



Information
Security Society
Switzerland
> *vormals FGSec*

Introduction to Security Architecture

30.9.2008, SAS Hotel Radisson, Luzern

ISSS Security Architecture Working Group

Tobias Christen, Beatrice Gruber, Roland Portmann, Lukas Ruf, Anthony Thorn

Speaker: Anthony Thorn, AT Systems & Services GmbH

ATSS

Version 2, 12.9.08

Types of Security Architecture

Three types with some features in common and some overlap.

Product or Technology Security Architecture

A product security architecture will typically confine itself to the security properties of that product. Thus the Common Data Security Architecture (CDSA) describes how security services are provided in a layered model.

Enterprise Security Architecture

An enterprise security architecture needs to address applications, infrastructure, processes, as well as security management and operations.

Application or Project Security Architecture

An application security architecture lies between the two. It must address not only the security provided within the applications, but also the additional (compensating) controls which are required outside the application. The latter are sometimes more important and almost always harder, to specify and implement.

Definitions

The term security architecture is interpreted very differently from organisation to organisation.

*Traditionally a security architecture is a document, which specifies **which security services are provided how and where, in a layered model**. Originally the model typically referred to OSI layers and specified the security elements or services and the mechanisms used to provide them.*

*Our understanding of Security elements has **expanded** to include for example Vulnerability management, Patch management, Identity Management and many more.*

Gestaltung

*A Security Architecture is a cohesive security **design**, which addresses the **requirements** (e.g. authentication, authorisation, etc.) – and in particular the risks– of a particular environment/scenario, and **specifies what security controls are to be applied where**. The design process should be reproducible.*


Design principles will usually be stated explicitly.

Interfaces are important

Detailed specifications of security controls are often found in separate documents.

Definition Summary

A “basket” of Controls (countermeasures), which:

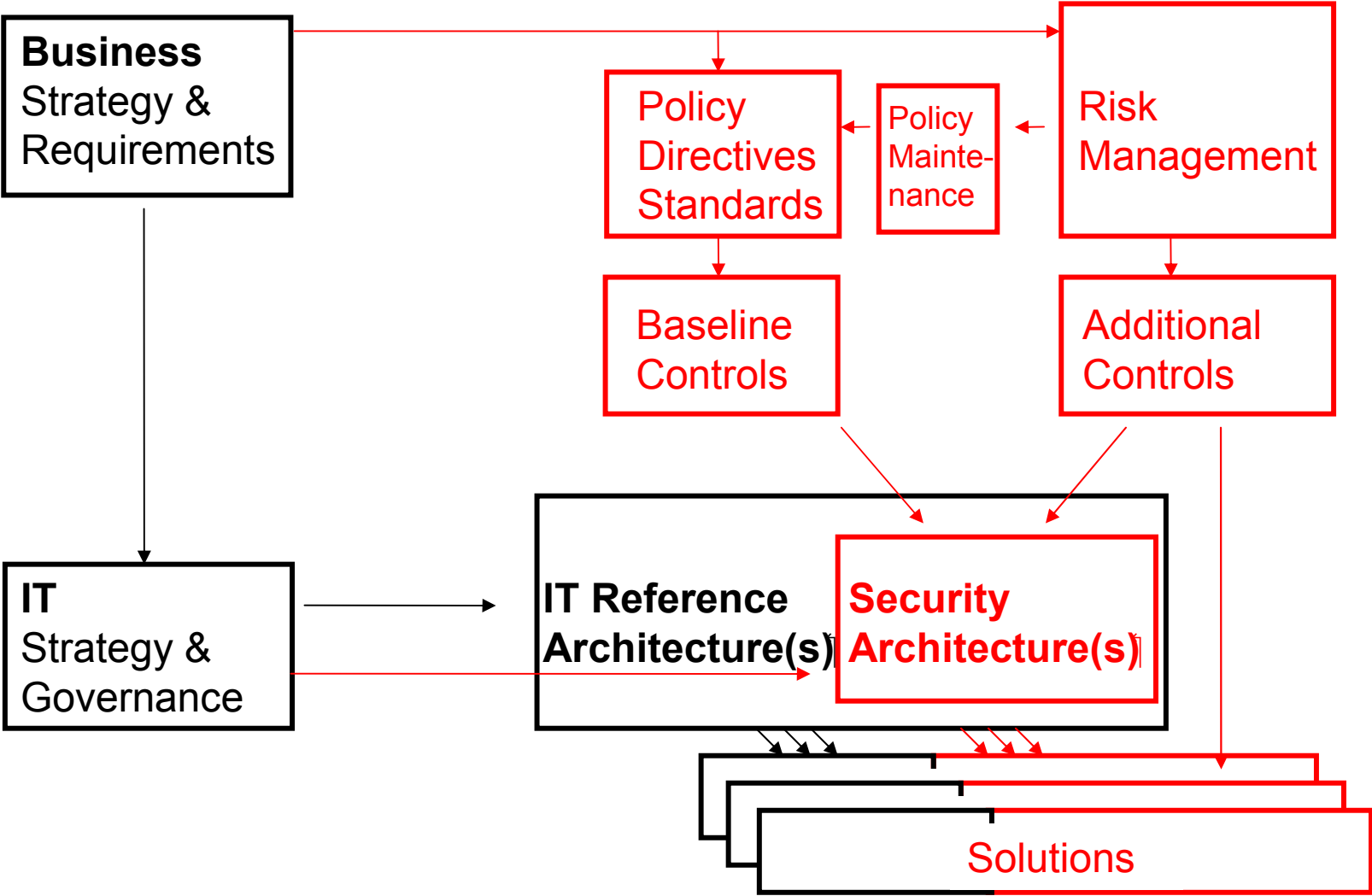
- is designed to meet requirements of a particular Scenario
- includes **design principles**
- involves **Risk management**
- has a **structure**
- addresses the **relationship between the components** (interfaces).
- *Layered models are very common* 

