ISSeG

Integrated Site Security for Grids

EU-FP6 Project 026745

What is a 'risk'?

David Jackson, STFC

CHEP 07, Victoria BC, 4 September 2007

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Content

1. **What is a 'risk'?**
2. **Is risk static?**
3. **Are there Grid-specific risks?**
4. **Emerging risks**

Integrated
Site
Security for
Grids

www.isseg.eu

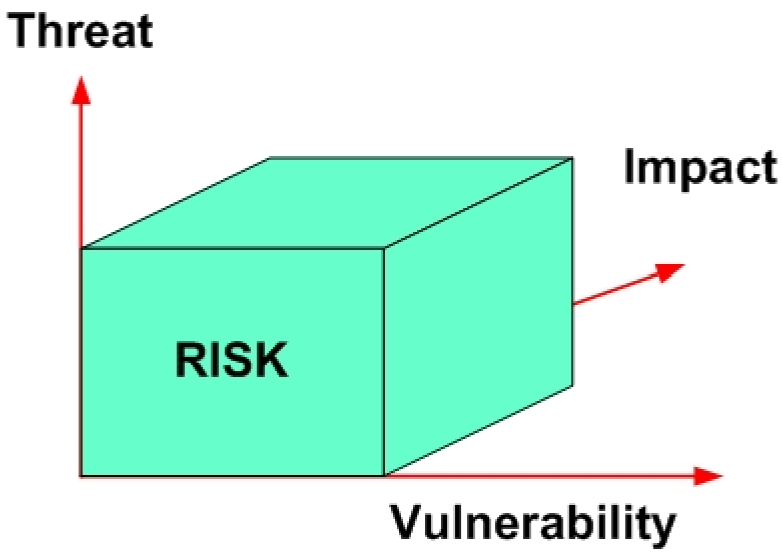
What is a risk?

- **A risk is the potential that some threat may use or exploit a vulnerability to compromise your site and cause you harm.**

> *“the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. It is measured in terms of a combination of the probability of an event and its consequence.”*
>
> *(Section 2.19, ISO/IEC 13335-1:2004)*

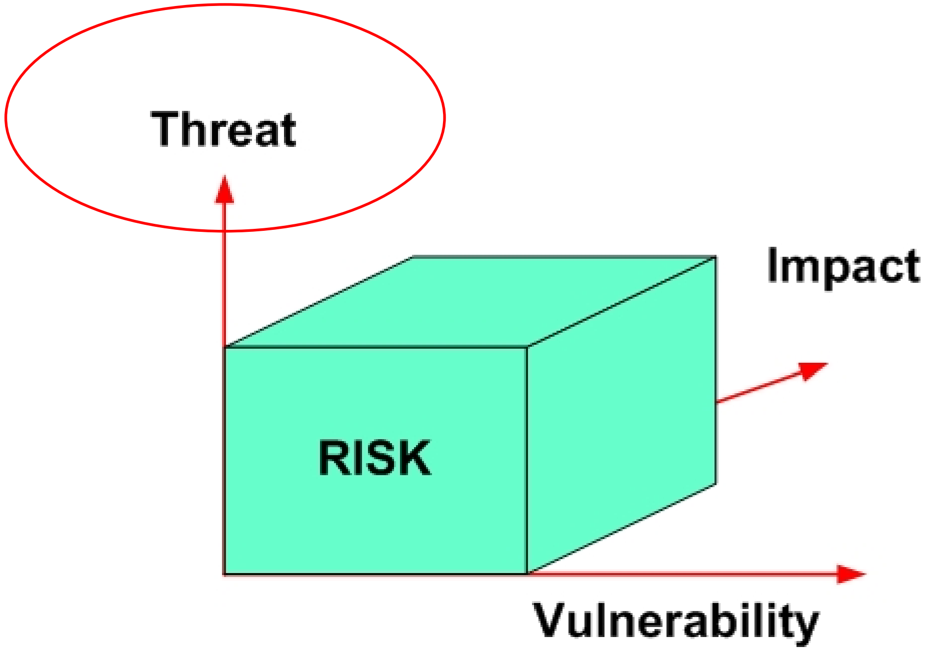
What is a risk?

- **For a risk to exist, three things need to be present:**
  - Threat
  - Vulnerability
  - An impact on an asset (or group of assets)



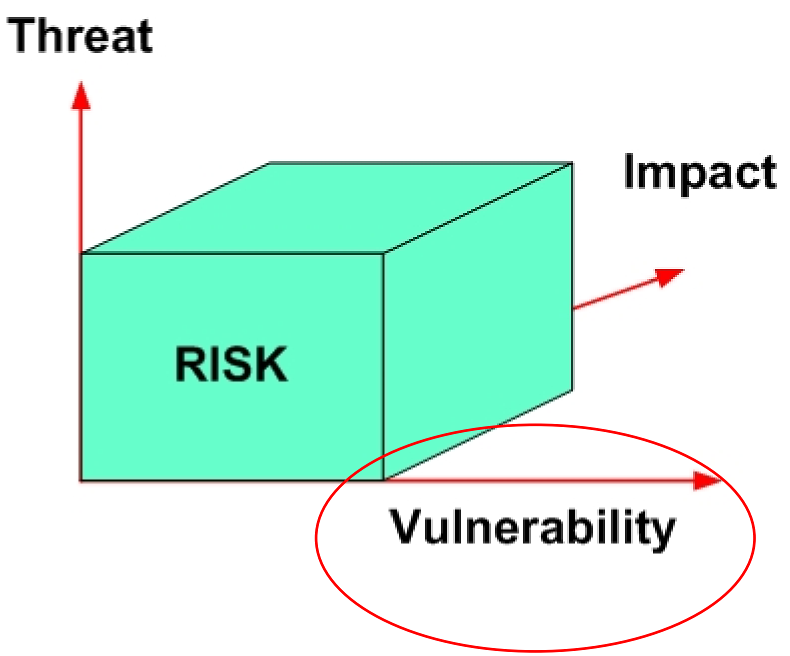
What is a risk?

