Disclaimer

This is an PILOT presentation provided by the ISSeG collaboration intended for non-commercial and non-profit training purposes only.

Where trademarks (registered or unregistered) are mentioned such mention is made merely to describe the goods and services related to such trademark, and does not affect the ownership thereof or the rights of the owners.

See **http://www.isseg.eu/03_About_IsseG/Partners/Partners.htm** for details on the copyright holders.

ISSeG

Integrated Site Security for Grids

EU-FP6 Project 026745

Management case for site security

David Jackson, STFC

CHEP 07, Victoria BC, 4 September 2007

Integrated
Site
Security for
Grids

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?*

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

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

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Contents

- **Source of electronic attacks**
- **Impact of an attack**
- **What has the Grid changed?**
- **Prevention: Effective security controls**
  - Concept of Integrated Site Security
  - Selection of effective security controls
- **Summary**

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Source of attacks

- **Who are the attackers?**
  - **Internal**: Sometimes known to you (e.g. staff, students, visitors)
  - **External**: Organised crime conducting electronic attacks - Not just lone teenagers!
- **What do they want?**
  - Potential to use the Grid/site resources for other attacks and/or illegal activity.

Internal - Source of attacks

Internal e.g. Known individual

Enron

- Fraud – Jeffrey Skilling sentenced to 24 years in prison.

Oxford University

- Two students hacked into the network and exposed personal data & CCTV images with “good intent” (2004)

In some cases the liability is clear and can result in the large direct losses (e.g. Enron). In other cases, the potential liability may be equally high (e.g. Data Protection issues for Oxford University) but the organization’s ***reputation is damaged first***

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

External - Source of attacks

External e.g. unknown individual

TK Maxx

- Parent company (TJX) lost 45 million customer payment card records as the result of an information security breach (2007)

Estonian e-government

- During early May 2007, most Estonian on line e-government services were targeted using a high bandwidth distributed denial of service attack.

It is believed that the TJX incident was the result of organised crime and not a lone teenager.

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

External - Near Grid example

- **Fermi National Accelerator Lab**

  In June 2002, the lab network was broken into 17 times and triggered a massive security alert. Due to uncertainty of the nature of the ‘attack’, the lab was disconnected from the Internet for 3 days. The clean up costs were estimated at £21,215 (~ 32,400 USD, 33,300 EUR) plus staff time.

  Fermi lab reputation for security is intact. They successfully reacted to the incident and could show due diligence.

  http://www.fnal.gov/pub/news04/inthenews20040105.html

External - Near Grid example

- **Fermi National Accelerator Lab**
  - Attacker: Joseph McElroy
  - Age: 16 (at time of attack)
  - Reason: Wanted to use the network resources to download and store GBs of copyrighted material.

©Image copyrighted by BBC.

http://news.bbc.co.uk/1/hi/technology/3452923.stm

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Q: Is the FERMI incident event relevant?

- **Grid sites are attractive targets as they have**
  - Large Internet connections (~ 10s of Gbps)
  - Large data storage (~10s TB)
  - Large computing resource (~1000s of CPUs)
  - Allow external access
  - Highly interconnected (e.g. breaking in at one point gives you access to many sites.)

The likelihood that some Grid sites will be compromised and used to attack other sites (Grid or non Grid) increases with Grid use.

A: Yes. The questions is not “If”, more “When” and “Who”.

Impact of attack

- **What is most at risk of damage?**
  - Reputation? Funding?
  - Grid nodes? Computing time?
  - Staff time? Staff time to restore service?

By reacting **appropriately** to incidents the reputation of an organization **can be strengthened.**

By reacting **inappropriately** to incidents the reputation of an organization **can be damaged**.

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

What has the Grid changed?