Properties of a Security Architecture?

In addition to the definition we consider

- 2. Relationships and dependencies**
- 3. Benefits**
- 4. Security Drivers**
- 5. Some examples**

Security Architecture Model



Explanation of Diagram

*Designing a security architecture should be a response to Business strategy and requirements.
The IT Strategy should be a response to the Business strategy and requirements.
The IT Reference Architecture(s) should be a response to the IT Strategy and Governance. The reference architecture will usually address multiple platforms.*

The Reference Security Architecture(s) is part of the IT Architecture even if it is published as a separate document.

IT Security Risk Management, process and criteria. Are derived from the Business strategy and requirements.

*A set of Baseline Controls is generated based on the Security Policy, Directives, Standards etc. By Baseline Controls we understand **mandatory minimum standards** for the organisation. Input comes from the legal/regulatory environment, Benchmarking and published security “good practice” etc. see section 5 below.*

Additional controls are derived from the Risk management process.

The security Architecture is the embodiment of the baseline and the additional security controls. It can also be defined to include the policies, directives, standards and the risk management process.

Some organisations use the term solution architecture to refer to the specific implementations derived from the reference architecture.

This diagram reflects the different interpretations of Security Architecture identified by the members of our working group.

Benefits of a Security Architecture?

Two categories:

- 1. Cost Effectiveness, Efficiency**
- 2. Communication**

Cost Effectiveness through standardisation

This is common to any IT Architecture.

The cost-effectiveness improvement stems from the re-use of the controls specified in the architecture,

In addition to the implementation cost, we can expect:

- **Easier, better cheaper implementation resulting from economies of scale**
- **Re-use of skills of support staff, application developers, analysts, (and sometimes users).**
- **Re-use of management interfaces**
- **Faster Implementation** *(last but not least!)*

in addition there are some special security benefits.

Security Benefits

Re-use of standard modules is particularly important for security, because an excellent security control can be nullified by an apparently trivial implementation error.

*Easier, better, cheaper **compliance checking***

*Easier, better, cheaper **effectiveness measurement**
(IS 27001)*

Fast Track approval

In large organisations an IT security approval is required as part of project governance. Typically a “triage” will be performed in order to identify candidate projects for a detailed risk analysis, while for “harmless” projects a high-level analysis is sufficient. In such an organisation compliance with a security (and an IT) architecture will provide a “fast track” to security approval.

Communication

An architecture helps to ensure that specialists separated by distance or time, share a **common understanding** of terminology, requirements and solutions.