- **A threat is a person (or event) with the motivation and capability to cause harm to an asset (or group of assets).**



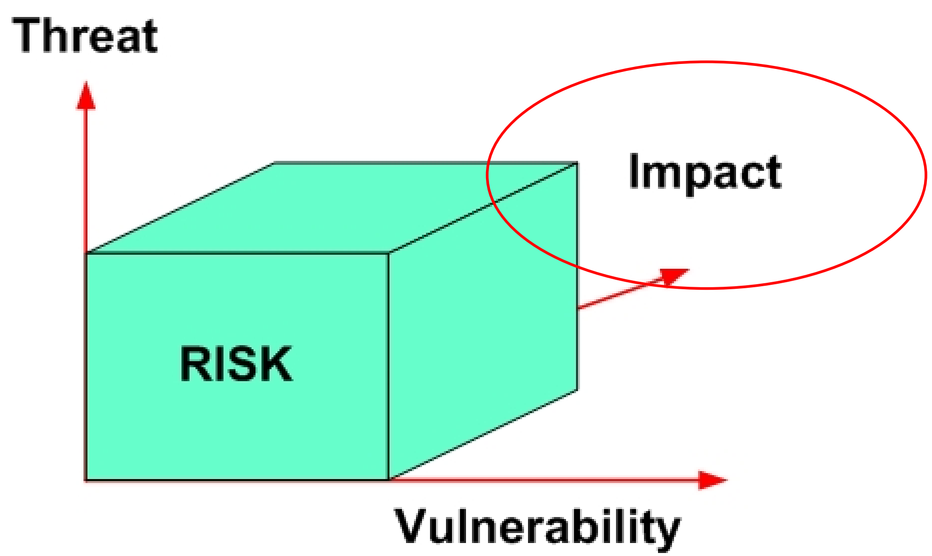
What is a risk?

- **A vulnerability is a weakness within the infrastructure or a management process that can be exploited to expose an asset (or group of assets) to possible compromise or damage.**



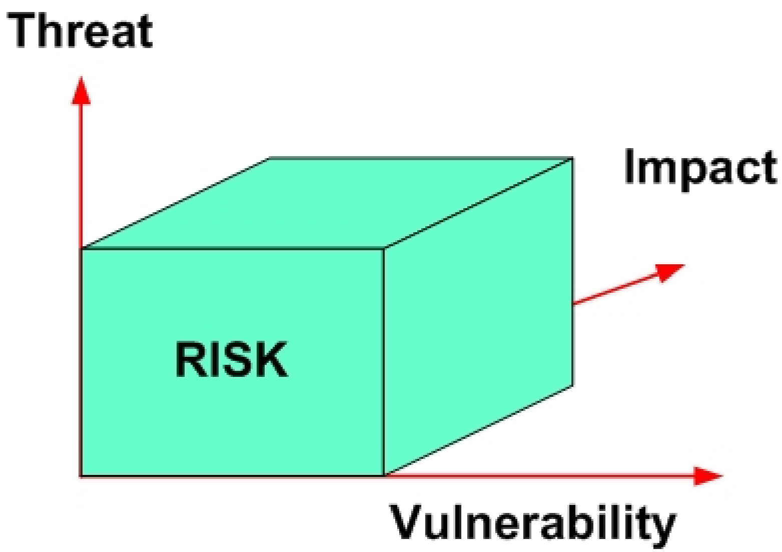
What is a risk?

- The **impact** is the effect on your business.



What is a risk?

- **If you remove any one of the three components of risk, you have removed the risk.**



