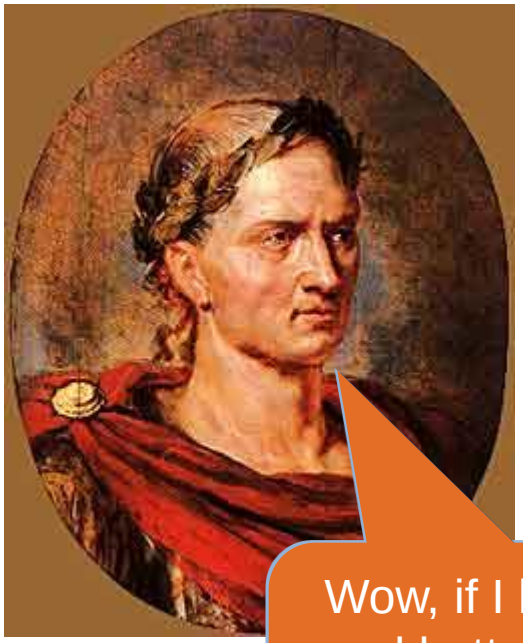
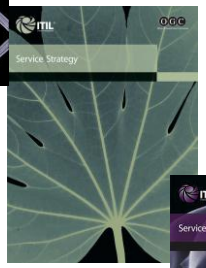
Security Management and ITIL®

History of Information Security and ITIL®



Wow, if I had ITIL ® V3 and better processes , I might have lived longer!