Similarly for a complex system a security architecture is essential to ensure that developers working on different sub-systems, understand the **relationship of their contribution to the whole, and what security requirements their product must meet.**

Security Drivers

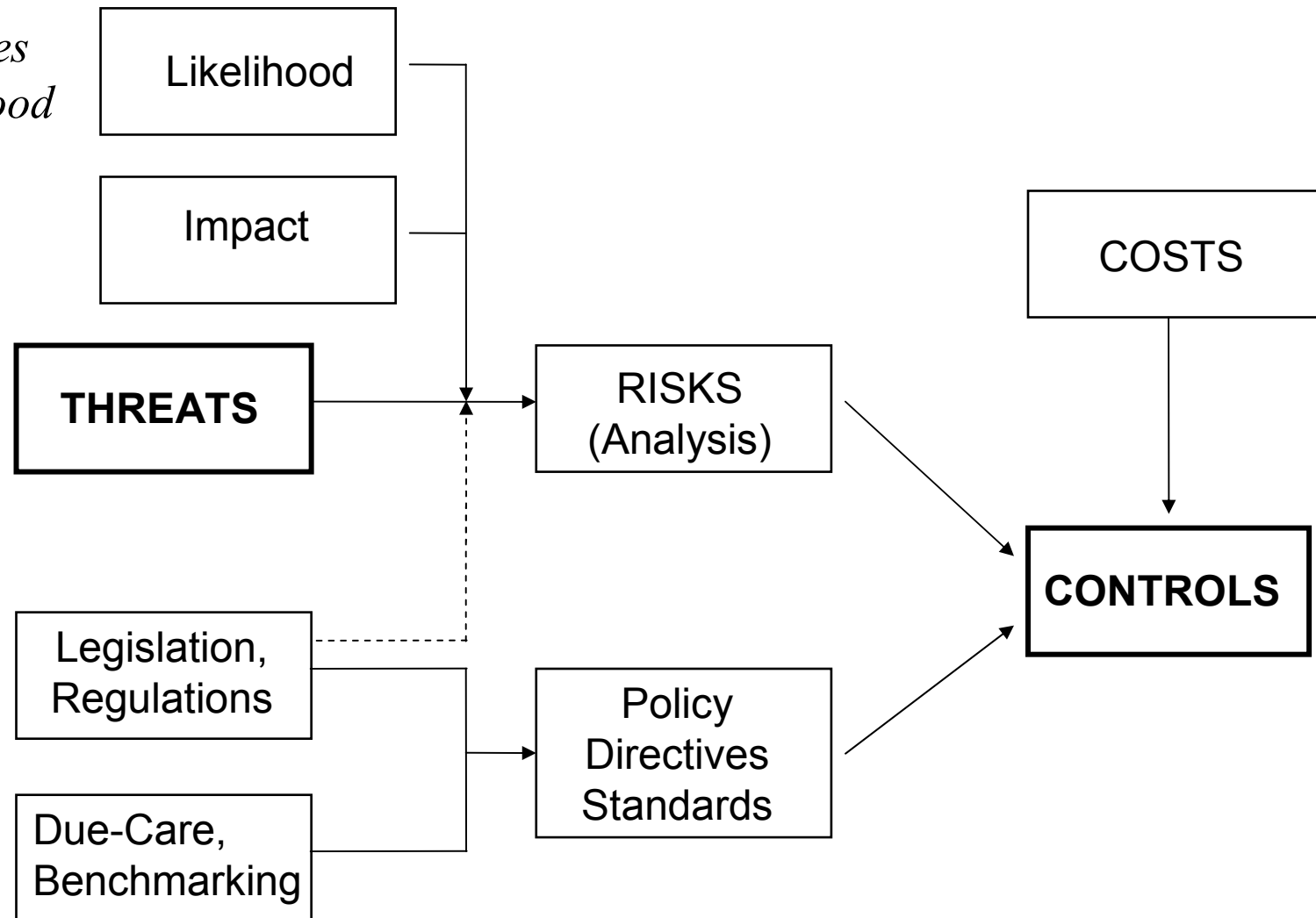
Because a Security Architecture is a basket of controls, we should understand why controls are adopted, in addition to the benefits of having an architecture.

*Despite the prevailing doctrine,
Not all controls are Risk based.*

Risk is important, but the drivers can usefully be grouped into 4 categories

Threats & Controls Model

*Vulnerabilities
affect likelihood*



4 Security Drivers

1. Financial

This is a financial cost/benefit analysis – ROI or ROSI

2. Address Risks (*like Insurance*)

The risks which we are not prepared to accept.

3. Due-Care

Decisions based on benchmarking & published baselines, also audit reports and external reviews.

4. Legal / Regulatory

Requirements imposed by customers or suppliers also come into this category.

Each of these drivers on its own is potentially sufficient...