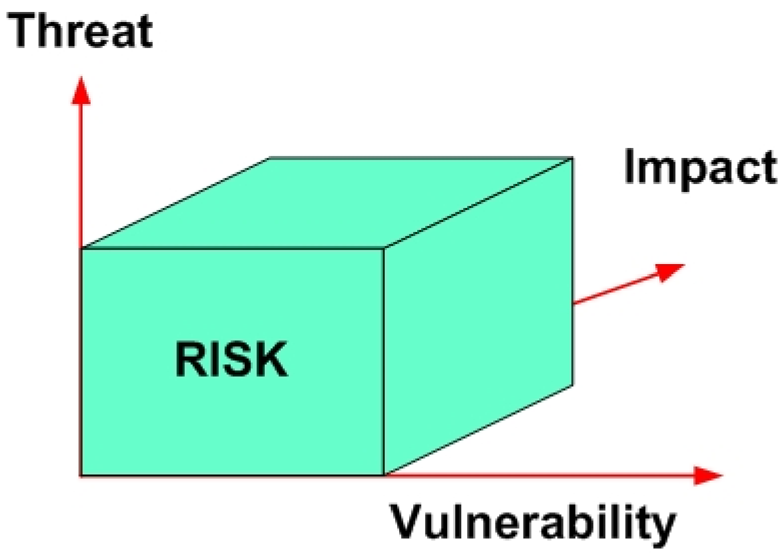
Integrated
Site
Security for
Grids

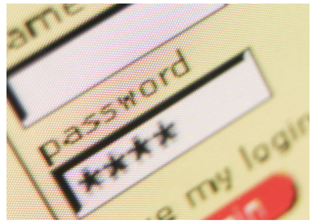
www.isseg.eu

Information Society and Media

What is a risk?

- **Example:** An external attacker used a weak password to gain access to your finance system.





What is a risk?

- **A threat is**

"a potential cause of an incident that may result in harm to a system or organisation."

(Section 2.25, ISO/IEC 13335-1:2004)

"a person (or event) with the motivation and capability to cause harm to an asset (or group of assets)."

(Slide 5)

"something or someone that has the potential to cause you harm"

Example threats

Human		Environmental
Deliberate	**Accidental**	
Eavesdropping Hacking Spam Phishing Theft Social engineering	Errors File deletion Omissions Accidents	Flood Fire Heating Power

Integrated
Site
Security for
Grids

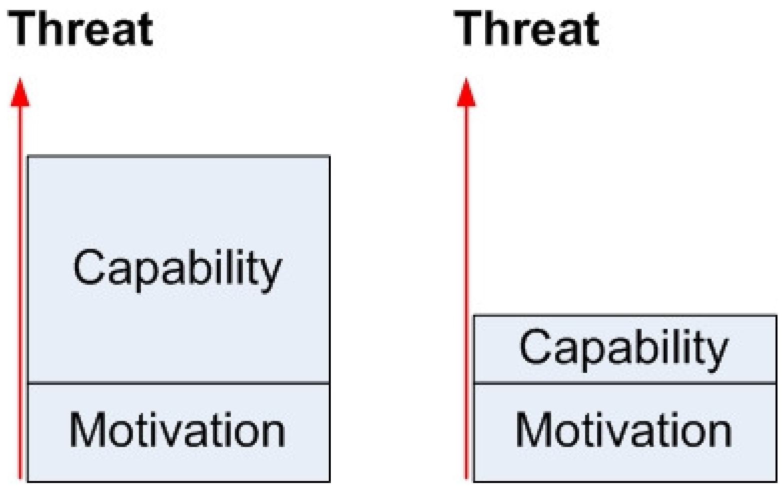
www.isseg.eu

Information Society and Media

What is a risk?

Removing a threat - Human, Deliberate

- **Threats can be from individuals who have the motivation and capability to attack you. If you remove their capability to attack you (e.g. make it more difficult), you are likely to reduce the threat.**

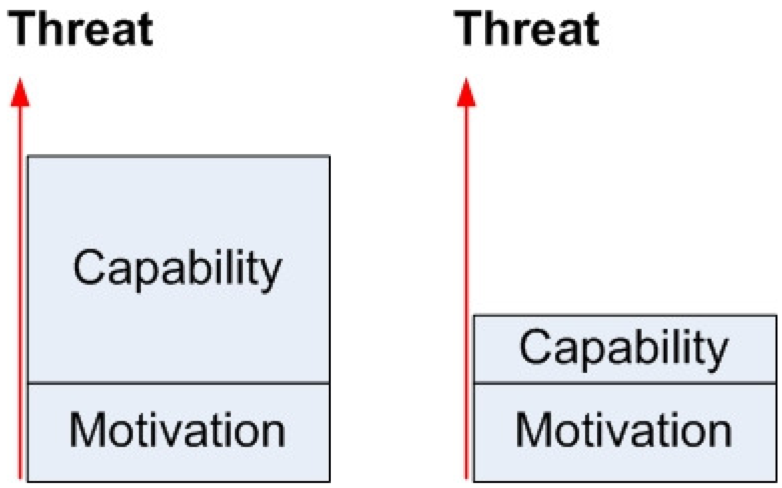


***Example**:*

Use a firewall to restrict access to your site.

Removing a threat - Human, Accidental

- **Individuals are not motivated to cause accidental damage. If you remove their capability to cause an accident (e.g. make it more difficult), you are likely to reduce the threat.**



Example:

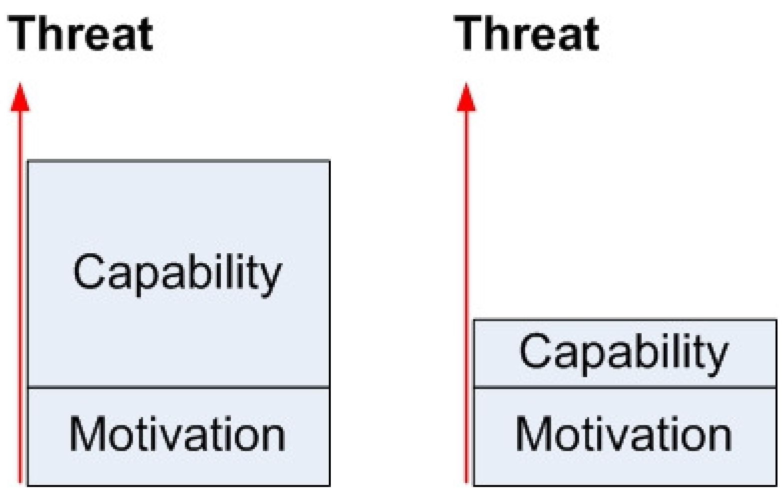
Users to not need to use Root or administrative privilege to access the Internet.

Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

Removing a threat - Environmental

- **Environmental threats have are not motivated to cause damage and are difficult to remove. It is possible to avoid some but not all such threats.**



***Example**:*

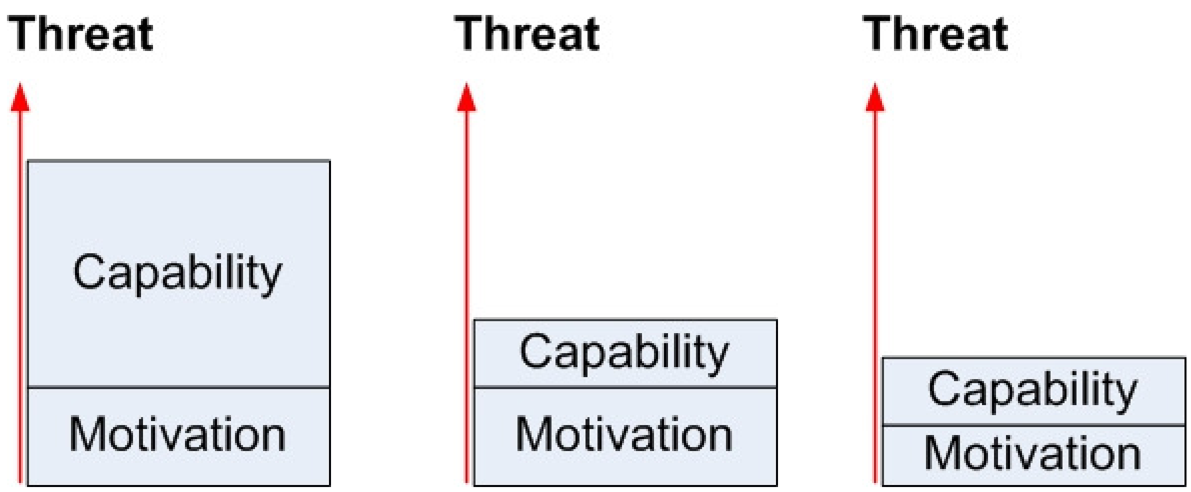
Do build data centres in flood plains near rivers.

Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

Removing a threat

- It is difficult to change the motivation of external attackers. Policies, guidance and training can motivate users to be less of a threat.



Removing a vulnerability

- **Once you know the vulnerabilities within your site, you can remove them.**

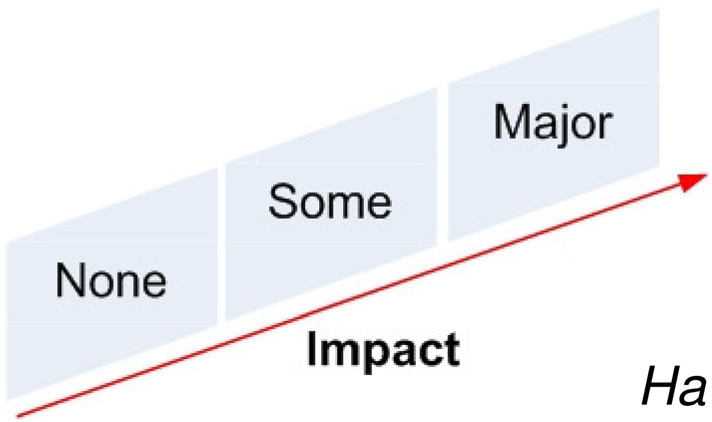
***Example**:*

Keep IT software updated.

