Metrics for Information Security Management

Jesus Leonardo Garcia Rojas
Innovaciones Telemáticas
lgarcia@intelematica.com.mx

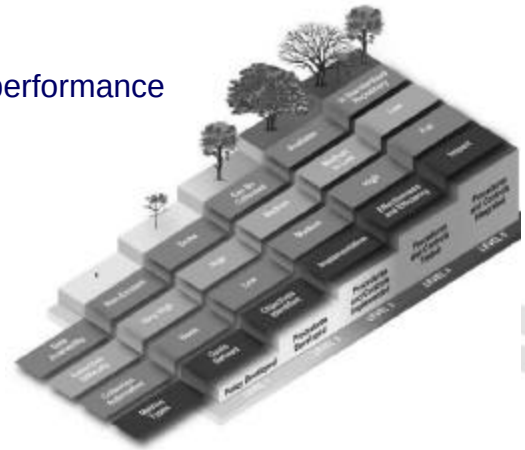
How do we know how „secure an organization is?

- Manager asks, „Are we secure?“
  - *Without metrics:*
    - „Well that depends on how you look at it.“
  - *With metrics:*
    - „No doubt about it. Look at our risk score before we implemented that firewall project. It‘s down 10 points risk. We are definitely more secure today than we were before.“
- Manager asks, „Have the changes that we implemented improved our security posture?“
  - *Without metrics:*
    - „sure, they must have right?“
  - *With metrics:*
    - „Absolutely. Look at our risk score before we made the recommended changes, and now it‘s down 25 points. No question, the changes reduced our security risk.“

What is a metric?

- FIPS 140-1/2 metrics for cryptosystems,
  - The standard provides four increasing, qualitative levels of security. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

- SSE-CMM (Carnegie Mellon university)
  - A five step maturity model to evaluate a company software development performance



- The National Institute of Standards and Technology (NIST) (SP 800-53, SP 800-55)
  - The NIST use the CMM model in the security area.

- We learned from the SECurity METrics (SECMET) consortium, that “Network security experts can’t be measure their success without security metrics, and what can’t be measured can’t be effectively managed”

- 27004 Information security management measurements – is at the WorkingDraft stage

- A more formalized mathematical Method can be derived from the mass-theorie. It exist for that problem only an solution for a countable set. This set must be fulfill a sigma-algebra

Measuring process

- Indentifying the object of measurement
  - A particular ISMS process
  - A control or a group of controls
- Identifying the method of measurement
- Identifying the measurement frecuency
- Identifiying measuremetn criteria
- Definition of data collection, analysis and reporting procedures
- Execute the measurement and improve it where necesary

Measurement, Metrics, Indicators

- **Measure:** A quantitative indication of the extent, amount, dimension, capacity or size of some attribute of a control or process.
  - A single data point (e.g. number of defects from a single review)
- **Measurement:** The act of determining a measure
- **Metric:** A measure of the degree to which a system, component, control or process possesses a given attribute.
  - Metrics relate measures (e.g. Average number of defects found in reviews)
  - Relate data points to each other
- **Indicator:** A metric or series of metrics that provide insight into a process, project or product.

Why Measure?

- Characterise
  - To gain understanding of processes, control, products, etc.
- Evaluate
  - To determine status with respect to plans.
- Predict
  - So that we may plan.
- Improve
  - Rational use of quantitative information to identify problems and strategies to remove them

What to Measure?

- Process
  - Measure the efficacy of processes
  - Effectiveness of ISMS
  - What works, what doesn't
- Project
  - Assess the status of projects
  - Track risk
  - Identify problem areas
  - Adjust work flow
- Controls
  - Measure predefined control attributes

- Majority focus on goals achieved as a consequence of a repeatable or managed process
- statistical data
  - defect categorization & analysis
- defect removal efficiency
  - propagation from phase to phase
- reuse data

- Effort/time per task
- Defects detected per review hour
- Scheduled vs. actual milestone dates
- Changes (number) and their characteristics
- Distribution of effort on tasks

Control Metrics

- focus on deliverables
- measures of analysis model
- complexity of the design
  - internal algorithmic complexity
  - architectural complexity
  - data flow complexity
- code measures
- measures of process effectiveness
  - e.g., defect removal efficiency

Metrics Guidelines

- Use common sense and organizational sensitivity when interpreting metrics data.
- Provide regular feedback to the individuals and teams who have worked to collect measures and metrics.
- Don’t use metrics to appraise individuals.
- Work with practitioners and teams to set clear goals and metrics that will be used to achieve them.
- Never use metrics to threaten individuals or teams.
- Metrics data that indicate a problem area should not be considered negative. These data are merely an indicator for process improvement.
- Don’t obsess on a single metric to the exclusion of other important metrics.