Security Driver 1

Financial

The financial driver is “return on investment” (ROI) – although it may be measured as; NPV (Net Present Value), IRR (Internal Rate of Return), etc. Quite simply the cost after implementing the control is less than if the control had not been implemented.

Where the risk is included in the calculation – i.e. values for the risk with and without the control are used- this is called “ROSI”.

Some security controls can be cost effective even without taking the reduction of risk into account. e.g. less help desk calls, as a result of a “self-service” password reset included in an identity management project.

*Note that this is **not** the same as risk management, although it is applied in the selection of controls in the risk management process.*

Security Driver 2

Risk Management

*Risk management is a process, which identifies risks and selects an appropriate treatment. The reason for managing risks is to make the **total cost of adverse incidents predictable**. Here total cost means the sum of the impact of the incident and the cost of controls intended to mitigate (or transfer) the risk.*

Note that the priority in risk management is the (estimated) magnitude of the risk, and not the expected cost saving through treatment (see above). We may well be prepared to pay a premium over the annualised loss expectancy for this predictability.

By risk management we mean analysing the risk, comparing the estimated risk with pre-defined criteria and trying to find appropriate controls to mitigate risks, which exceed the “acceptable” level (“high risks”).

This is the same reasoning for a private person buying accident insurance.

Even though he expects the cost of insurance over the years to exceed the actuarial risk, he pays the premium for “peace of mind”. I.e. we prefer to pay X every year for ten years rather than (e.g.) “only” 9 times X once in ten years.

Note that detailed risk analyses are resource intensive, and where relevant actuarial / statistical information is not available the estimate degenerates to guesswork (also known as expert opinion!).

Security Driver 3

Benchmarking & Good Practice

Many controls are specified because they are included in (authoritative) published standards, or because peer organisations use them.

Again the specific controls may not be cost effective in the particular environment, but few security officers will want to expose themselves, as well as their organisations, by not implementing (or at least putting a tick in the box for) a control, which constitutes “recognised good practice”.

This is also referred to as “due diligence” or famously by Bruce Schneier as “CYA” (cover your ass). However in fairness there is huge uncertainty about the magnitude of certain risks –especially the most improbable category- and so in certain cases it may be impossible to be sufficiently confident that a control is not justified.

Security Driver 4

Legal and Regulatory

Obviously we should all obey the law of the land, but this category also includes, for example, banking regulations, Federal Drug Authority requirements, etc. as well as controls specified in contracts with suppliers or customers, e.g. to connect with their order and logistic systems.

