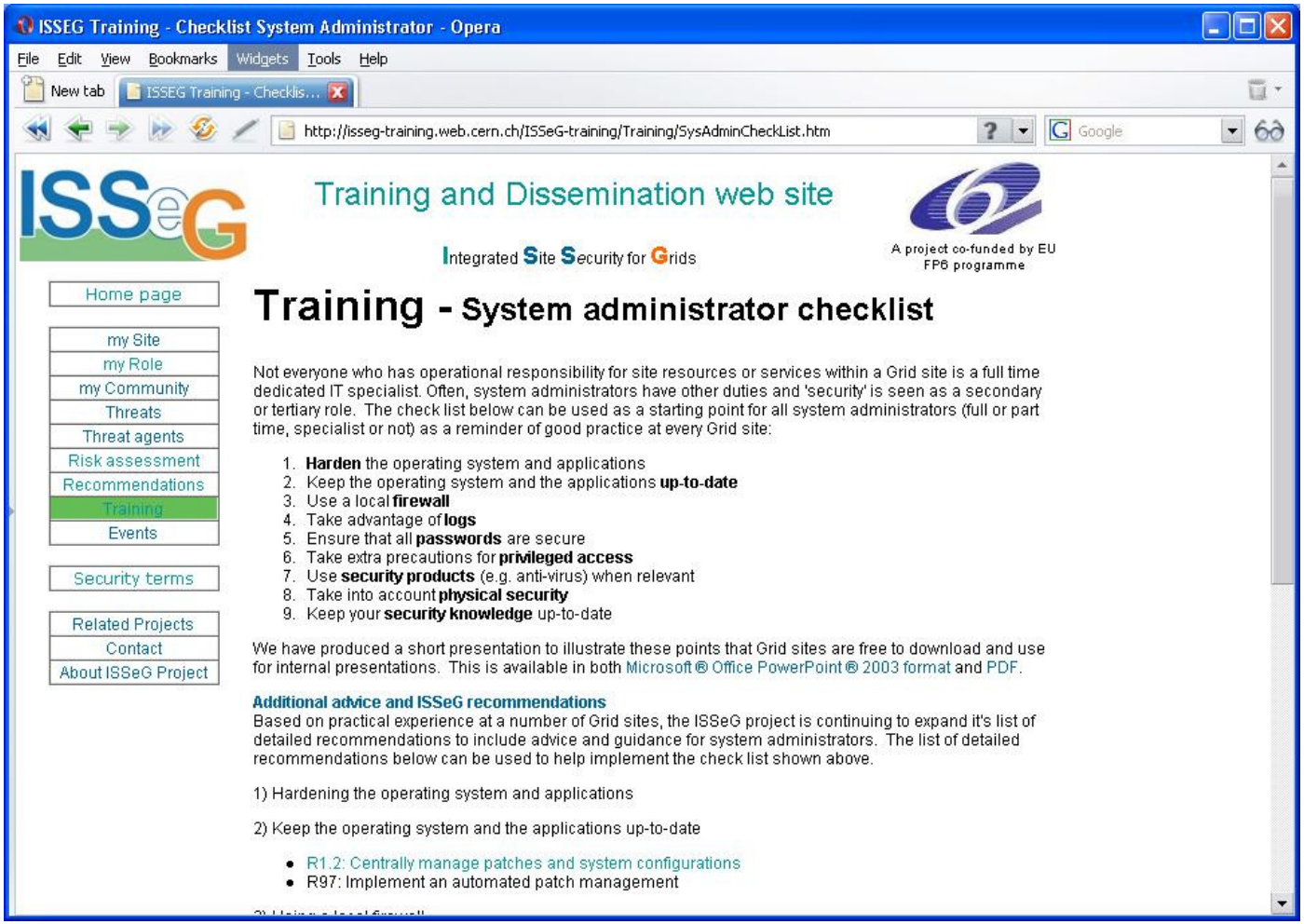


Integrated Site Security for Grids
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Example recommendations

- **System Administrators**
  - Check lists can be useful aids



Integrated Site Security for Grids
www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu
Information Society and Media

General users

- **General advice & material for users**
  - Computer security advice for users (V4)

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

System Administrators

- **General advice & material for Sys. Admins.**
  - Checklist for system administrators (V4)

Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Information Society and Media

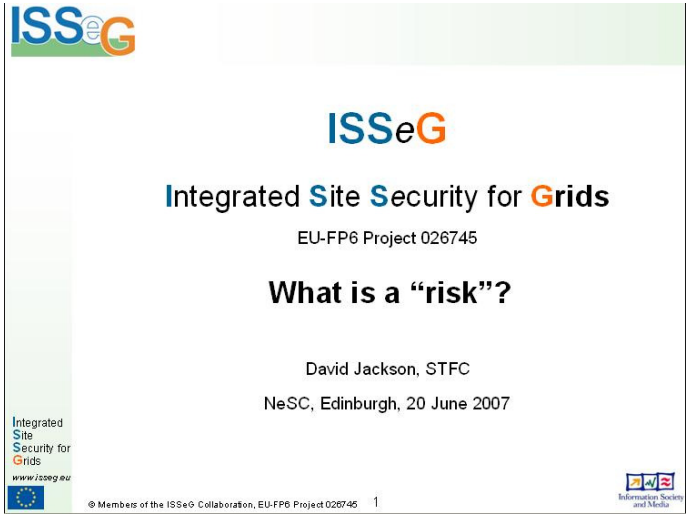
Developers

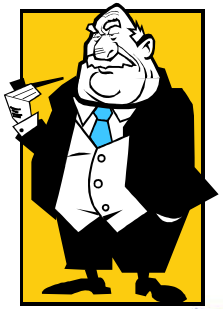
- **General advice & material for developers**
  - Checklist for developers (V1)

http://www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

- **General advice & material for managers**





Integrated Site Security for Grids
www.isseg.eu

http://www.isseg.eu

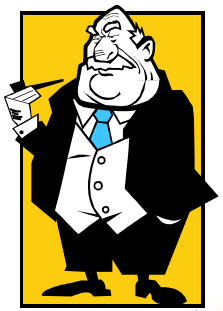
Information Society and Media

How to sell security – working with managers

- We want resources (staff time and money)
- We need support
- Managers want reassurance
- Managers see security as a necessary evil

Guidance notes are being developed

- Management case for site security (V6)



Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

http://www.isseg.eu

Information Society and Media

Premise

Science today requires participation in Grid environments where multiple sites act as one entity and share resources.

