Business Application security through Information Risk Management

by Serge Moreno Global IRM

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Agenda

- Why is application security important?
- Information risk management: definitions
- Project: Introduction of IRM in the methodology
- Result: Risk analysis during project lifecycle
- Next steps
- Conclusion / Benefits

Why application security?

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Today's Climate & Challenge

- Rapidly changing information technologies and compressed technology life cycles
- Growing complexity of IT applications and systems and increasing connectivity between systems
- Increased regulatory requirements and raising industry security standards
- New vulnerabilities continue to be found, making the game of catch-up never-ending
- Effective application security is critical for ensuring proper business control
- Security is a transparent issue to many customers – They believe that the services are as safe as it is convenient

- **Bottom line: The best infrastructure defenses are useless if the application is not secured**

Some Statistics

- **"Close to 75% of today's attacks are tunneling through applications."** – Gartner Group
- **The market for Web application security products and services was worth $140 million in 2002, and predicts it to grow at a compound annual growth rate (CAGR) of 65% to $1.74 billion by 2007** - Yankee Group
- **3 out of 4 business websites are vulnerable to attack** – Gartner Group
- **80% of companies report outsider breaches** - IDG.net
- **The average security defect takes 75 minutes to diagnose and 6 hours to fix.** - 5-year Pentagon Study
- **Web application security will be one of the hottest segments of the security industry over the next 5 years** - Yankee Group

The list of Application Attack Techniques Grows Every Day

Top Application Layers & Threats

User	Cross- site Scripting Spoofing/ Trickery Cookie Poisoning
Transport layer HTTP/S	Passive Monitoring Man-in-the-Middle Session Hijack
Web Server	Buffer Overflow Format String Directory Traversal Default Account
Web Application	Filter- Bypass Manipulation SQL Injection Authentication Hijacking
Database	Direct SQL Command Restricted Database Query Database Exploits

Business Impact

- Access to unpublished pages
- Unauthorized app access
- Password theft
- Privacy and Identity theft
- Theft of customer data
- Modification of data
- Disruption of service
- Website defacement
- Recovery and cleanup
- Loss of Customer Confidence

General Aspects When It Comes To Software Projects…

- Security is generally an afterthought
- Developers usually focus on efficient, reusable and bug-free codes rather than secure ones.
- Security is not an inherent part of the process, and is always the first one to be dropped in case of budget constrains.
- Unit Testing & QA testing usually validate only desired behavior & functionality while "neglecting" security issues.
- Development & QA staff suffers from lack of security knowledge.

Our vision

- Our business relies on information
  - Information and information systems are vital to running our business.
  - Information needs to be up-to-date, accurate and reliable
- Need to take the right measures to ensure our information is adequately protected.
- Threats can cause serious business damage
  - Confidentiality (e.g. keeping information secret),
  - Integrity (e.g. validity, accuracy and timeliness) or
  - Availability (e.g. accessibility) of information.
- The consequences of the threats can be extremely damaging for our business.

Information risk management - Definitions

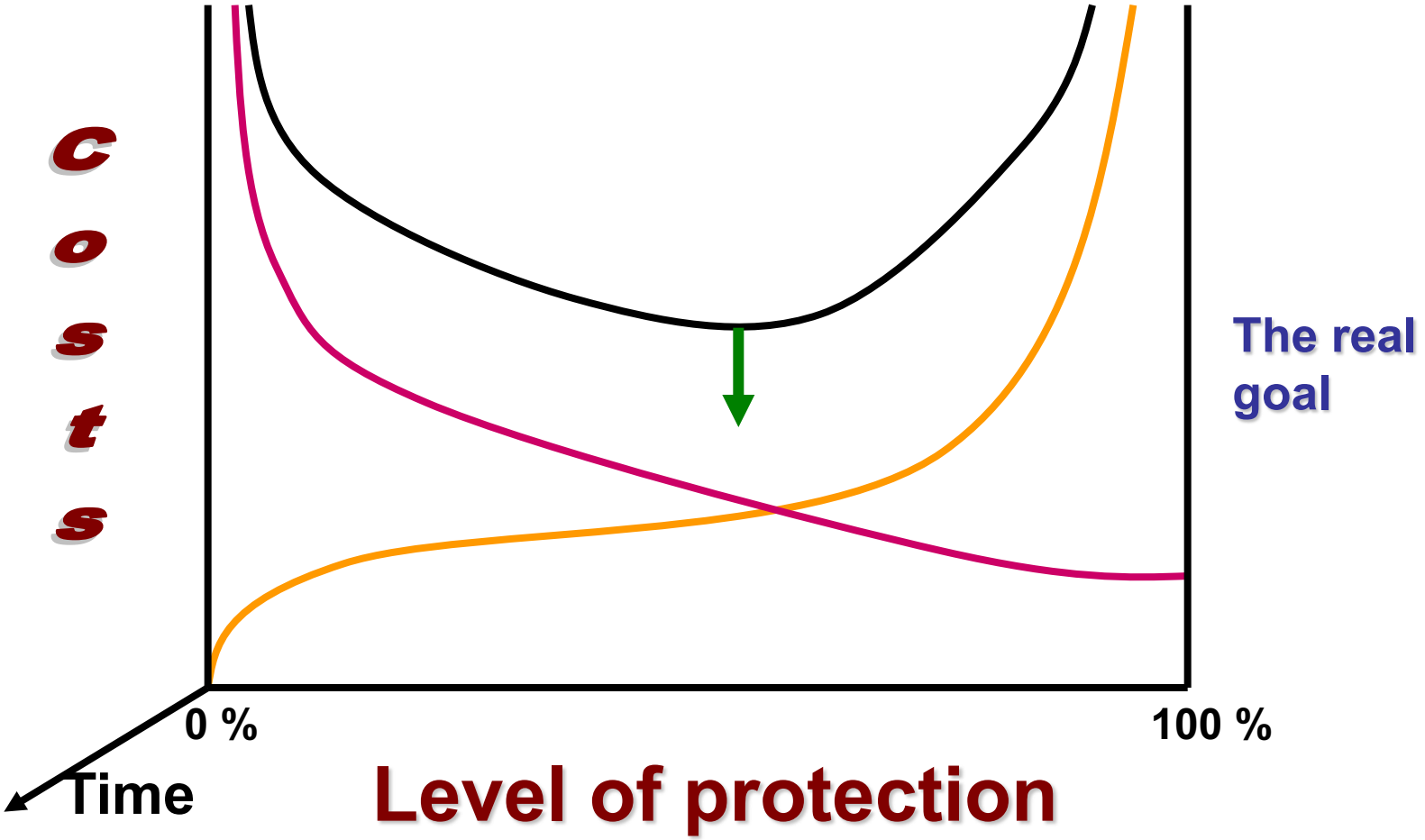
OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Information security or Risk management