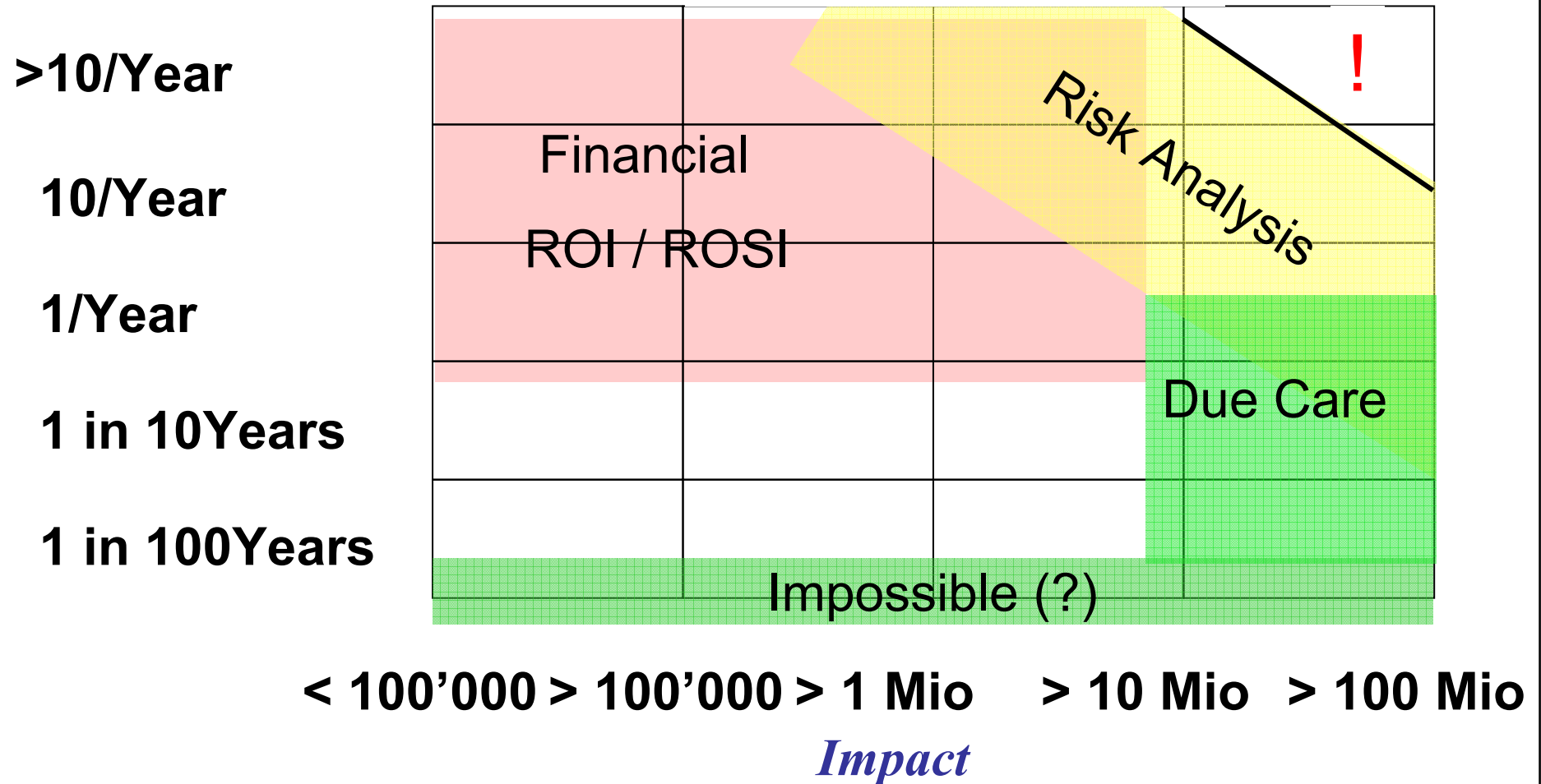
For a multi-national organisation ensuring compliance in every country in which they operate is anything but straightforward.

What ought to be the easiest decision (“just do it!”) becomes a major challenge.

Risk Landscape

NB. arbitrary units