Measurement Criteria

- Measurements should be:
  - Objective
    - Repeatable
  - Timely
    - Available in time to affect development/maintenance
  - Available
    - Difficulty to obtain
  - Representative
    - Degree of representation of customers perception
  - Controllable
    - Extent to which value can be changed by action

Examples of metrics

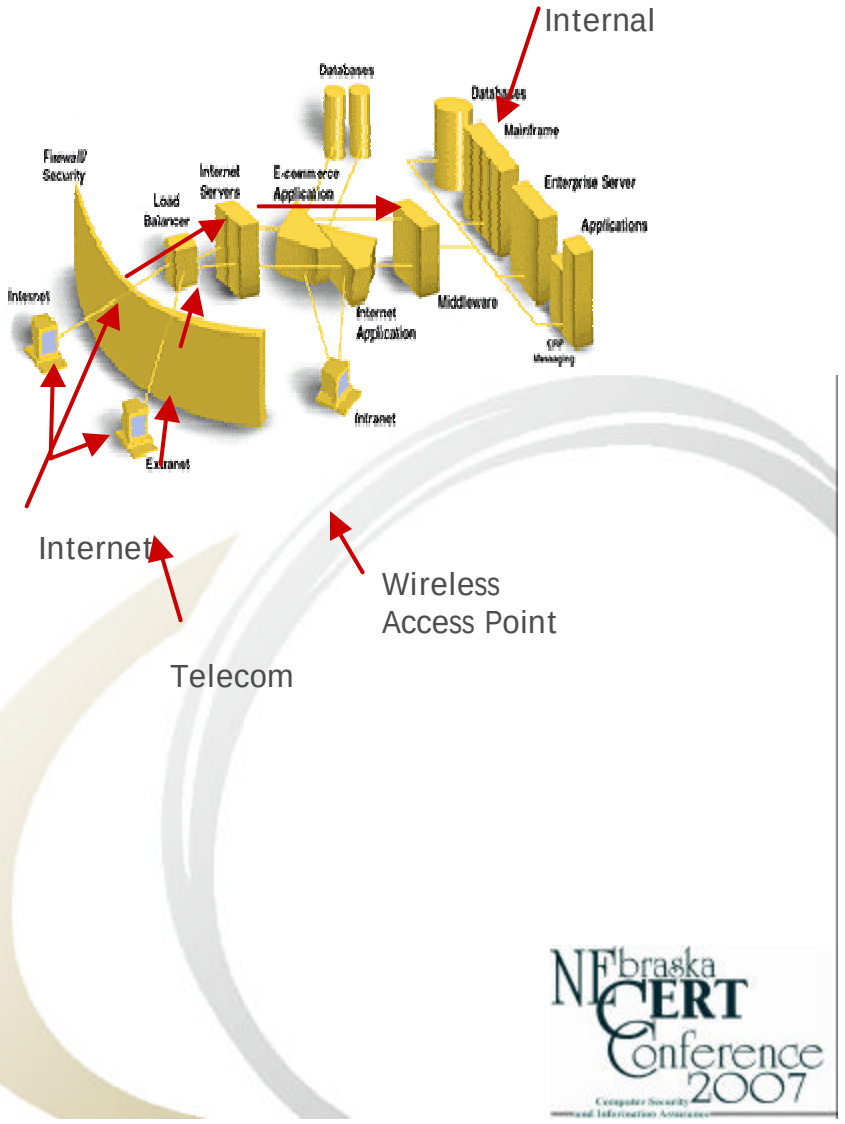
- Total number of remote connections over a one month period (VPN, ISDN, dial-up, remote desktop)
- Maximum number of concurrent remote by user
- The percentage of total applications that have a contingency plan by application criticality.
- Time to analyze and recommend action on a security event
- Number of Linux servers at least 90% compliant with the Linux platform security standard
- Quantitative or qualitative values that result from evaluation processes (manual, automated, or a combination) such as
  - Scoring < -> Assessing
  - Ranking < -> Measuring