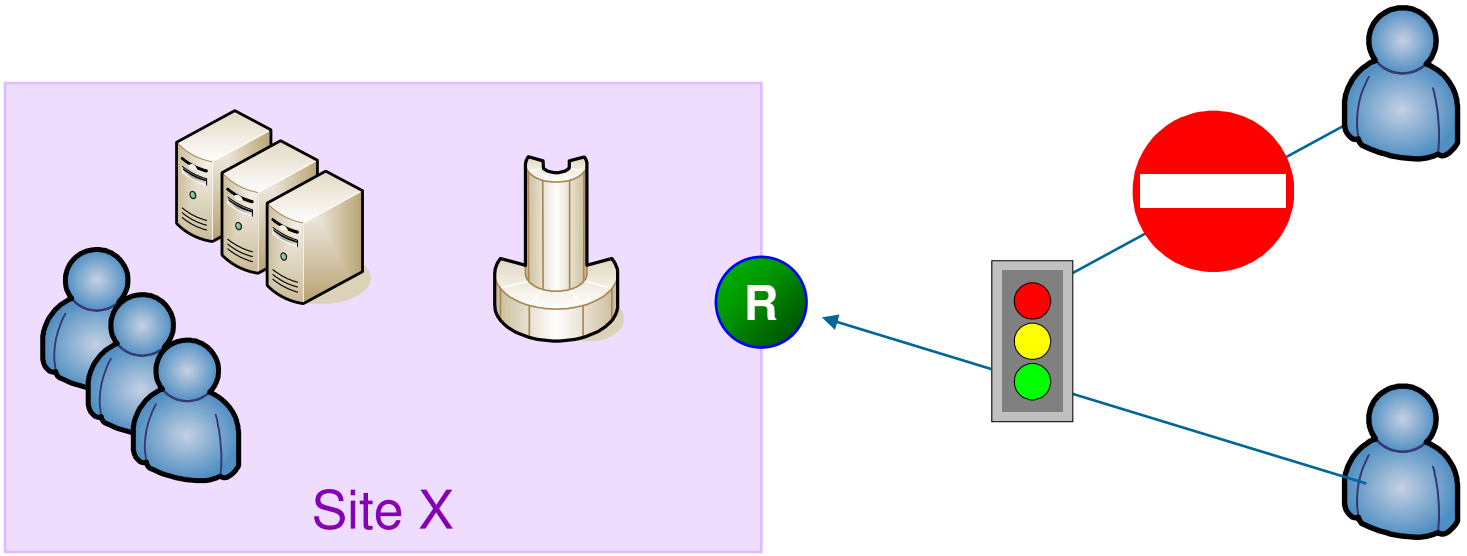
- **Q: What has changed with Grids?**
  - Site boundaries?
  - Number of users?
  - Closer interaction and operation with academic partners?
- **A:** All three have changed and expanded. That was how the Grid was designed and we all use it for Science. Turning it off is not a realistic option.