Likelihood



Examples

The following examples are provided only as illustration.

Our group does not endorse them.

Examples

<http://www.rites.uic.edu/csaw/>

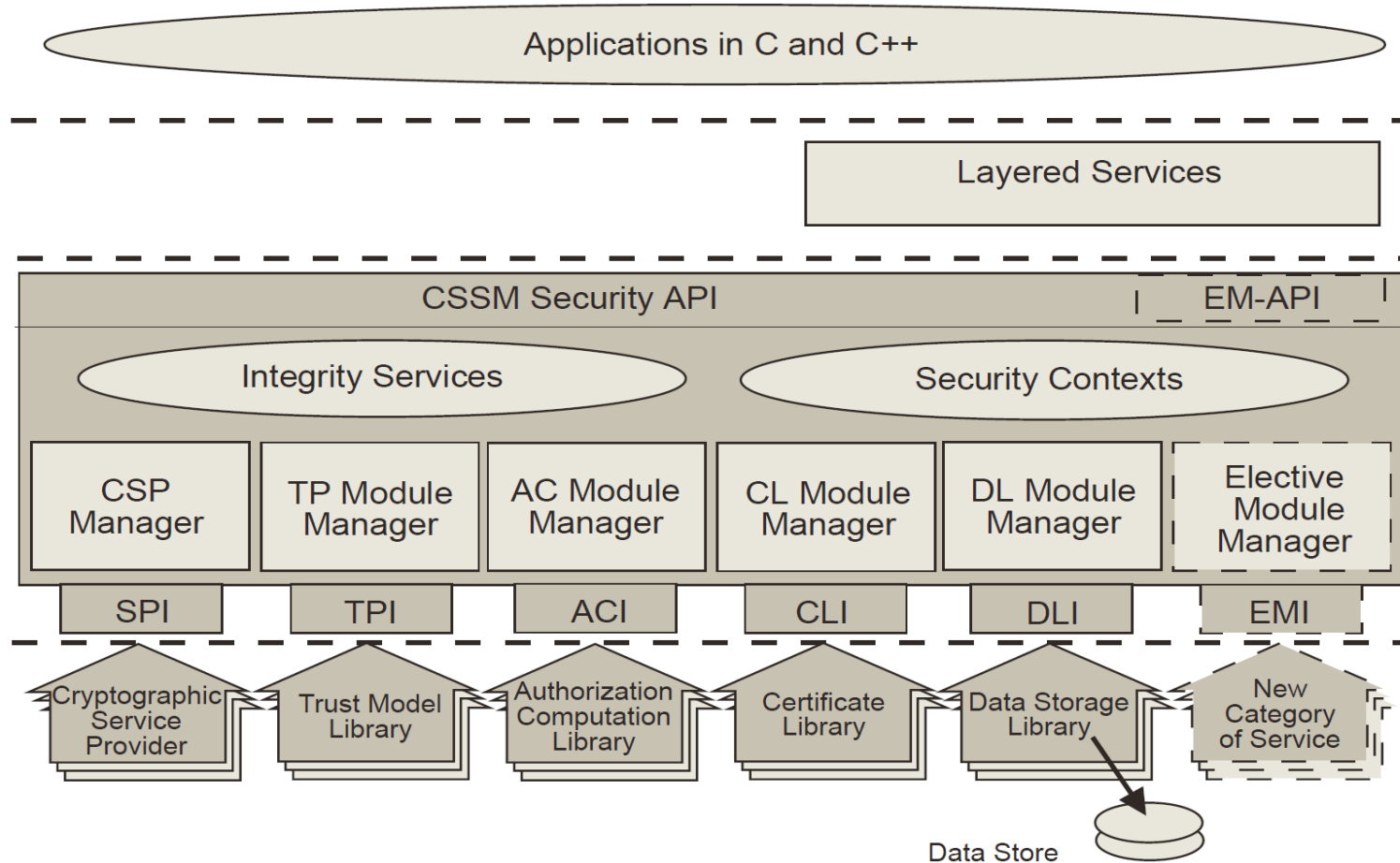
*Computer Security Architecture Workshop call for papers provides this **definition**:*