Security Metric Categories

- Platform
  - Number of Linux servers that are compliant with EFS policy
- Network
  - DMZ port scans
- Incident
  - Number of hosts infected with worm XYZ
- Vendor
  - Average security rating for vendors that touch active customer files
- People
  - Number of terminated employees with administrator access
- Industry
  - Number of public security incidents in sector ABC with severity score Z
- Political
  - Hacktivism scores, amount of sites listing sector/company ABC as potential target

Security Metric Types

- Real Time
  - Number of concurrent connections to VPN
  - Usually from incident response systems
- Polled
  - Number of password reset requests (monthly),
  - Usually from Security Alert & Security Event Manager
- Incident based
  - Number of machines
  - Number of vendors suffering from infections
  - Usually from industry intelligence/incident response



Gathering Data

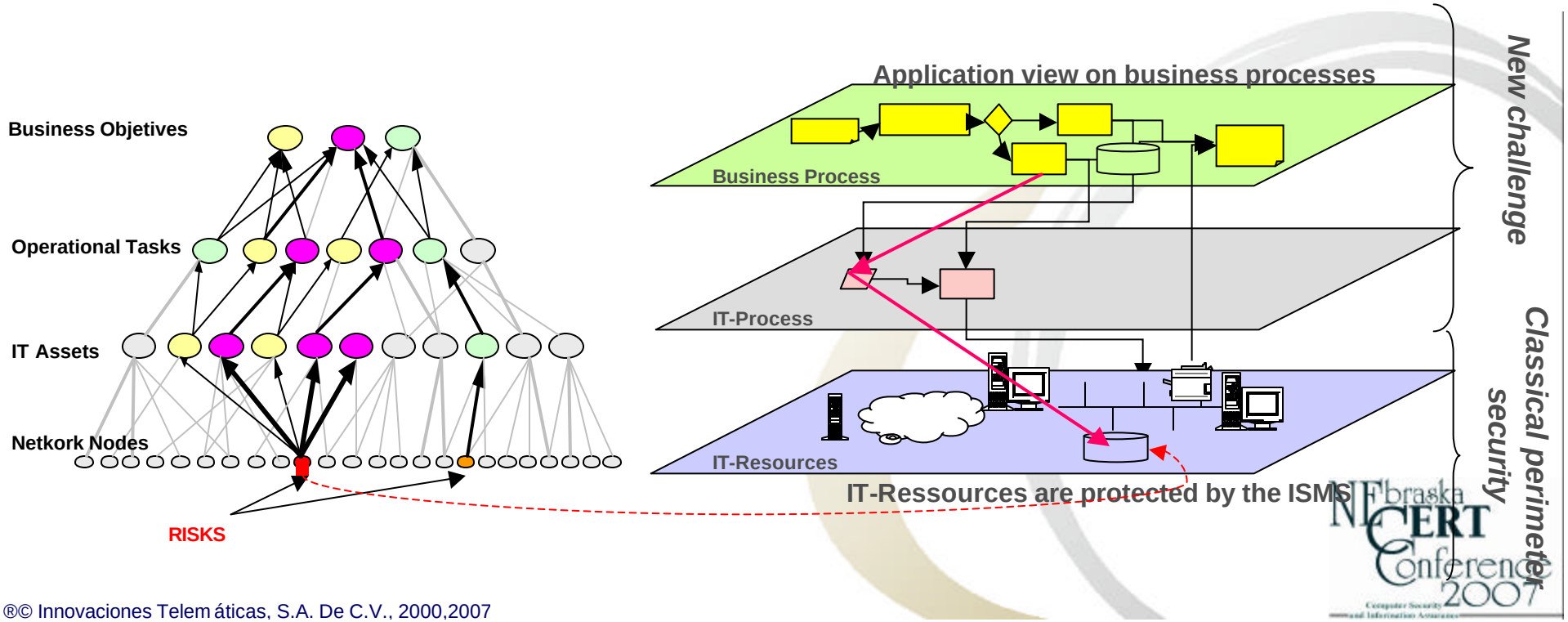
- Inquiry
- Observation
- Questionnarie
- Knowledge Assessment
- Inspection
- Re-performance
- System queries
- Testing and sampling
- Time.related considerations

How do we decide which one's to collect?