As Grid use rises, all sites are at increased risk from electronic attack and compromise.

Due to the interconnected nature of Grid sites, once one site has been compromised, all others sites are at increased risk of compromise.

***Q**: Do we want to be the first site compromised?*
***Q**: What if we were, what would be the impact?*
***Q**: What can we do to prevent being compromised?*

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

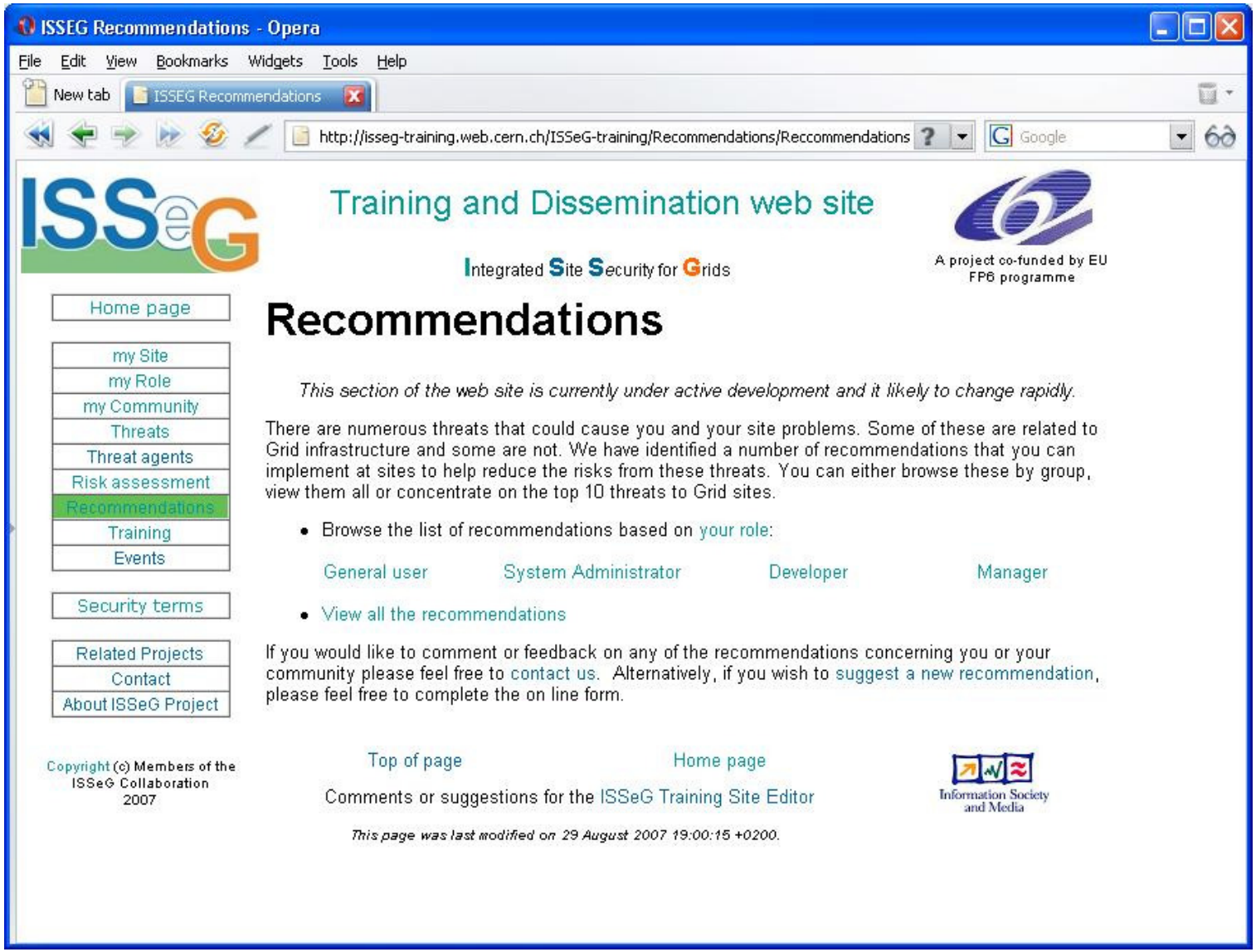
Summary

You are asked to:

1. **Support** the implementation of an annual risk assessment process to:
   - identify what assets are most at risk
   - review the current level of protection and detection
   - propose annual improvement plans
   - identify any additional staff time & costs required
2. **Allocate** appropriate resources to implement the agreed annual improvement plans
3. **Support** an integrated approach within the improvement plans to ensure that technical, administrative and educational security aspects are coordinated

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Summary: Session 3



Integrated Site Security for Grids

www.isseg.eu

© Members of the ISSeG Collaboration, EU-FP6 Project 026745

Feedback and questions

- We would like to improve the training materials based on your feedback, comments and questions
- Please complete the attendance form
- Please return your completed feedback forms

Thank you for your time and attendance!

© Members of the ISSeG Collaboration, EU-FP6 Project 026745