Continual Service Improvement



Service Strategy

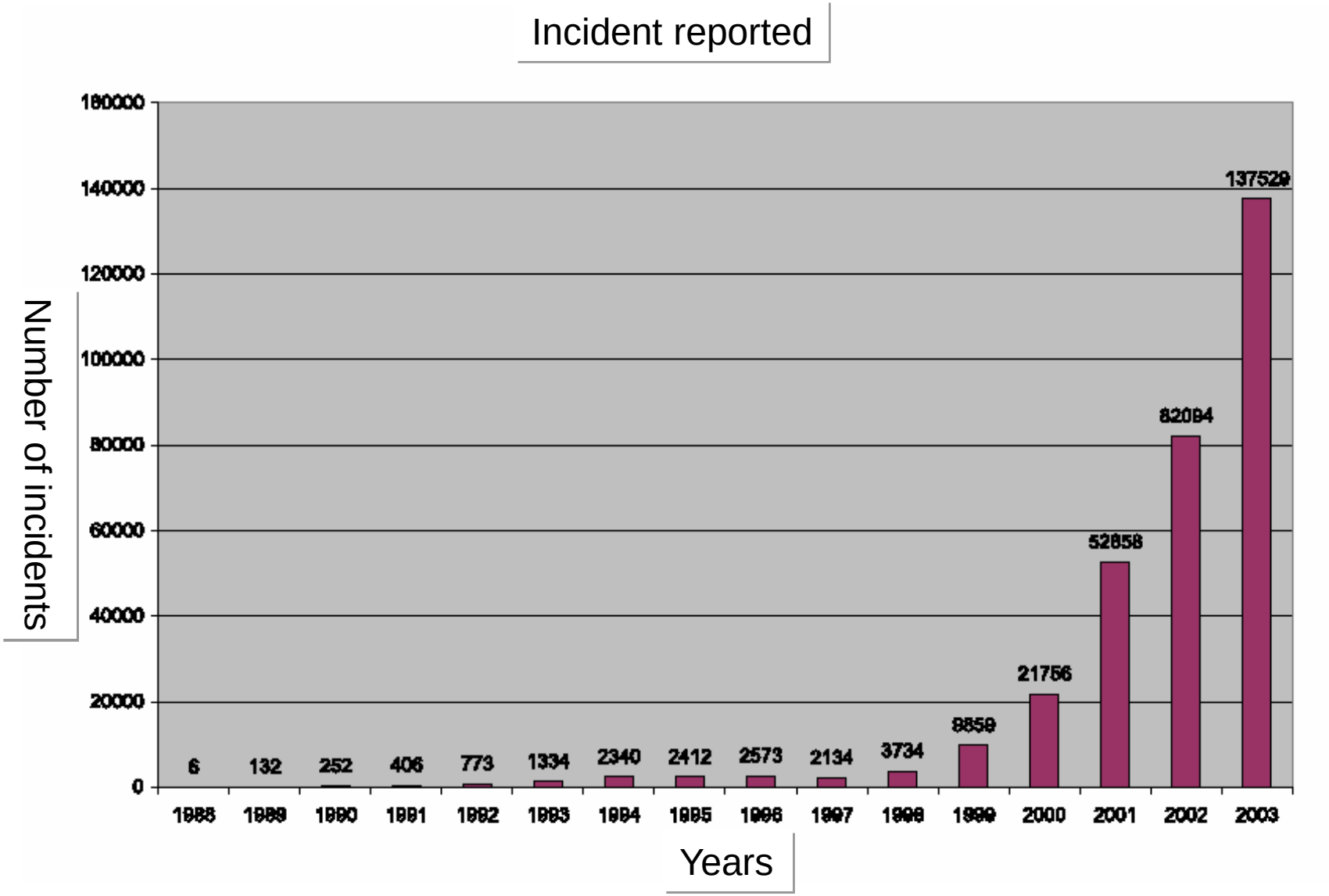
Design Service

Service Transition

Service Operation

Julius Caesar is credited wi…which was created in order to prevent his secret message…rong hands, but for the most part protection was achieved thr…s. Sensitive information was marked up to indicate that it s…persons, guarded and stored in a secure environment or strong box. As postal services expanded governments created official organisations to intercept, decipher, read and reseal letters (e.g. the UK Secret Office and Deciphering Branch in 1653).

Statistics



Statistics

- "The total losses in 2004 by 269 companies as a result of a computer security incident has reached a total of $ 141.5 million, which is an average of 526 000 per company. "

  Reference : *"2004 CSI/FBI Computer Crime and Security Survey" Computer Security Institute, 2004.*

- "93% of companies that have experienced a disaster and did not backup their data disappeared."

  Reference : *"Disaster Recovery", Interex 98 Conference, May 12, 1998.*

- "Several surveys have shown that about half of attacks against computer systems came from inside the company."

  Reference : *"2004 CSI/FBI Computer Crime and Security Survey" Computer Security Institute, 2004.*

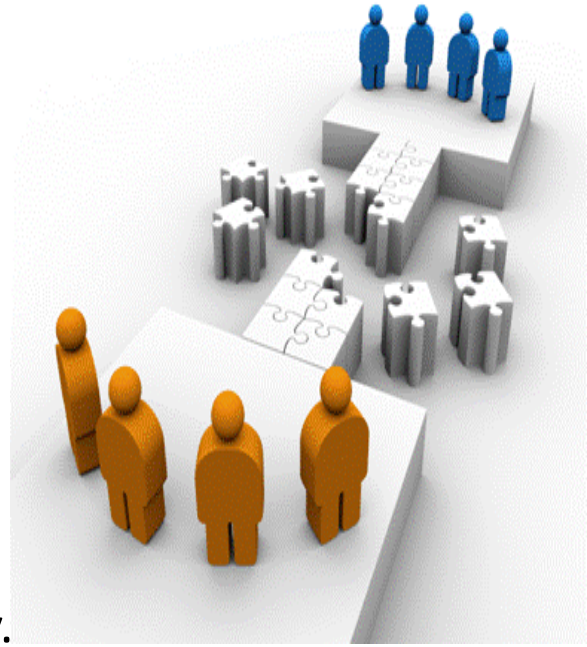
A sound security management should be based on well-established processes

How to manage and control information security?