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

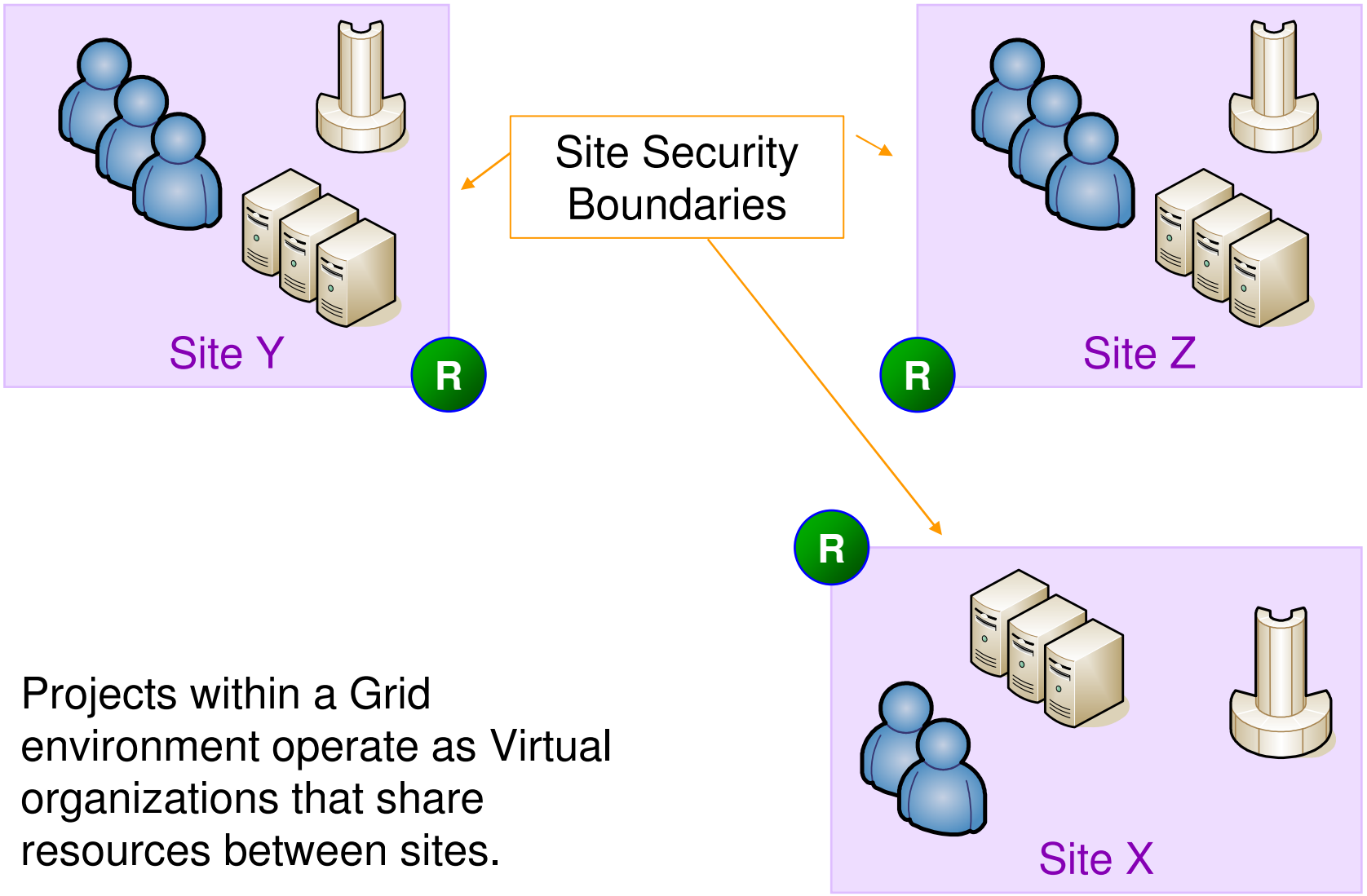
Change in site boundaries

- The traditional or conventional approach to site security is to draw a border around your site and only let in people that you trust.



- **You** have administrative control and can decide who can use the resources at your site. **You set the boundaries**.