Information Risk

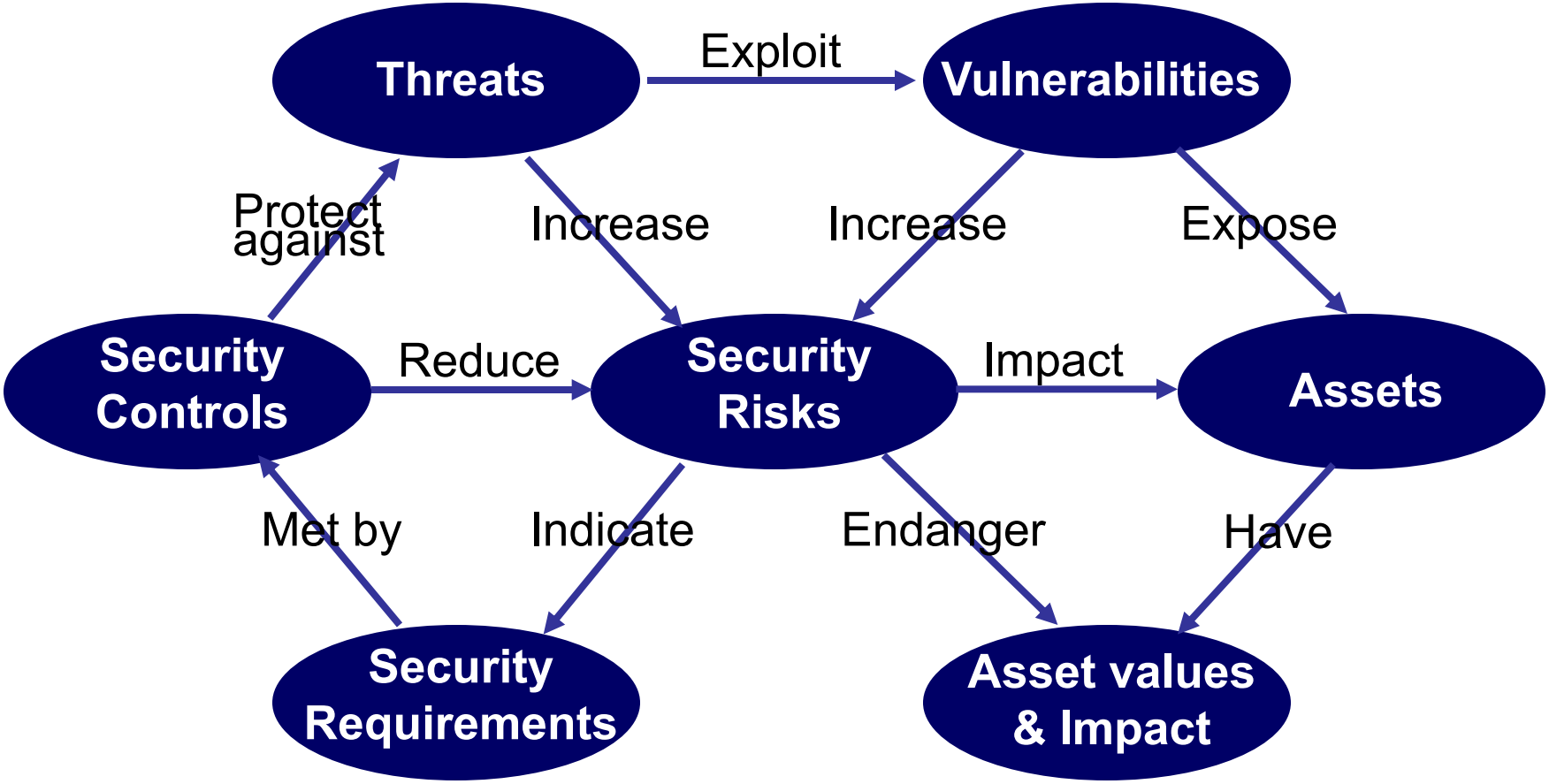
What is information risk?