ITIL® and the Management of Information Security

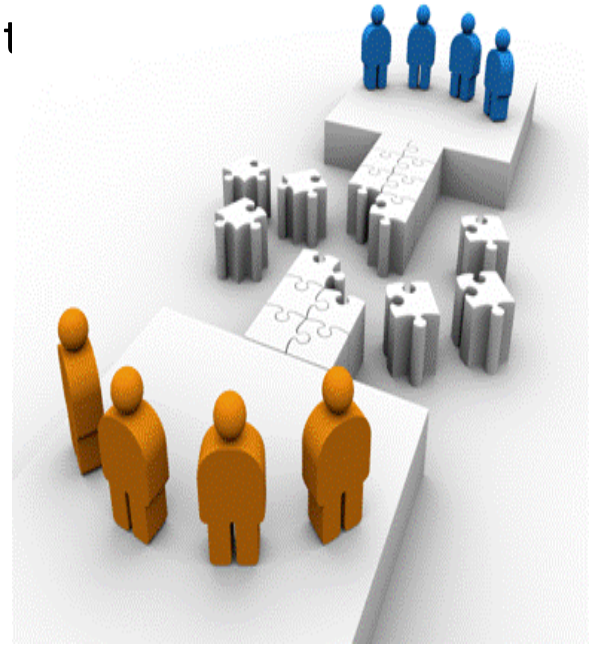
History of Information Security and ITIL®

- Late 80's, the first version of ITIL® V1
  - Security management almost nonexistent.
- 2001 ITIL® V2
  - Safety management introduced within the process of managing availability.
  - The security management is primarily guided by the principle that IT security provides: Confidentiality, Integrity and Availability (CIA) of information. Rather focused on technology.



History of Information Security and ITIL®

- 2007 ITIL® V3
  - Formal recognition that Security Management is an important process in ITSM and its life cycle.
  - Mainly used in the design, transition, and operations of IT services.
  - Axée sur la gestion de service tout au long du cycle de vie.
  - Focused on Service Management throughout the lifecycle.
  - Link established with ISO 27001.



Key Concept - Elements of Value Creation: Utility and Warranty

- **UTILITY** of a service
  - Service attributes that have a positive effect on the execution of activities, objects and tasks associated with the outcome.
  - The removal or reduction of **constraints** on the execution may also have a positive eff
  - **= ed to the needs**

But security is also a useful factor for an organization

- **WARRANTY** of service
  - An assurance that some products or services will be provided or that they meet certain specifications.
  - (e.g.: available when needed, where the quality and reliability are sufficient in terms of continuity and **security**)
  - **= Suitable for use**
- **The WARRANTY duces variation in pe ance.**