Change in site boundaries



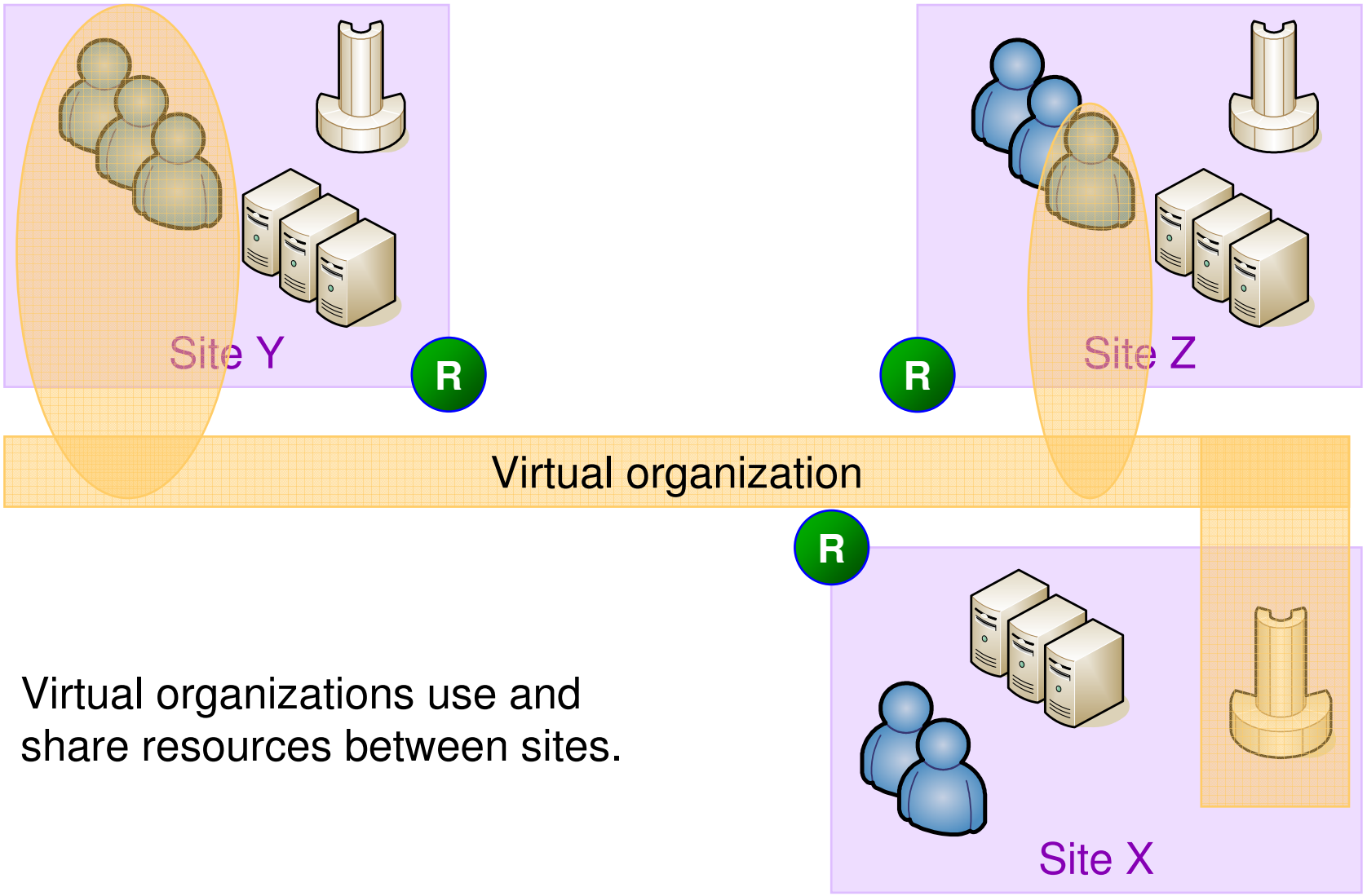
Projects within a Grid environment operate as Virtual organizations that share resources between sites.

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Change in site boundaries



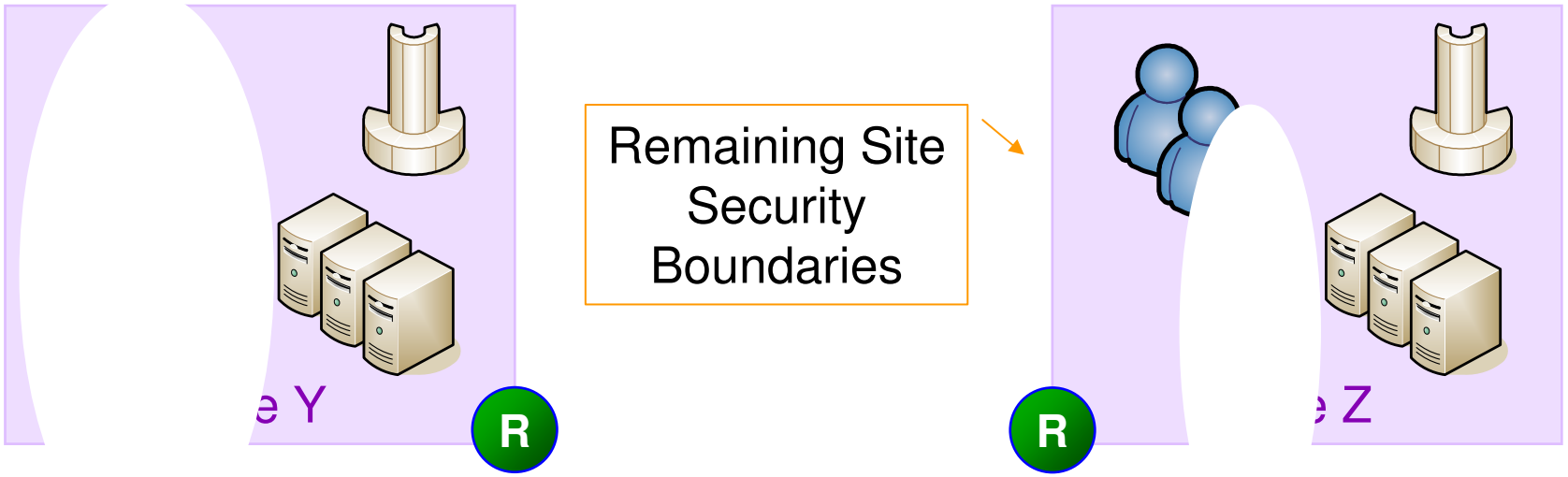
Virtual organizations use and share resources between sites.