Information risk can be defined as...

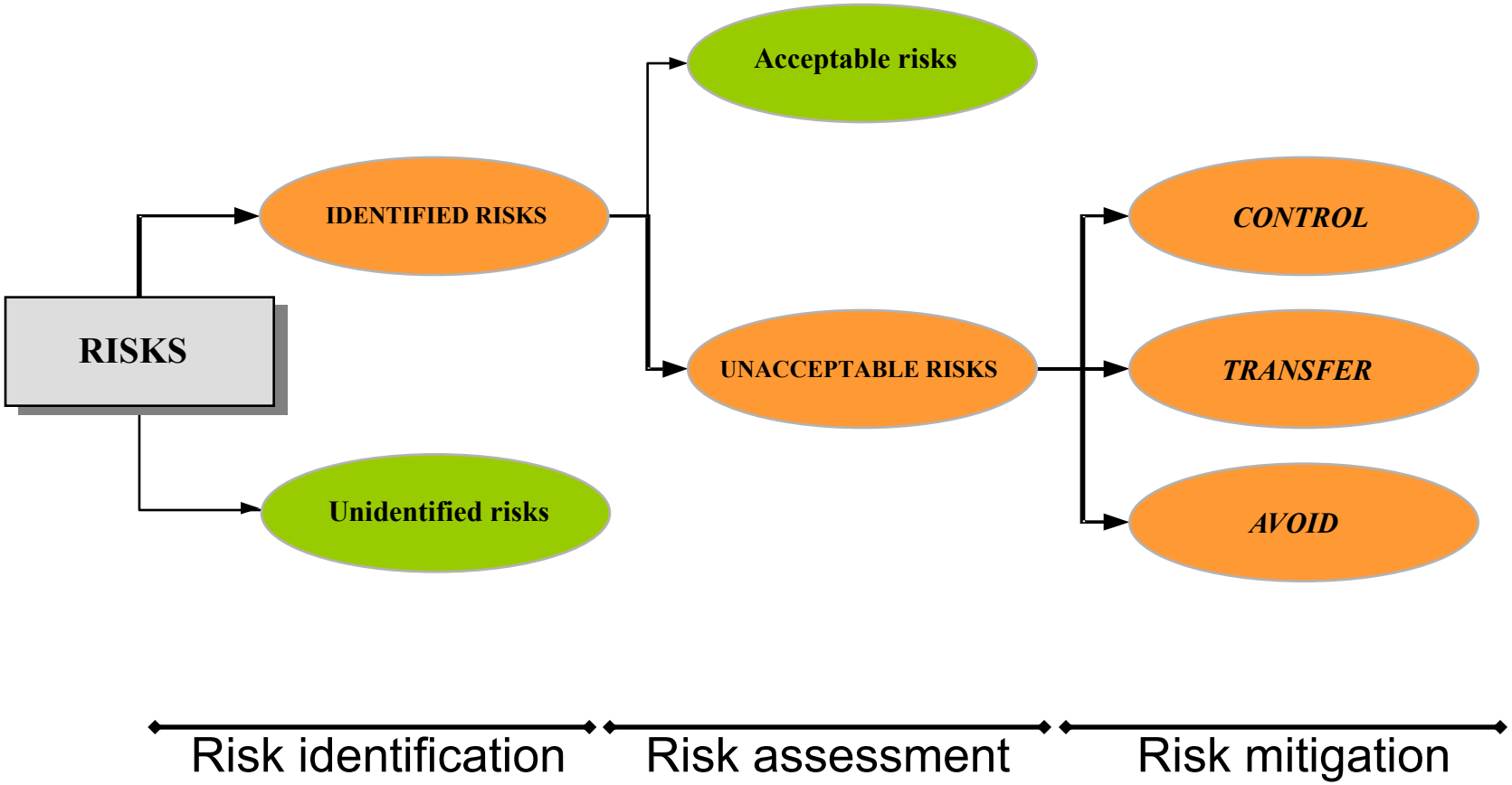
Core concepts

The potential that a threat will exploit a vulnerability to cause harm to the system, to damage the value of an asset and impact the organization business