Interpreted as a guaranteed element

Information Security Management - Concepts

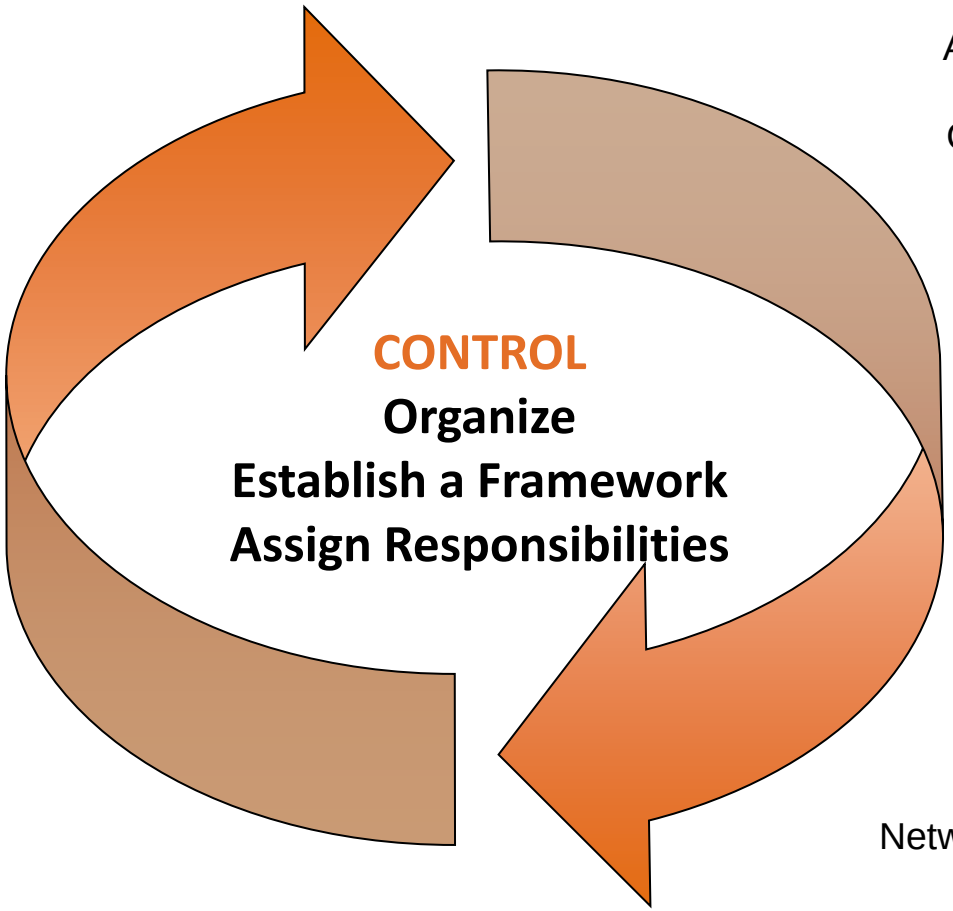
- Related with ISO/IEC 27001
- Is not documented as a business process, but rather a strategic one.
- Support processes to all other IT Service Management processes

Objective: Align IT security on the security of the business and ensure that information security is effectively managed in all departments and in all activities of management services

Information Security Management - Concepts

Maintain
Learn
Improve
Plan
Enforce

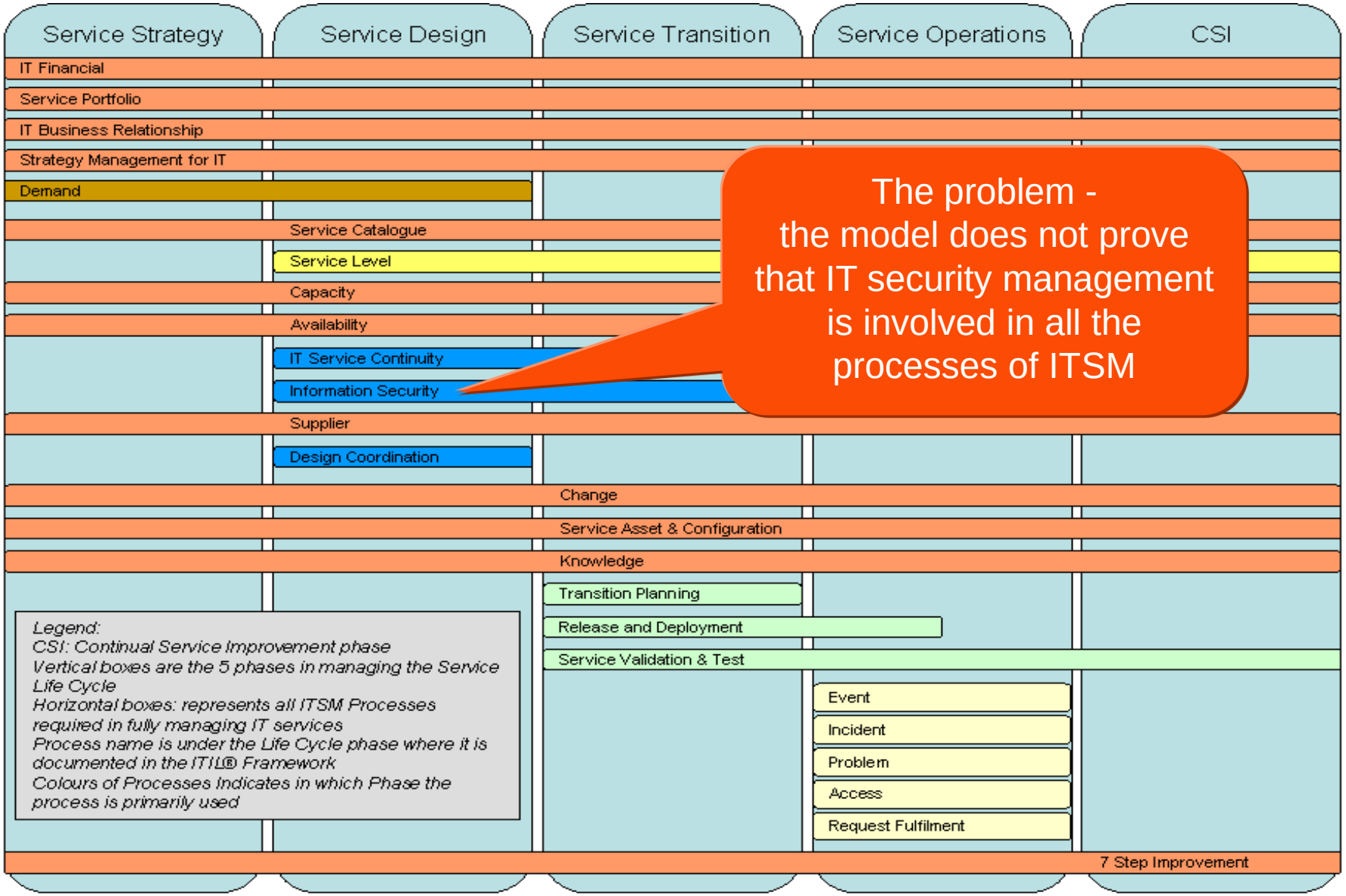
Plan
Agreements on Service Levels
Outsourcing Contracts
Operational Level Agreements
Policy Statements