Integrated Site Security for Grids

www.isseg.eu

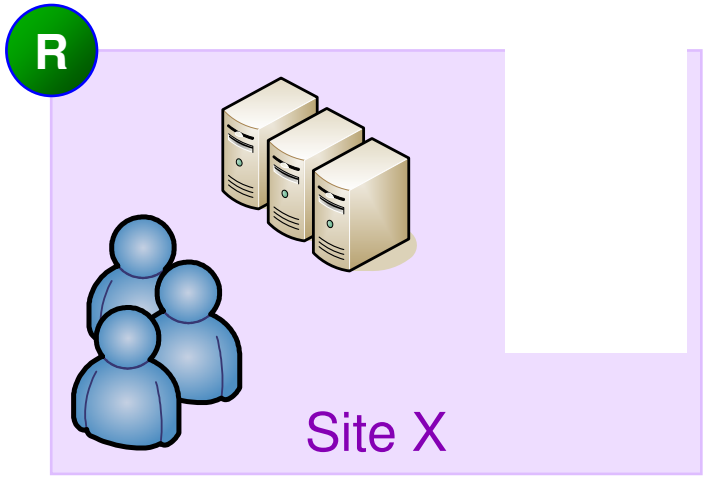
Information Society and Media

Change in site boundaries



Virtual organization holes in ‘traditional’ site boundaries.

Your site now has holes within its original boundary. You are at increased risk from others and pose a risk to them as well.