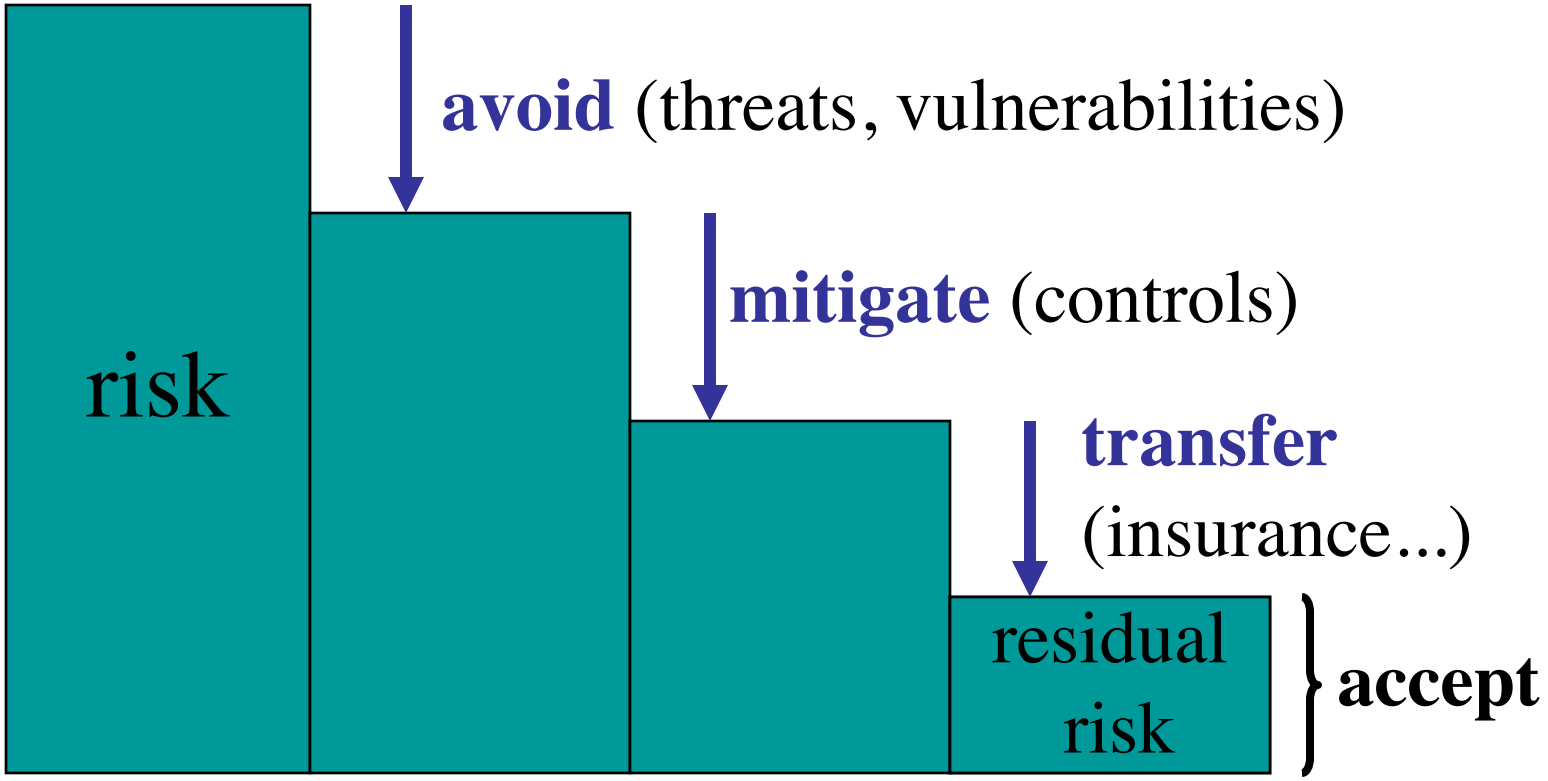
Risk components relationships



Risk Management



Risk Management (cont.)



PROCESS for Risk & Countermeasure identification

- ***Identify*** **all possible risks and risk areas that are of concern and /or need attention which relate to the individual SLC process steps.**
  - **Validate and complete pre defined risks**
  - **Validation risks are correctly categorised**