Architectures, whether system or application, are composed of abstractions (interfaces) and their implementations. Security Architectures are architectures which enable implementations that are resilient to an appropriate and broad-based spectrum of threats. An evaluation of a Security Architecture requires understanding these threats; the tradeoffs between different system goals, including between security and non-security goals; the long-term appropriateness of its interfaces; and the implementations it allows. The best interfaces are those that capture the most important issues, enable different implementations, and are flexible enough to adapt (or be adapted) to different threats.

Examples

<http://www.opengroup.org/publications/catalog/c914.htm>

Common Data Security Architecture



Examples

<http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/026.pdf>

5.1 The ISO 7498-2 Security Elements

The ISO 7498-2 standard provides a reference model for communications between open systems. It also specifies a set of security services that can be used as a frame of reference for exploring the services required in distributed data integration. When viewed in the form of a control matrix (refer to Table 1), the services in the model can be shown as to their implementation in the main areas of integration.

Security Element	Data Store	Network Medium	Data Source
<i>Confidentiality</i>	√	√	√
<i>Data Integrity</i>	√	√	√
<i>Authentication</i>	√		√
<i>Non-Repudiation</i>	√		√
<i>Access Control</i>	√		√

Table 1: Security services per area.

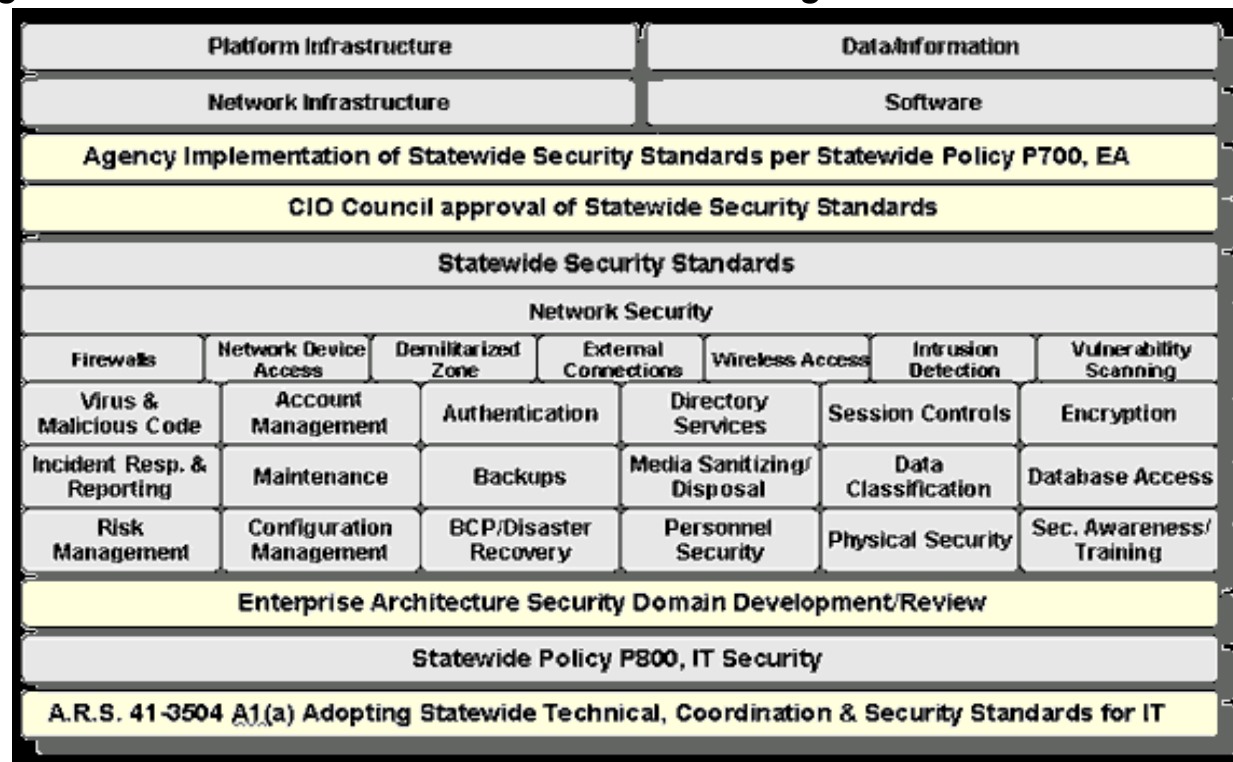
Example

http://gita.state.az.us/enterprise_architecture/NEW/Security_Arch/

Provides this definition:

Security Architecture provides the framework and foundation to enable secure communication, protect agency business processes and information resources, and ensures that new methods for delivering service are secure.