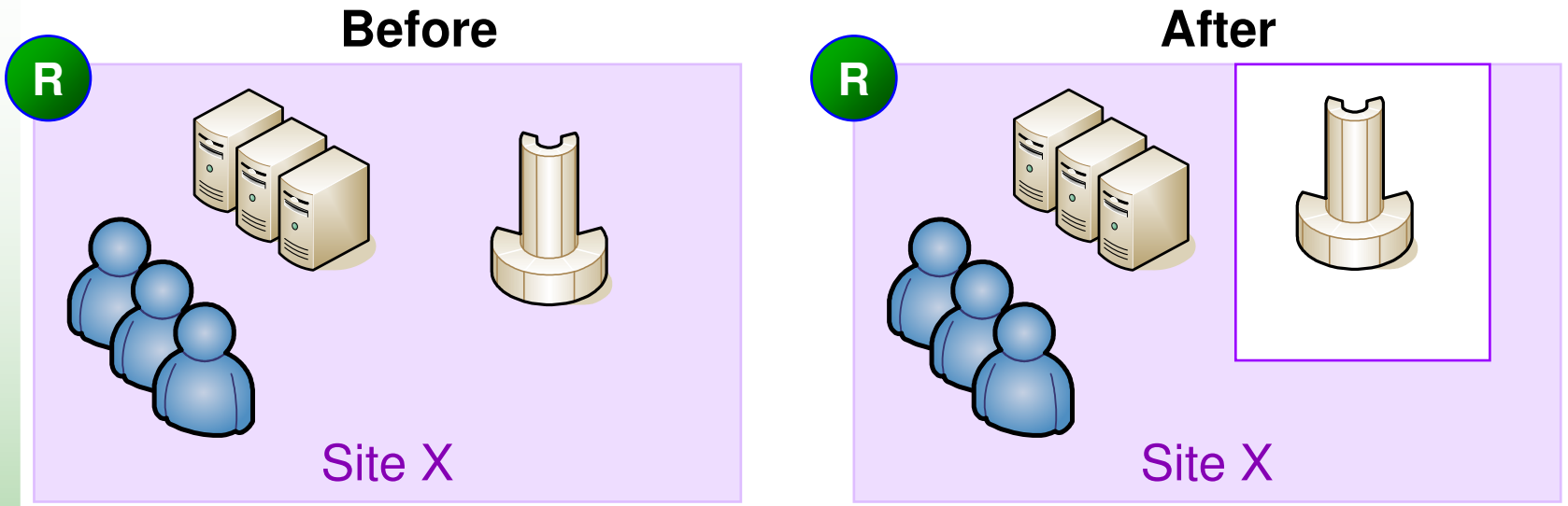


Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Change in site boundaries



Our effective site security boundary is now world wide and limited only by the location of users.

consequently

For effective security we must collaborate with other partners to implement controls to detect and respond to security incidents.

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Prevention: effective security controls

- **Security controls**

  A security control is a means of managing risk. They can include:

Policies	Procedures	Guidelines
Practices	organizational structures	etc.

  Typically administrative, technical or educational in nature they are used to:

  - Protect
  - Detect
  - Respond

  → Against security incidents/events

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Prevention: effective security controls

So how do you implement security controls?

Administrative controls:
The **Security Policy** states that every PC must run a valid anti-virus software product.

Technical controls:
All PCs have anti-virus software on them and they get updates automatically.

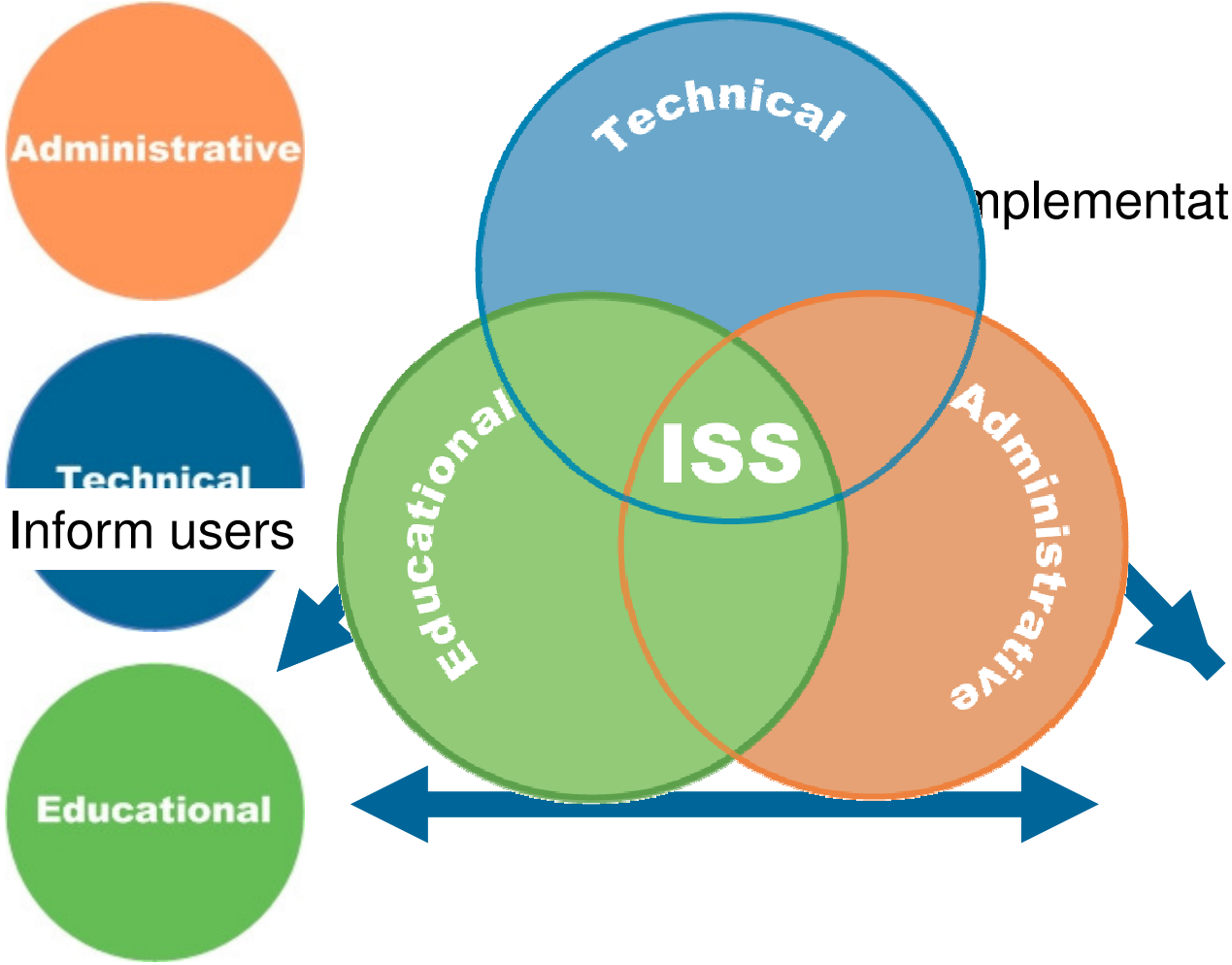
Education:
Explain to users why anti-virus software is on their PC and that they should not turn if off.