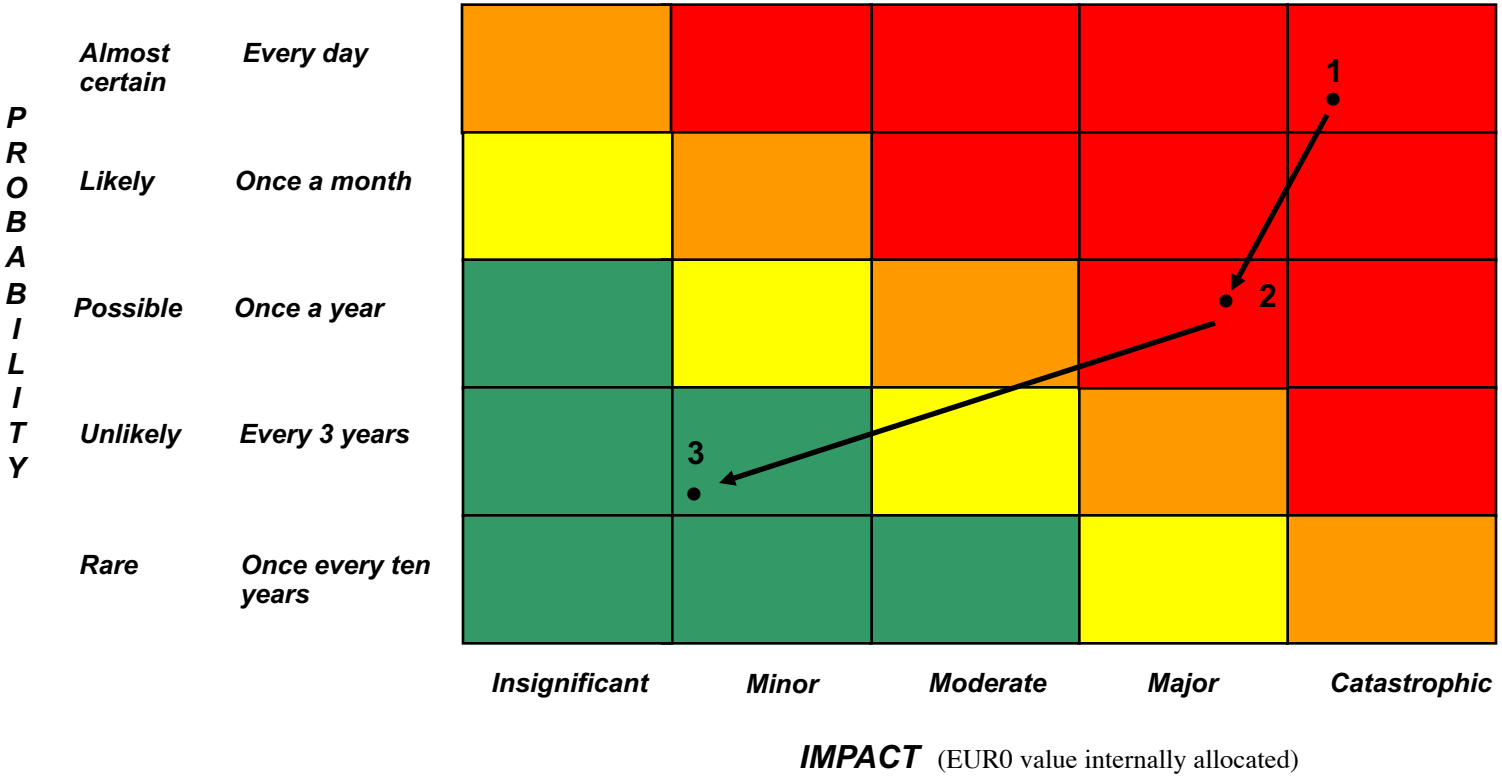
- ***Identify*** **all relevant countermeasures who do exist**
  - **Validate and complete pre defined countermeasure list**
  - **Validation if countermeasures are correctly categorised**

- ***Assess*** **the level of risk of the prioritised risks as identified**
  - **Existing Controls identification & evaluation (adequacy)**
  - **Managed Risk**

- ***Assess*** **the level of risk of the residual risks as identified**
  - **Identification of new actions and new controlmeasures**
  - **Assessment of residual Risk**

PROCESS for Risk & Countermeasure identification (cont.)

LEVEL OF RISK CONTROL MATRIX



1. Level of Absolute Risk (without controls)
2. Level of Managed Risk (with existing controls)
3. Level of Residual Risk (after implementing new controls)

Risk Management (conclusion)

Objectives:

- Identify and analyze the risks associated with the possession and use of information assets within the scope of the assessment
- Analyse the security requirements
- Determine appropriate means to minimize those risks
- Doesn’t include remediation activities