And this diagram which shows what an architecture might look like-



Examples

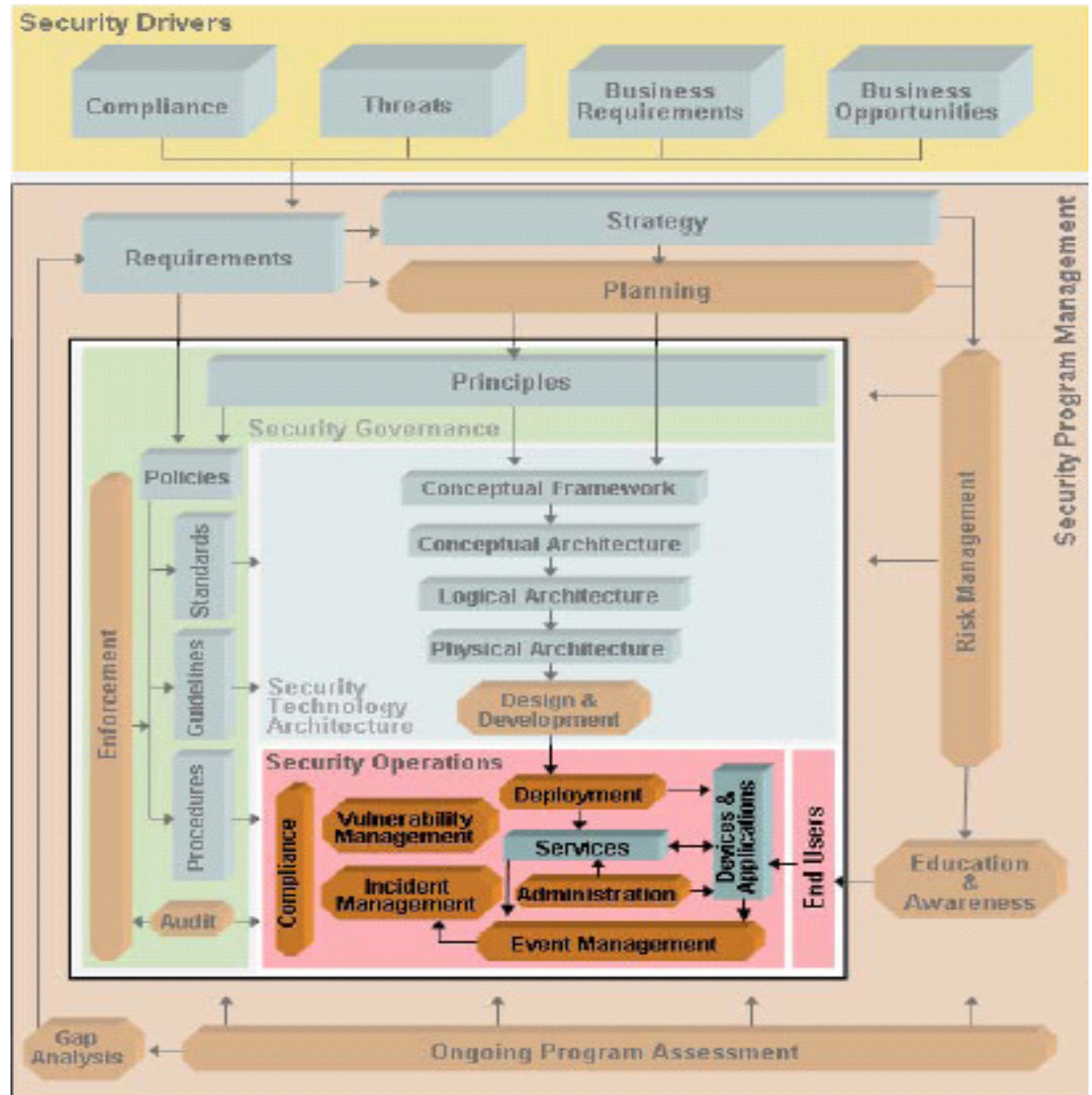
<http://www.linux.com/articles/49803>

Bruce Byfield

Lists 9 principles of a (good) security architecture.

1. Set a security policy for your system and know what's on it
2. Actions should be verifiable
3. Always give the least privilege practical
4. Practice defense in depth
5. Auditing the system: keep (and review) system logs
6. Build to contain intrusions
7. A system is only as strong as its weakest link
8. Locking the barn door after the horse is gone is ineffective
9. Practice full disclosure

Examples



Examples

Enterprise Architecture Security Viewpoint

Security related environmental trends, business drivers and requirements, business strategy – security items highlighted.

**Business
Context**

Security related vision, principles, high level models from other viewpoints that include security elements, and models showing conceptual security only functions

- Security Policy Framework
- Data Classification Framework
- Security Services Model
- Process Model
- Trust level definitions

Conceptual

Artifacts from other viewpoints that show logical, more detailed relationships and include security elements, and models showing security only functions

- Design Principles
- Logical Design Models
- Trust Modelling and Security Domain Modelling

Logical

Detailed artifacts from other viewpoints that include security elements and security only functions and services that can be implemented

- Security Infrastructure Architectures
- Security Services Architecture
- Application Security Architectures
- Bricks

Implementation

Gartner

Definitions: Vulnerabilities

DoD 5200.40

A weakness of a system, its assets or processes, which could be exploited by threats.

CERT CC

an aspect of a system or network that leaves it open to attack

ISO/IEC 13335-1: 2004-11-15

a weakness of an asset or group of assets that can be exploited by one or more threats

[ISO/IEC 13335-1:2004]" ISO/IEC 17799: 2005-06-15

"a weakness of an asset or group of assets that can be exploited by one or more threats

[ISO 13335-1:1996]. ISO/IEC 21827: 2002-10-01

Includes a weakness of an asset or group of assets which can be exploited by a threat

Definitions: Threats

NIST 800-30

The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

CERT CC

any circumstances or event that has the potential to cause harm to a system or network

ISO/IEC 13335-1: 2004-11-15

a potential cause of an incident that may result in harm to a system or organization

ISO/IEC 17799: 2005-06-15

a potential cause of an unwanted incident, which may result in harm to a system or organization

Definitions: Risk

DoD 5200.40

A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact

[ISO/IEC Guide 73:2002] ISO/IEC 17799: 2005-06-15

combination of the probability of an event and its consequence

[ISO 13335-1:1996]. ISO/IEC 21827: 2002-10-01

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

[ISO/IEC 13335-1:2005] ISO/IEC DTR 19791:2005-06-30

the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence

New Arbeitsgruppen

*Please contact Anthony Thorn with ideas for new AGs
Anthony.Thorn@isss.ch*

Speaker: Anthony Thorn, AT Systems & Services GmbH
ATSS