- Policy Mining / Easy to Spot Anomalies
- Risk Scoring
- ROI / Vendor Evaluations
- "Tips" / Visionaries
- Tools of Security Event Management
- IT security is often techniques orientated

Business meets IT Information Security

- Information, finance data and knowledge are stored in databases, operating systems and application
- How can we be sure that a company has a sufficient data to improve the effectiveness of the ISMS?

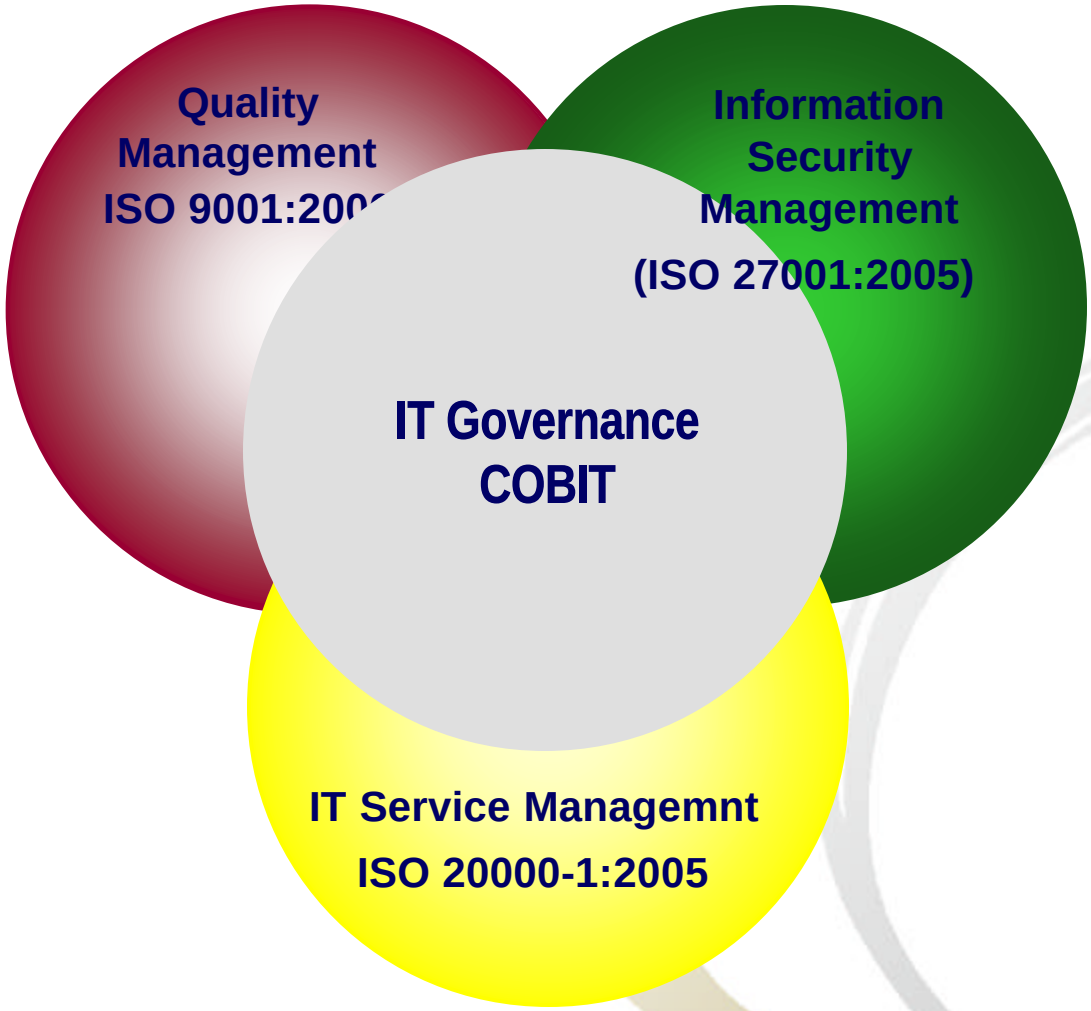


- Typically the organizations implements an information security manegement System