Introduction of Information Risk requirements in the Project life cycle

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

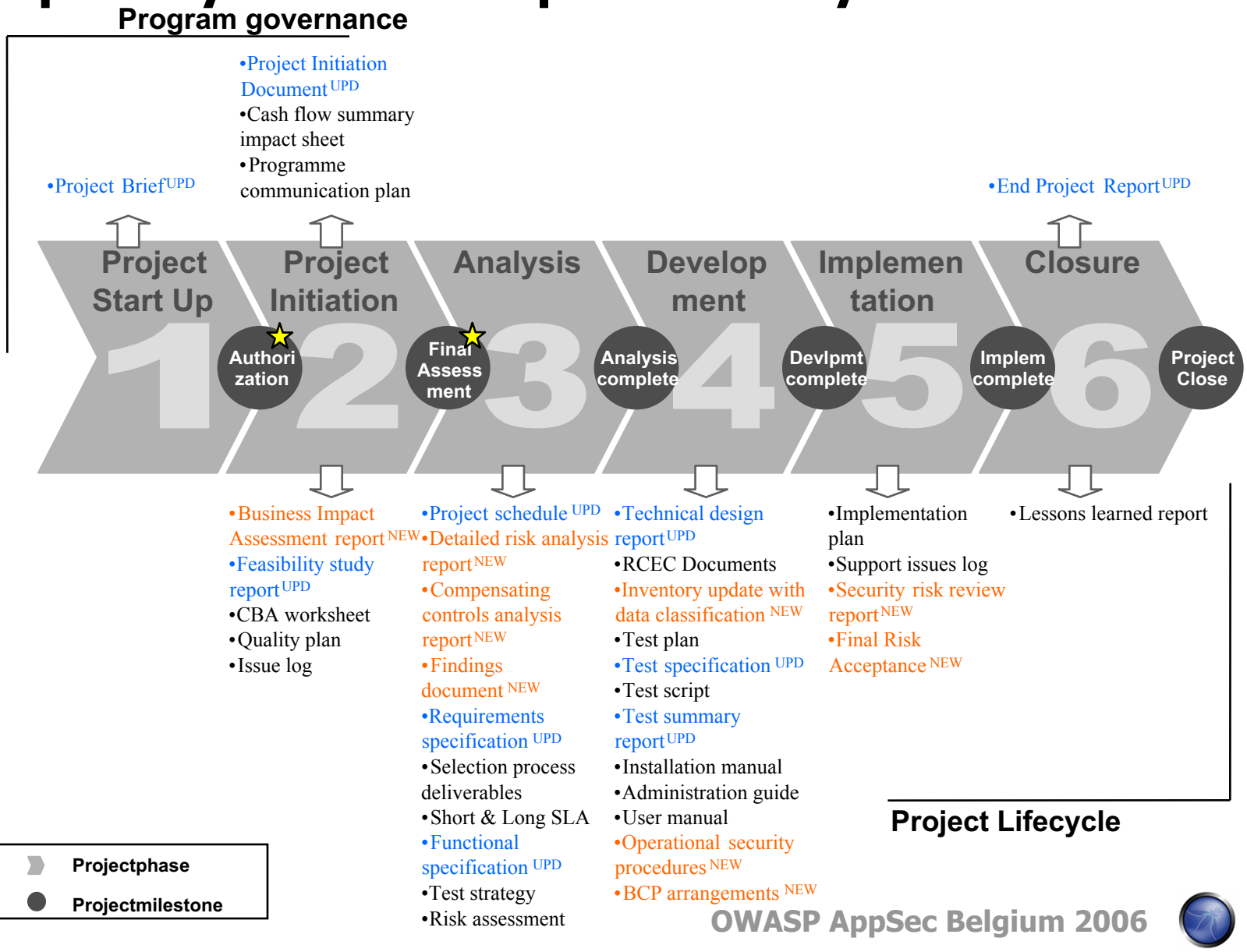
http://www.owasp.org/

Purpose

- Integration of the the IRM requirements into the common steps of the project lifecycle, which should enforce the overall project governance and result in risk governance.

- In order to…
  - Reduce life-cycle costs associated with appropriate protection of sensitive information and systems.
  - Ensure all systems provide an appropriate baseline of protection based on the Group's information security policies and standards.
  - Address application and environment-specific risks using a proactive risk management approach.
  - Harmonization of information risk management approach
  - Compliance with the Group security policies & standards
  - Adhere to ORM (Basel2) principles