Evaluate
Internal Audits
External Audits
Self-assessments
Security Incidents

Enforce
Sensitization
Classification and Recording
Staff Security
Physical Security
Networks, Applications, Computers
Access Rights Management
Procedures related to Security Incidents

Scope of the ITIL® framework and lifecycle services



Point of view and suggestions on Managing Information Security in relation to the IT Services Management

The reality of the security management information

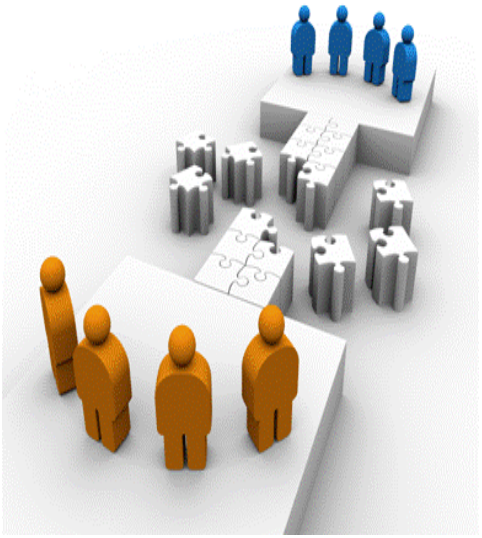
- Subject that management would like to avoid
- Seen as a cost rather than a value
- People who work in this field are sometimes regarded as not being in line with the needs of business
- The subject can put someone to sleep in 5.4 seconds
- Connect the concepts of security management with the reality of business is difficult

Why improve the ITSM ... 5 Business Reasons

1. Increase your revenues
2. Rationalize the cost of services
3. Meet your obligations
4. Enhance the customer and user experience
5. Improve internal efficiency