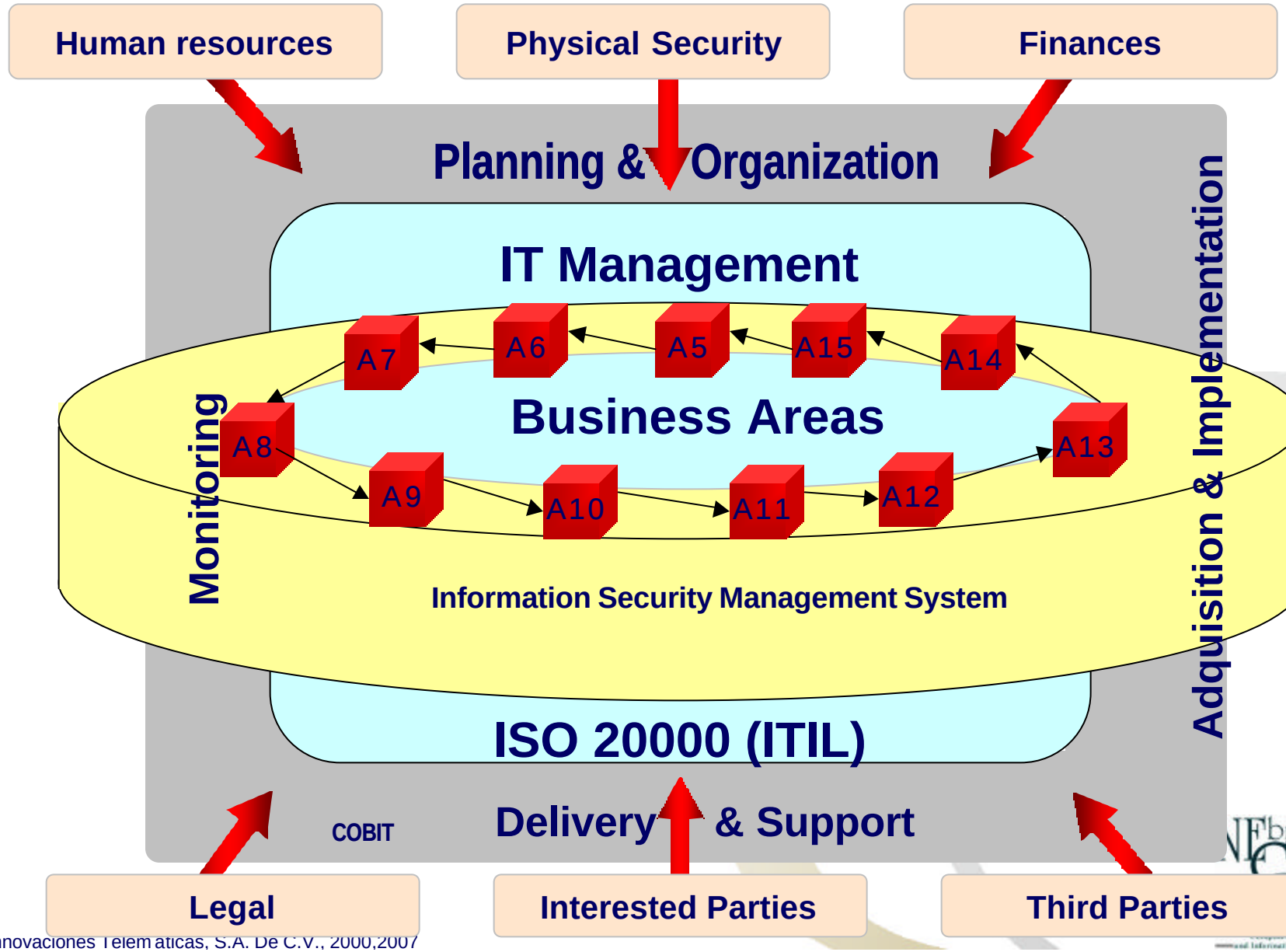
- An ISMS is an Management System (like other management system e.g. ISO 9001, ISO 14001) with a focus on Information security

- In this contribution an approach for the evaluation of the quality of ISMS is proposed