Adapted System Development Lifecycle

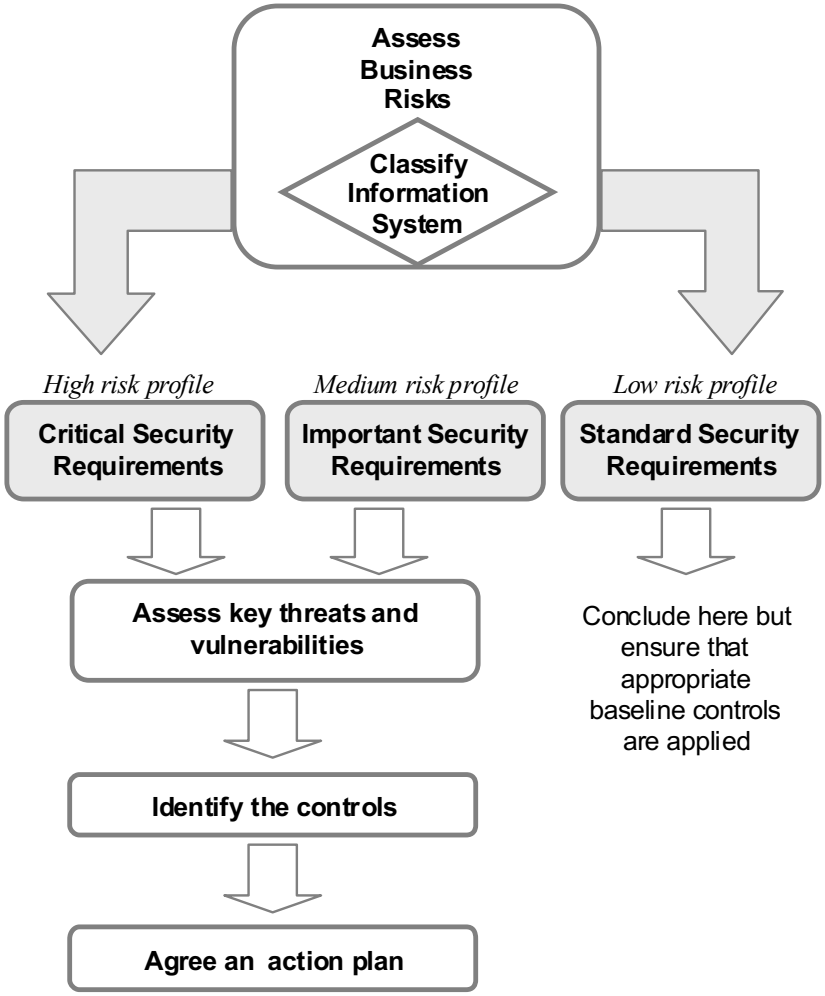


Information Risk Management Process in Project lifecycle

- Business Impact Analysis (BIA)
- Detailed risk analysis (threats & vulnerabilities)
- Compensating controls analysis
- Global action plan
- Security review

Guidelines

Business Impact Assessment provisioned in each project brief.



Guidelines (cont.)

- **Clear criteria for conducting a risk assessment:**
  - **medium or high risk projects (as identified through BIA),**
  - **projects including an external connection (cf. Review Committee External Connections rests on a previously conducted risk assessment),**
  - **e-commerce applications (cf. compliance to policy),**
  - **deviations to Group Information Security policies and standards,**
  - **projects involving new technology (new systems, new products…).**
- **Qualitative and quantitative aspects in analyzing the risks for a single information system (as delivered by the project)**
- **Business activity as a whole already assessed during the BCP risk analysis**

Guidelines (cont.):

- Qualitative & quantitative measures of impact(single IS)

	Qualitative measure	Quantitative measure: potential losses
D	Insignificant/Minor	< 50.000 €
C	Moderate	50.000 <> 1 M €
B	Major	1 M € <> 10 M €
A	Catastrophic	> 10 M €

- Qualitative & quantitative measures of probability(single IS)

	Qualitative measure	Quantitative measure: potential occurrence
D	Unlikely / Rare	Once every 100 years
C	Possible	Once every 10 years
B	Likely	Once every year
A	Almost certain	Every month

⇒ Approval by other bodies as and where appropriate

Risk analysis in Project lifecycle

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Methodology: SPRINT of ISF

- Current risk analysis methodology used across the enterprise
- Simple and formal method for analyzing the business risks associated with an Information System and for agreeing what safeguards or controls are necessary

ISF : Information Security Forum

Risk analysis in details
Summary

- **The risk analysis is guided by a** co-ordinator **working in conjunction with the** business manager **responsible for the system under review.**
- **A typical breakdown of the effort involved in preparing for and conducting a SPRINT review is as follows:**

Phase	Co-ordination	Business manager
1- Assess business risks	½ day	1-1 ½ hours
2- Assess threats, vulnerability and controls	½ day	3-4 hours
3- Produce agreed action plan	1 day	½-1 hour

Co-ordination= Account Manager / Project manager & IRM
Account Manager/Project Manager: initiation & follow-up
IRM role: support & review & approval