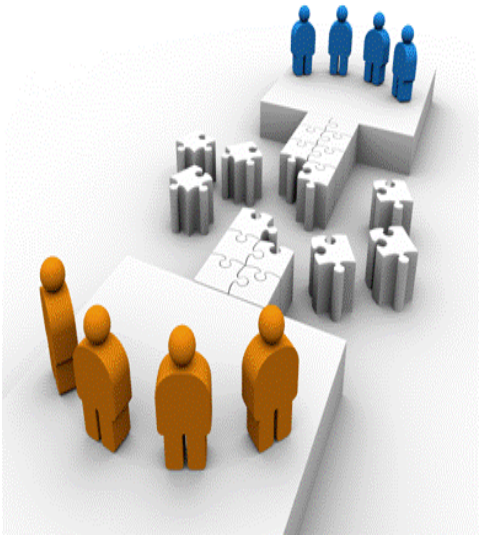
Connect IT Security Management to the Broad Objectives of ITSM

- Improve the alignment of IM / IT with business strategy
  - All elements of the ITSM policy related to the business security policy
- Improving expectations in terms of customer and internal IM / IT service
  - Have a catalog that connects customer service to the technical security management services
- Better understanding of cost factors associated to the IM / IT performance services
  - Link your customer service to technical safety service to understand the real cost of managing security.
  - Our experience on the additional costs of security management is in many cases, only 0.65% of the total requests made to the supplier



Connect IT Security Management to the Broad Objectives of ITSM

- Improve the efficiency of the IM / IT Group
  - Ensure that any major change has an impact analysis related to safety
- Enable the successful implementation of the agreements (ANS, ANO)
  - Include the value of IT Security in agreements
  - Example: Service level achieved if we mitigates the security issues



ITIL ® Processes (partial list)
Recommended Concepts

ITSM Process	Benefits to Security Management
Incident Management	Troubleshooting with impact on safety. Confirmation of the use and understanding of the security policy
Change Management	All changes must have an assessment on the impact of the security
Configuration Management	Confirmation that security is an attribute of all the infrastructure components
Service Level Management	Security is a standard element of negotiation and agreements
Catalog Service Management	Visualize the dependence of customer services on the security services

Delivery Chain - Security Service Management

Linking Security Management to the chain of service performances ...