Integrated
Site
Security for
Grids
www.isseg.eu

Reducing the imapct

- **Reduce the impact that the potential risk could have on your organization.**



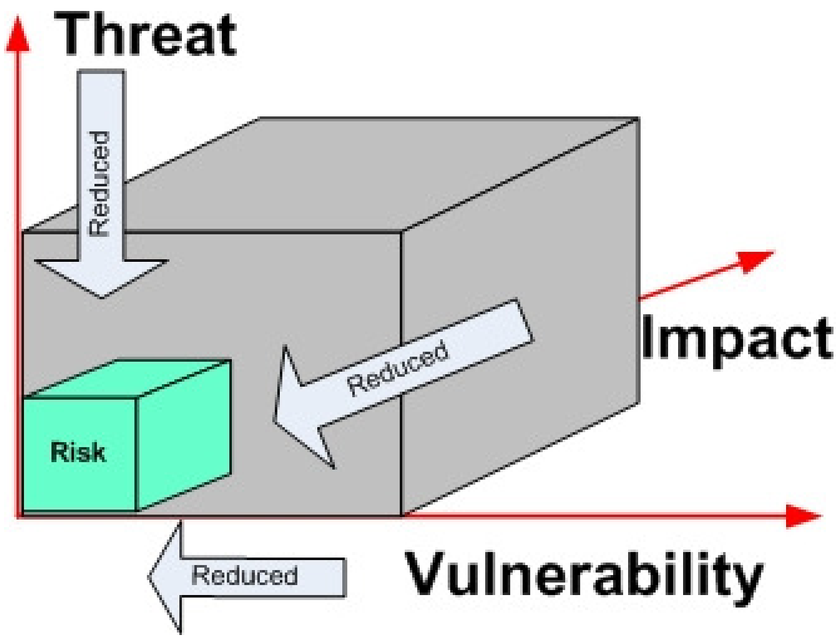
***Example**:*

Have more than one connection to the Internet.

Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

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



***Example**:*

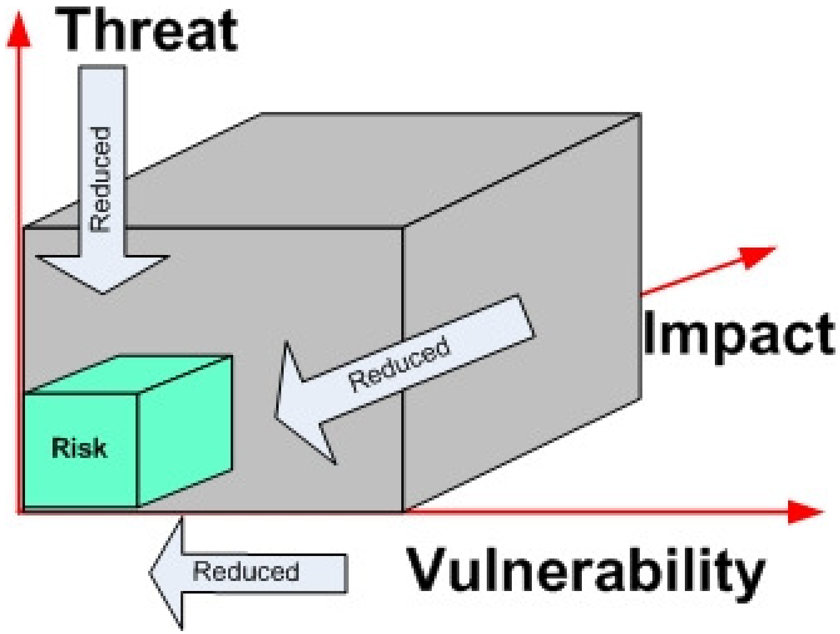
Have more that one connection to the Internet.

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

What is risk?

$$Risk \propto \frac{Threat(C,M).impact(A).Vul.(A)}{Safeguards(A)}$$



So how do you implement security controls?

Administrative

Administrative controls:
The **Security Policy** states that Internet services must be used safely.

Technical

Technical controls:
Site implements a firewall to stop external attackers but allow academic collaboration.

Educational

Education:
Explain to users why there is a firewall (to stop attackers) and how to ask for exceptions (to allow collaboration).

Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

What is risk?

- **Risk is part of everyday life**
- **It gives us opportunities for development**
- **We need to accept some level of risk – you cannot get rid of it all**

1. What is a “risk”?
2. Is risk static?
3. Are there Grid-specific risks?
4. Emerging risks

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

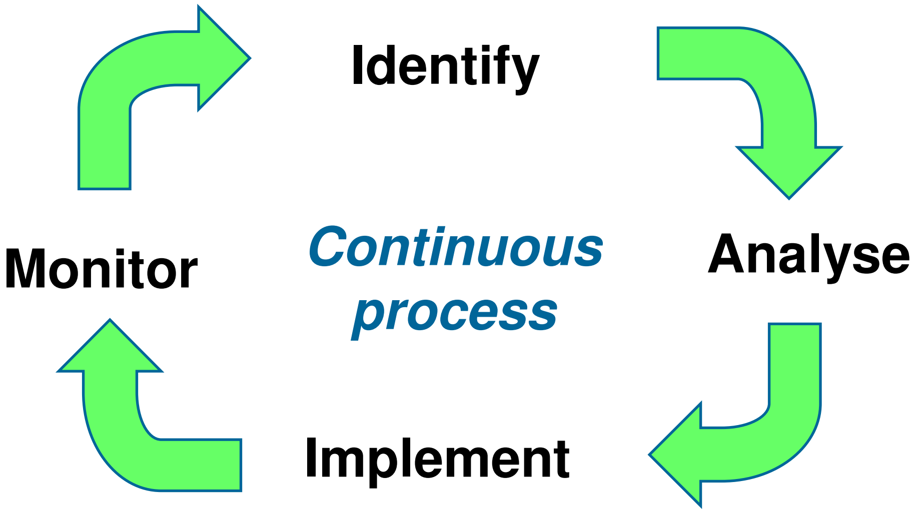
Is risk static?

Once you know the risks, are they static?

- **Administrative changes**
  - e.g. merge with another organization OR join a Virtual Organisation
- **Technical changes**
  - e.g. new patches for PCs/Grid nodes
- **Educational changes**
  - e.g. new users

Is risk static?