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

Concept of Integrated Site Security

In practice:



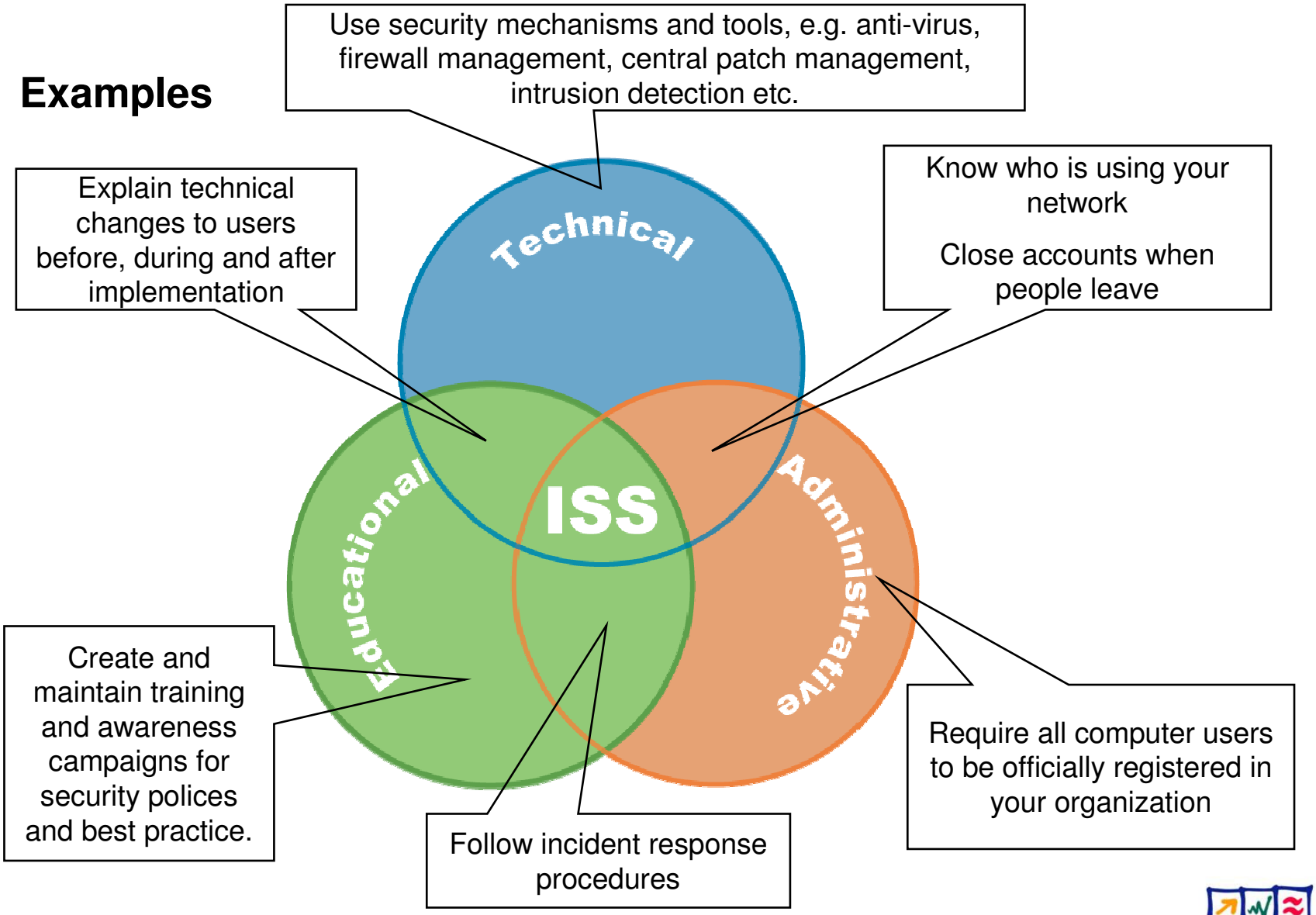
Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Concept of Integrated Site Security