Next Step

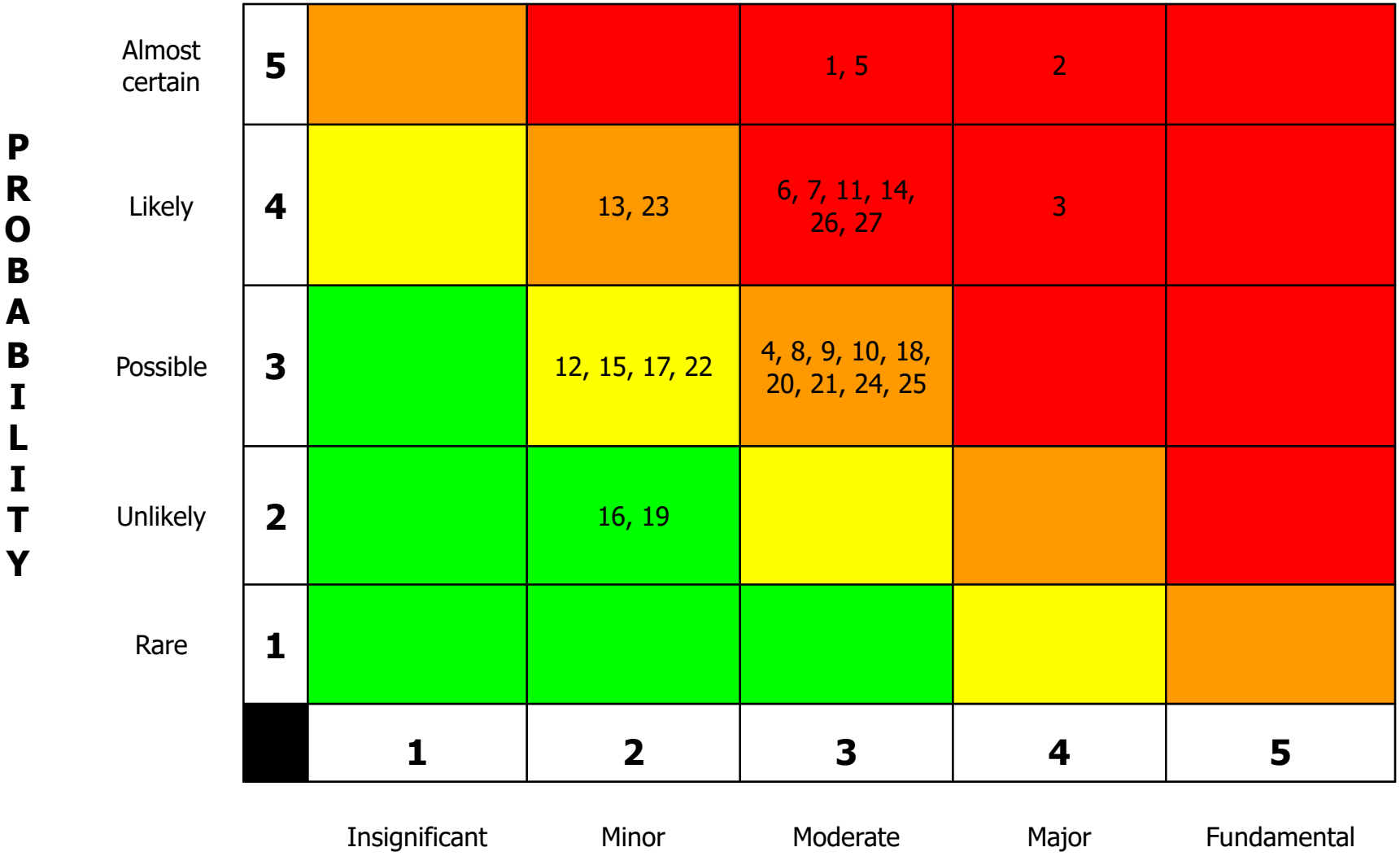
OWASP AppSec Belgium

Sept 2006

Evaluation of degree of assurance

- Meetings with key stakeholders from business and application development teams
- Workshops to identify Risks, existing countermeasures, new countermeasures
- Clustering of Risks and existing/new countermeasures
- Build relationship table between countermeasures and risks
- Evaluation by stakeholders of managed risks (taking into account existing countermeasures)
- Evaluation by stakeholders of residual risks after implementation of different sets of countermeasures (3 options)
- Validation of options / proposed roadmap with key stakeholders

Current Risk Ranking



Future of application security

- Awareness campaign to business managers and sponsors
- Closer involvement of application development teams in general security strategies
- Development of Standardised Security Review and clearly defined associated security measures
- Imposed sign-off of residual risks by business and IT under supervision of IRM
- Development of a security architecture framework
- Secure coding guidelines
- Implementation of approved DTAP (Development, Test, Acceptance, Production) environment strategy

- Code reviews
- Documentation standards & guidelines
- Disposal & de-commisioning specialists

Conclusion / Benefits

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Benefits

- Common approach to risk management within project governance and the project lifecycle
- Improved security support for Project Managers
- Greater visibility of security requirements to Sponsors
- Company-wide, consistent coverage of security requirements within projects, resulting in:
  - an appropriate level of security measures and cost across the board.
  - reduced levels of vulnerabilities.
  - economic value to the company due to reduced risk exposure.
- The company will be better positioned for future audits and visits by relevant regulatory bodies.
- Security measures are no longer add-ons (i.e. in later project phases) but are fully integrated into the functional requirements and therefore part of the final product.
- Awareness by the Business of the residual risk, which has to be accepted and managed.

Question time

Serge Moreno

Global Information Risk Management
Business Application Security
Amsterdam, Netherlands

Thank you!

Annex : extra definitions

OWASP AppSec Belgium

Sept 2006

The OWASP Foundation

http://www.owasp.org/

Information Risk (cont.)

- Threat

  Circumstance or set of circumstances that is likely to cause an incident, and in this case a possible event that could comprise the confidentiality, integrity or availability of information associated with an IT-based information system.

- Vulnerability

  Factor which affects the probability of a threat materializing.

Information Risk (cont.)

- Risk

  A risk is realized when a threat takes advantage of a vulnerability to cause harm to your system.

- Business impact

  Extent of disruption caused by an incident occurring and what effect the business consequence will have on organization.

- Assets

  Collective term covering information and associated IT facilities.