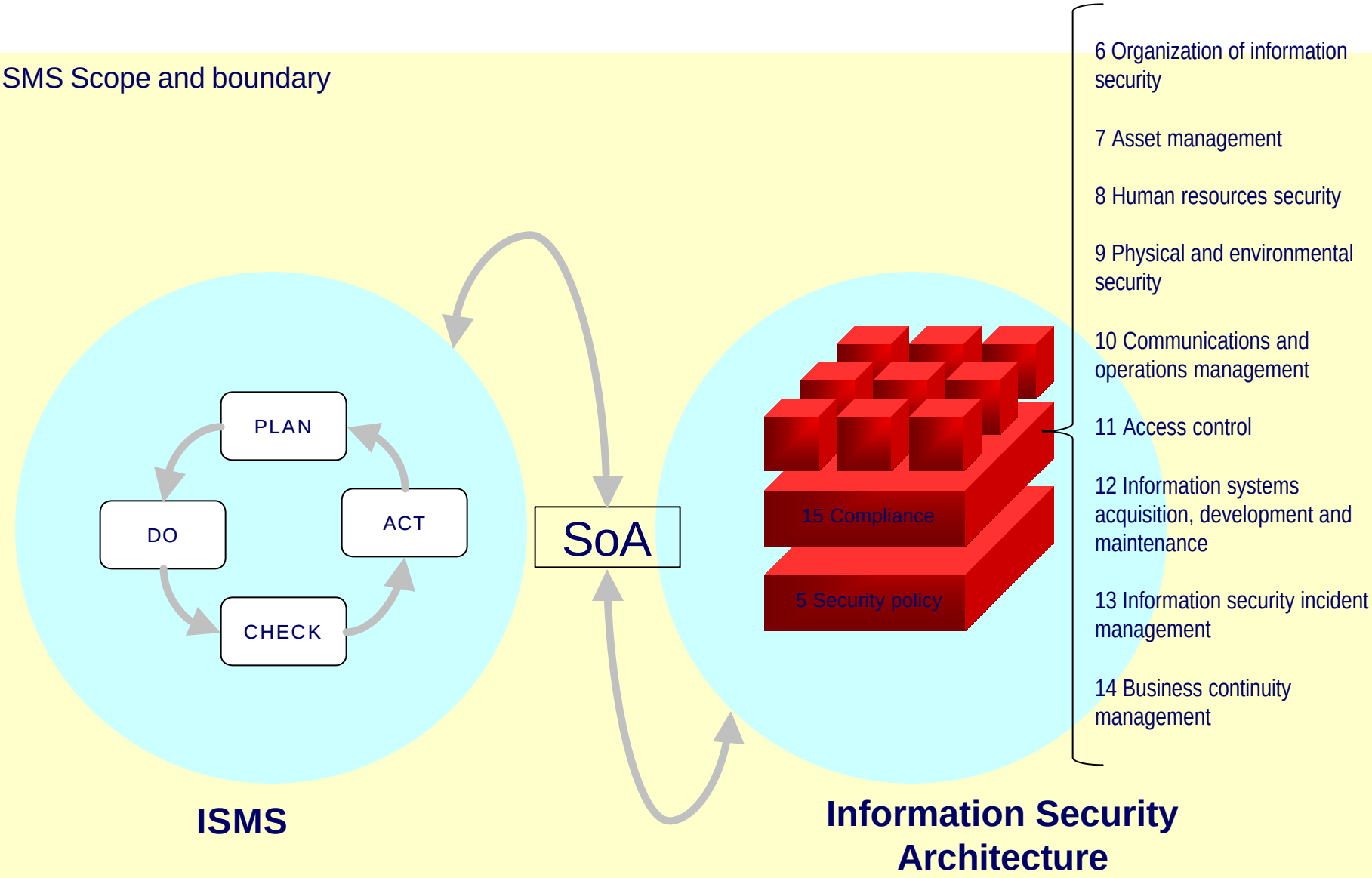
ISO standards relationships



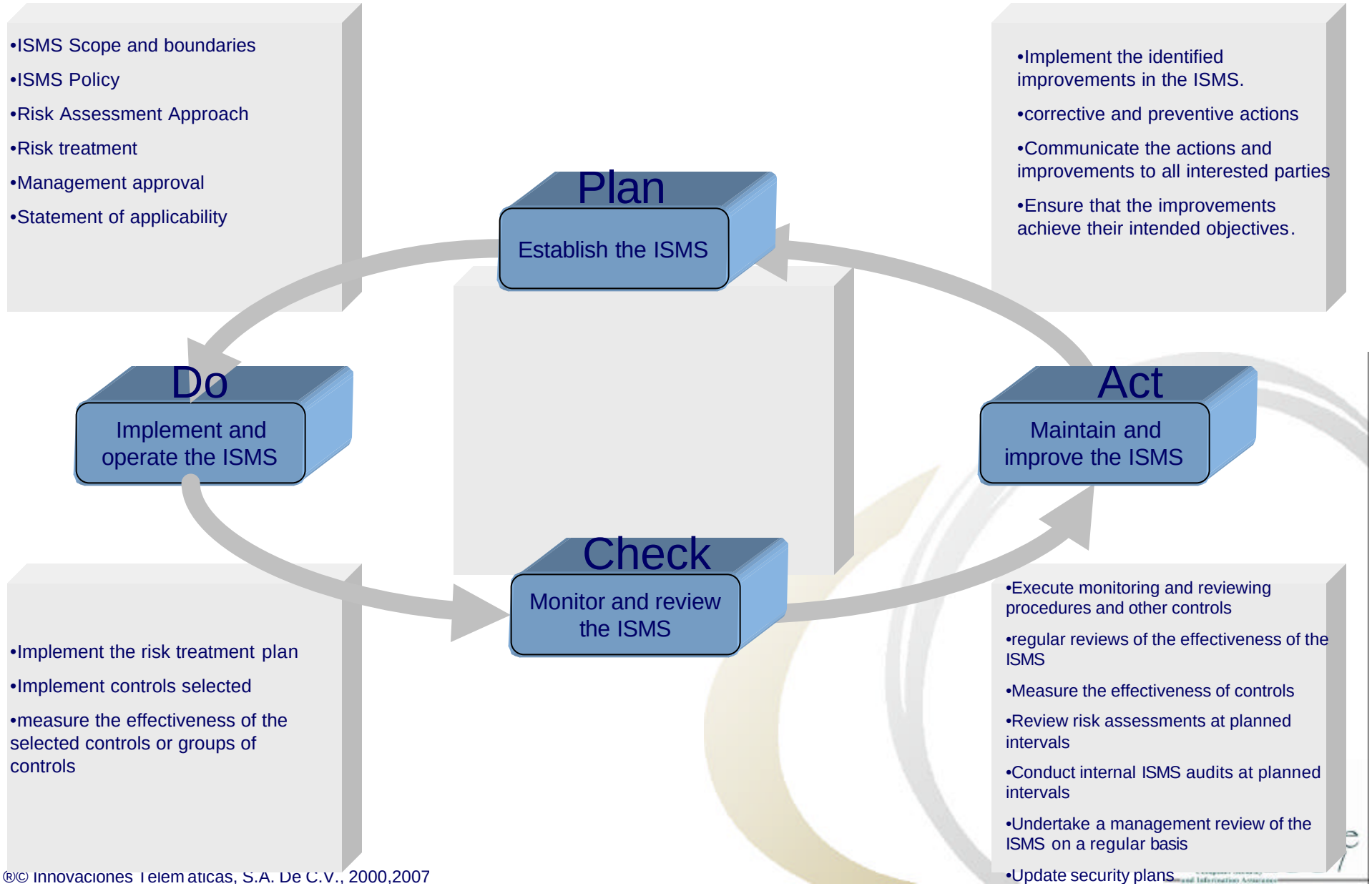
ISO standards relationships



ISMS Scope and boundary



Information Security Management System



Brief overview of different risk methods

- Return on Security Investment (ROSI) Model
  - University Idaho
  - University California
  - Massachusetts Institute of Technology (MIT)

- different Models, different views
  - Checklist, simple approach
  - Value at Risk Method (economy, simple approach to BASEL II)
  - CRAMM Method (CTT) is based on aprx. 3000 events of threats -> possible to use with BS 7799-2/ISO27001
  - Pure risk assessment followed BS 7799-2/ISO27001 -> a roughly method to couple in a simple way threats, vulnerabilities and risks
  - HazOP e.g. Fault trees / decision trees (FTA, FMEA, FMCA)
    - binary decision about bifurcation conduct to cognitions (failure, reasons, etc.)
  - OCTAVE (Operationally Critical Threat and Vulnerability Evaluation) from the Carnegie Mellon University
  - Risk Scenario-techniques (RST)
    - Risk scenario are be able to learn from hypothetical risk events, which are become possible happen in the near future, to create countermeasures in the presence, so that the hypothetical events are not happens.

Metrics for Information Security Management

Jesus Leonardo Garcia Rojas
Innovaciones Telemáticas
lgarcia@intelematica.com.mx