- **New** **opportunities** **for science often result in changes at your site.**
- **Sites should use a management process to assess any risk associated with the change. Once you know what you have, you can gauge how much risk you will accept. Commonly called "risk analysis"**



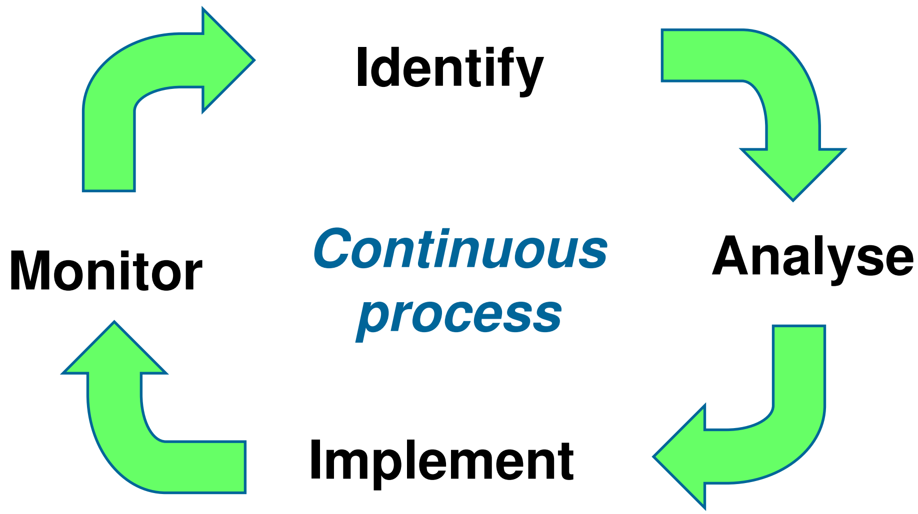
Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Is risk static?

- **Q: Once done, are you "safe"?**
- **A: No. Risk is not static and evolves with time. As such, you must continually (or at least regularly) reassess how much risk you are prepared to accept.**



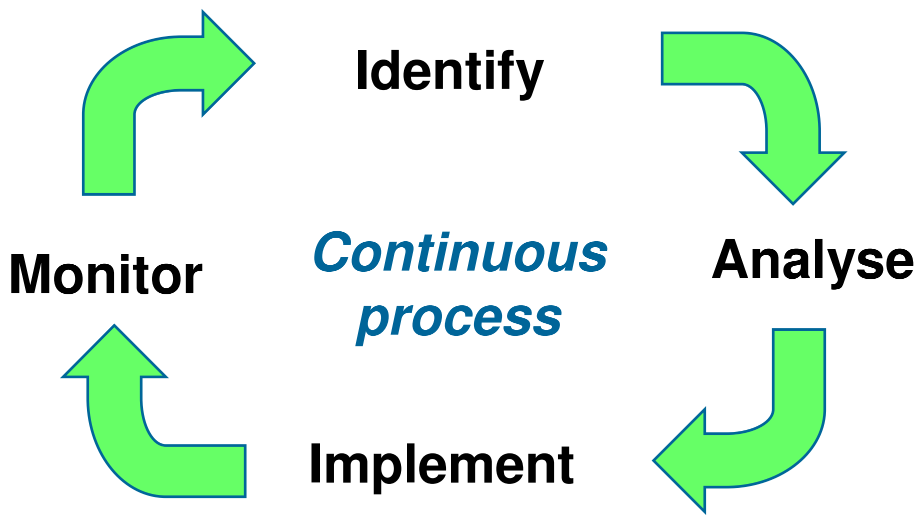
Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Is risk static?

As a natural consequence of your activates (and life) risk levels change, giving opportunities for improvement. Some individuals and organisations accept more risk, some less. If risk is managed, it can be a **positive driver for improvement**. If not, it can be disruptive.