Examples



Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Prevention: selecting security controls

- **Selecting appropriate security controls**

  There are numerous potential security controls that we could use, some appropriate, some not.

  We should establish a “risk assessment” management process to regularly

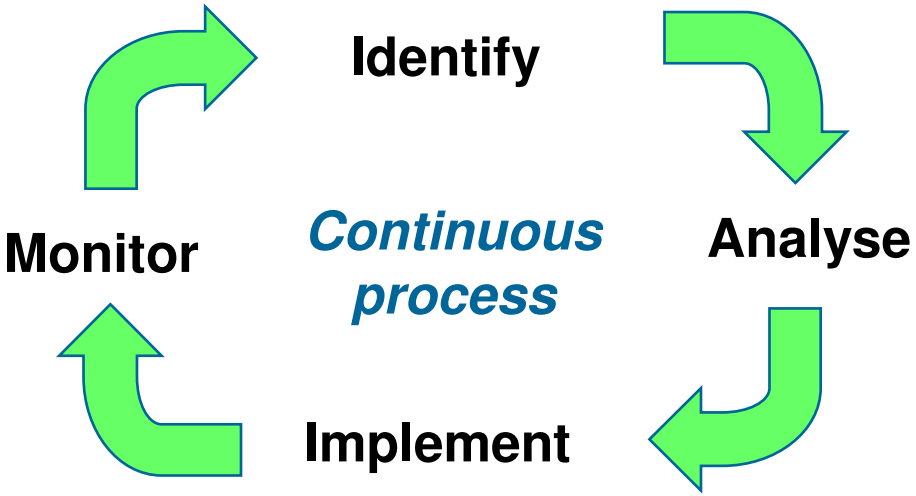
  - Identify what assets or resources are at risk
  - Analyse the impact these resources have on our site
  - Implement any agreed safeguards or controls based on the level of risk we are prepared to accept
  - Monitor that the controls are effective

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Prevention: selecting security controls



Annual improvement plans can be identified and resourced with your help.

Changes within the site are opportunities to develop and enhance our security needs.

This will help demonstrate due diligence and protect our reputation.

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

Summary (1 of 2)

- As Grid use ↑ => the risk of attack ↑ and attractiveness to attack.
- Internal and external individuals may attack us.
- Our effective site security boundary is now world wide and limited only by the location of users.
- For effective security we must collaborate with other partners to implement controls to detect and respond to security incidents.

Appropriate resources need to be allocated to:

- Detect and respond to security incidents appropriately
- Protect you from the potential liability resulting from the action of others
- Protect the reputation of our site within the academic and wider community

Summary (2 of 2)

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

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

- **Questions**