Business Clients

Executives / BRM

Project Managers Analysts, Architects Developers, Etc…

Operations Service Desk Help Desk Technical Support

Users Consumers

Agreement

Project/ Change

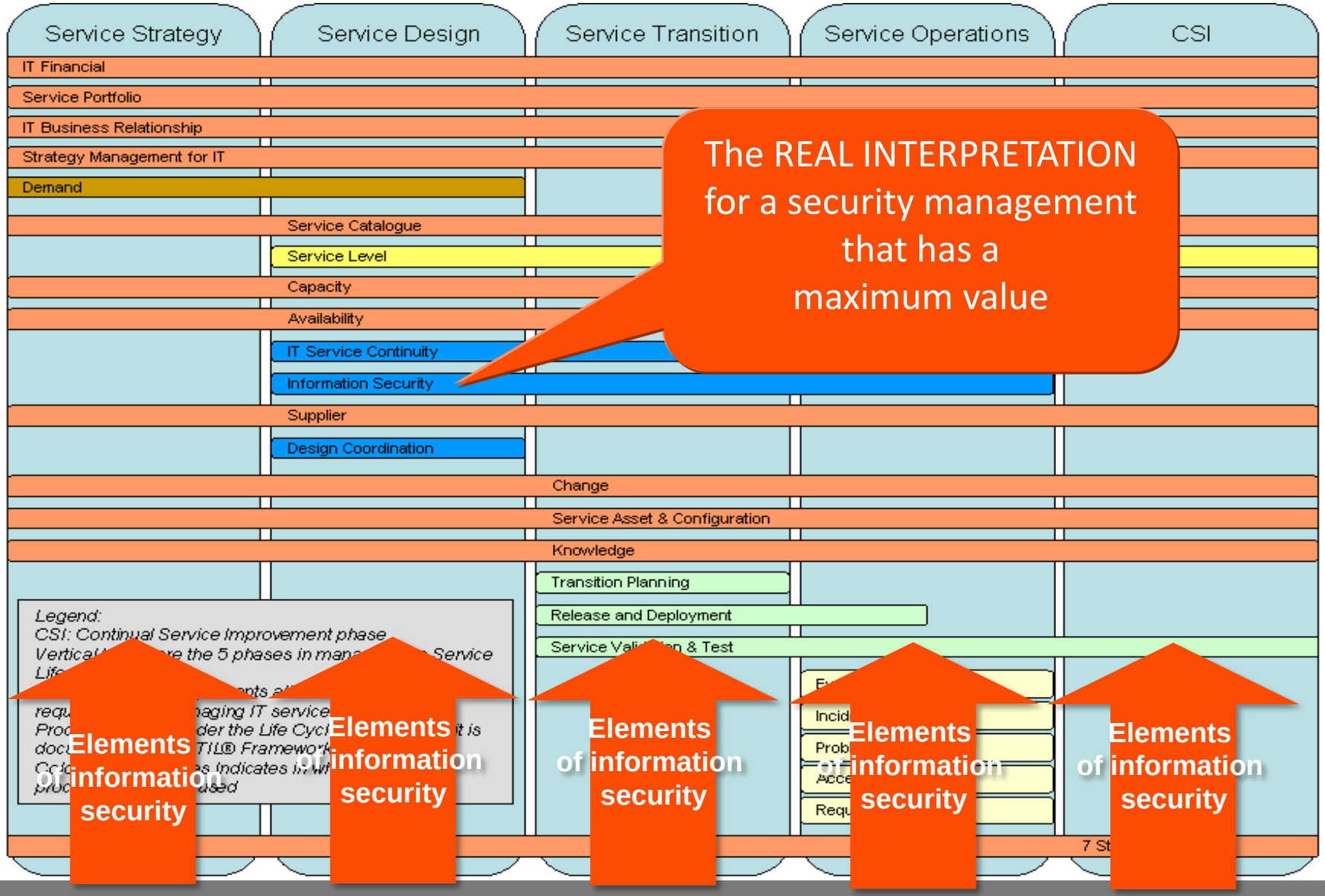
Build/Deploy

Support/ Delivery

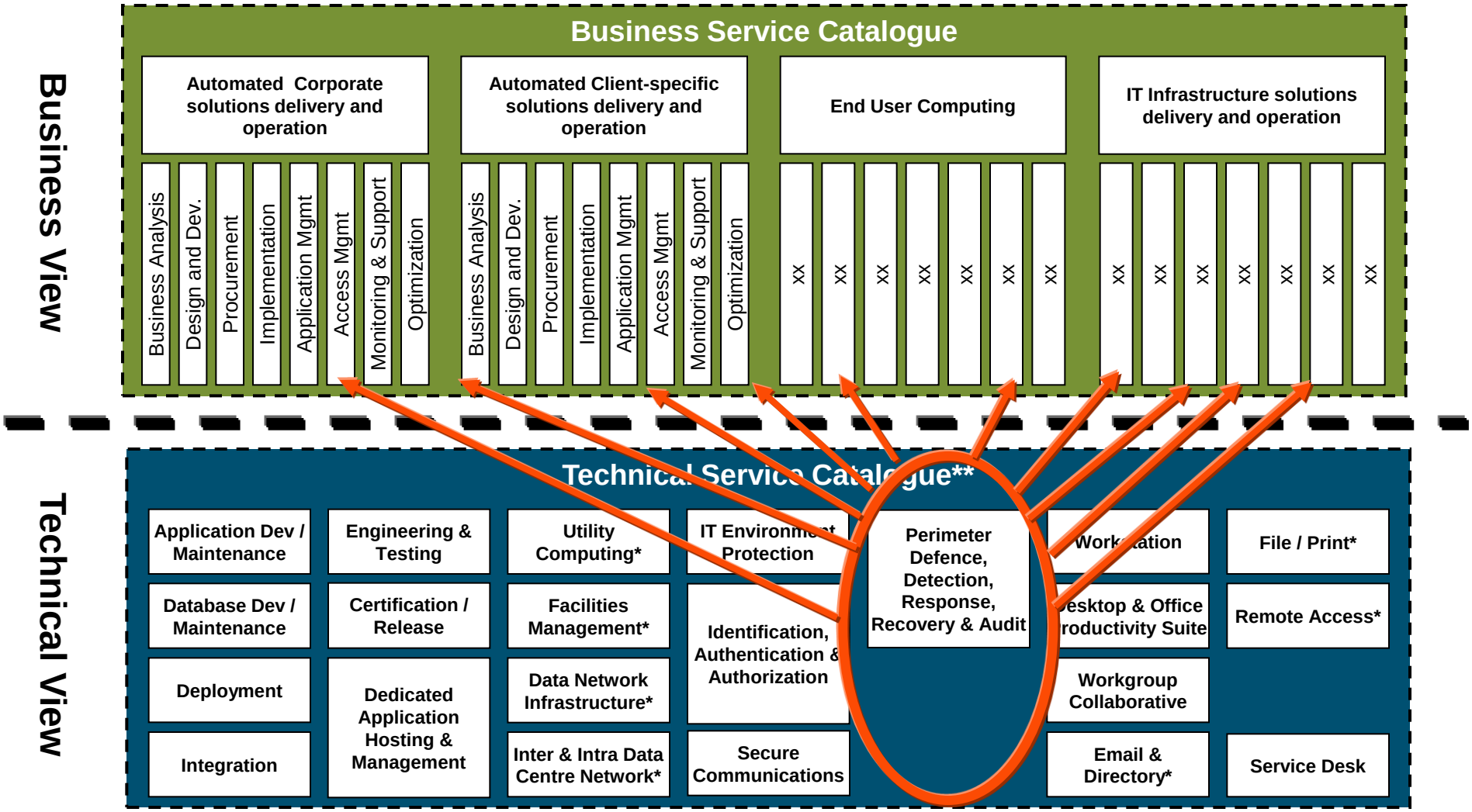
Using a business case approach speaking of security management

- What would be the effect if the information was used by someone from the outside?
- Is this in line with the IT strategy? Do we have the budgets? What would be the effect if the information was used by someone from the outside?
- What level of security are we going to need for this service and what mechanism / technology should we use?
- Have you been trained on the security policy and on the security elements of the procedures?
- Do I have the rights to see this information or do I have access to this request?

Scope of the ITIL® framework and lifecycle services



Highlighting Security Management services in the catalog of services ... an example



ITSM Integration Table processes of ITIL® Process: Security Management

ITIL® Process	Security Management given to...	Given to the Security Management ...
Incident	Scale to categorize an incident as having an impact on safety	Statistics on incident safety type
	Assistance in the investigation and resolution of security type incidents	Troubleshooting analysis

To be used for the development of procedures and work instructions

Roles

- Clients / Users
- Customer Relationship Manager (CRM)
- Software Manager
- Security Information Management
- Architecture and Planning
- Project Management Office
- Service Center
- Financial Management
- Infrastructure Management
- Etc.

- **" Security Relations Manager":** responsible for managing relationships with all internal the supplier groups and having a business approach — the bridge between the security jargon and the terminology case. Negotiates agreements with other operational IT sectors and ITSM processes.

Some Recommendations

- Create and assign the Relationship Manager role – Security
- Link the Security Management activities to the major ITSM business objectives
- Involve the Security Manager in all processes improvements of the Service Management Processes
- Include services from the security management into the services catalog, and linking to customer service
- Develop and negotiate operational level agreements (OLA) with all other IT sectors
- Hold a safety element in your ITSM improvement projects. Ex: in the process documents have a section called “Integrating safety information”

In conclusion

- ITIL® has contributed and demonstrated the importance of security management
- For ITSM and ITIL® V3, the security management process is a strategic control to ensure safety perspective in other ITSM processes and activities.
- There is always a security activity in all ITSM processes
- A sound security management should be based on well-established processes in an organization
- The identification of activities related to safety in all ITSM processes represent the success of the security management