Grid-specific risks

1. What is a “risk”?
2. Is risk static?
3. **Are there Grid-specific risks?**
4. Emerging risks

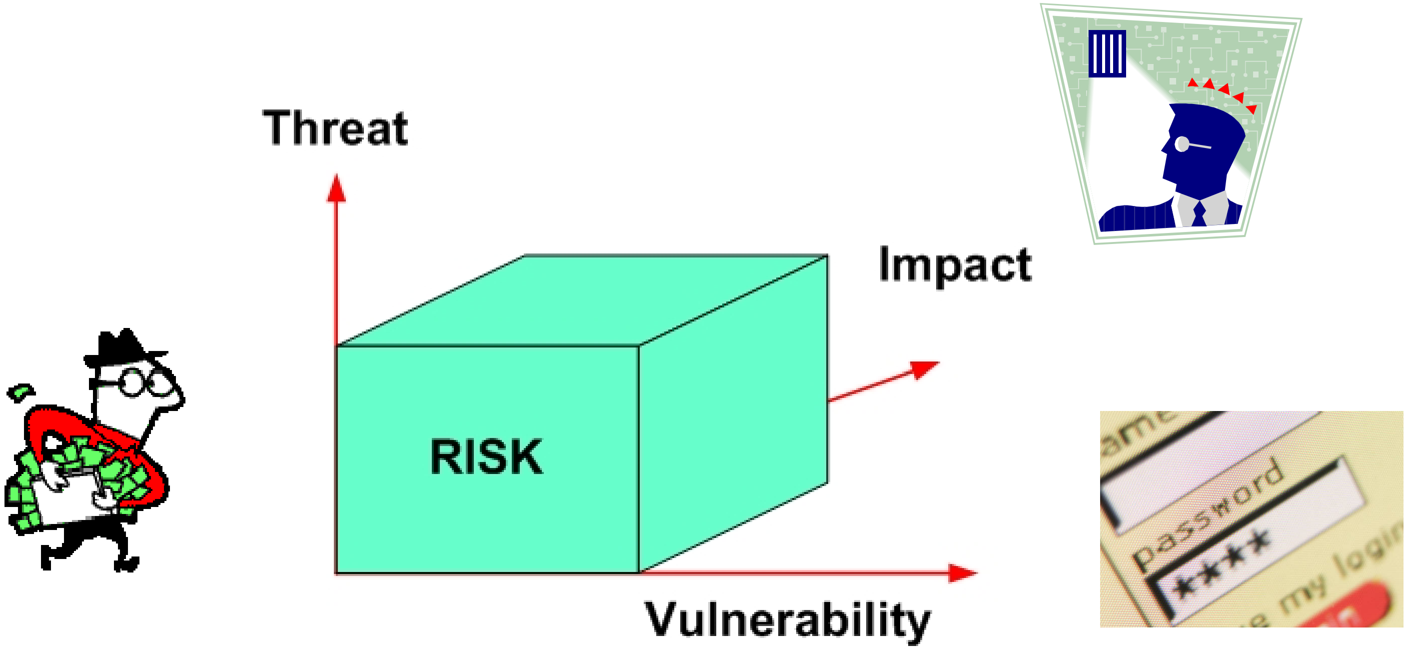
Integrated
Site
Security for
Grids

www.isseg.eu

Information Society
and Media

Grid specific risks?

- **Question:** Are there Grid specific risks?



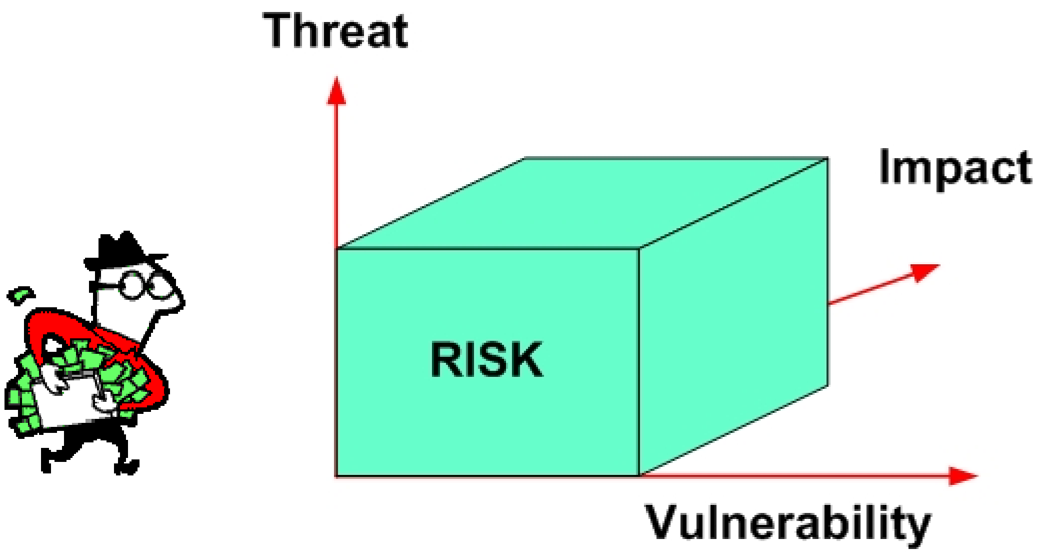
Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Grid specific risks?

- **Threats:** Some attackers are more motivated to attack Grid sites due to large resources.



Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Grid specific risks?

- **Threats:** There is at least one new class of Threat that can cause you harm, the **VO (Virtual Organisation)**.

  VOs have the capacity but **NO motivation** to harm you.

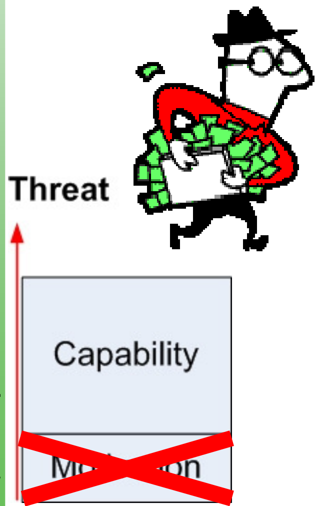
VO's control there own membership

•Researchers join VOs.

•As a site, you no longer know who is using the resources that you host for the VO.

Researchers can offer resources to VOs

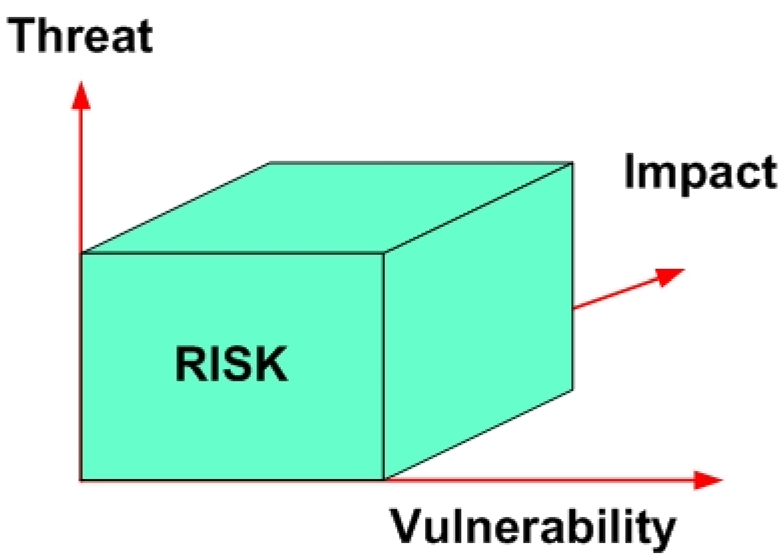
•As a site, do you know what VOs you have in your network?

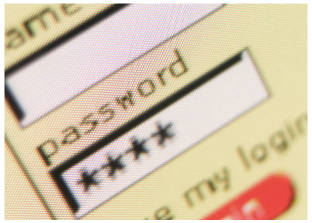


Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

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





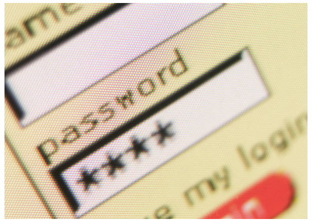
Grid specific risks?

- **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

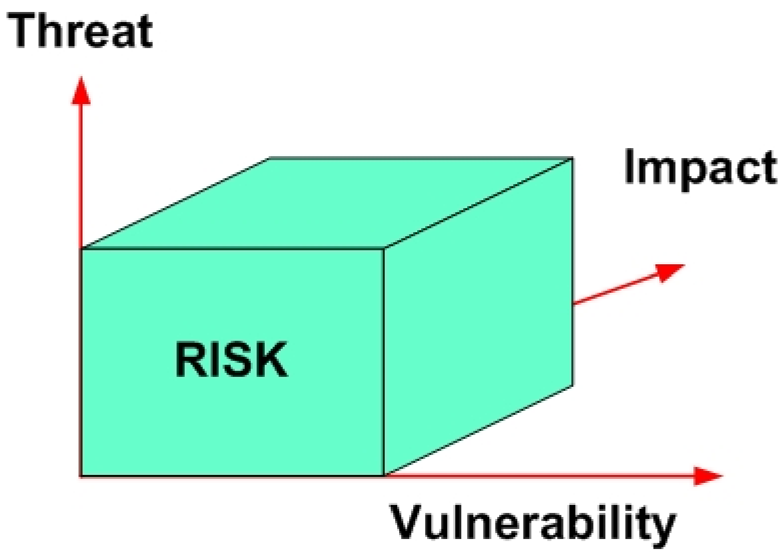
  Users and Activity
  The numbers of both are up. This is increases the probability of an password/pass phrase compromise.



Integrated
Site
Security for
Grids
www.isseg.eu

Information Society and Media

- **Impact:** Turning off the Grid at a site is a measure of last resort. Not impossible, just not probable.



Grid-specific risks

- **At present, only one Grid specific threats has been identified.**
- **By participating in Grid activity, you increase the probability of some risks, but they are not necessary new risks.**
  - *Attractiveness of site as a target*
  - *Number of vulnerabilities*
  - *Number of users*
  - *Level of activity*

Increased

1. What is a "risk"?
2. Is risk static?
3. Are there Grid-specific risks?
4. Emerging risks

Emerging risks

- **Emerging risks are new risks that are likely to arise within the next 3 years. These are in addition to the current risks.**

http://www.enisa.europa.eu/rmra/er_home.html

Emerging risks

Current risks

- SPAM
- Botnets
- Phishing
- Identity theft
- Route hijacking
- Instant Messaging
- Peer-to-peer systems
- Malware on Cell Phones
- Hackers in Stock Market
- Software vulnerabilities
- No protection (e.g. antivirus) in some devices

Emerging risks

- SCADA (Supervisory Control and Data Acquisition)
- Increased home automation
- Turning home appliances on/off
- Massive collections of personal data
- Invisible data collection in public places
- Invisible data collection in private premises
- Security is more an art than a science
- DoS attack on the home telephone
- Hacking home heat and/or air-conditioning system
- Internet users are younger, less experienced and more prone to subtle attacks
- Internet users may not have strong motives to clean up their compromised computers
- Malware over multiple networks (GSM, GPRS, Internet, Bluetooth)

http://www.enisa.europa.eu/rmra/er_home.html

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Summary

- **Risk is a fact of life. Each site has to set and agree what level of residual risk it is able to accept.**
- By being part of a Grid service, you are at risk from electronic attack and compromise**.**
- By managing your risks you **improve your site security** and protect yourself.

- **ISSeG resources:**
  - Training materials
  - Recommendations
  - Generic slides/resources

All available from the www.isseg.eu web site

- **Questions**