8th Central and Eastern European Software Engineering Conference in Russia - CEE-SECR 2012

November 1 - 2, Moscow

2012 CEE-SEC(R)

Software Engineering Conference in Russia

Bridging the Gap between Security/Risk Assessment and Quality Evaluation Methods

Luis **Olsina**, Alexander **Dieser**, Guillermo **Covella**

GIDIS_Web, Engineering School at Universidad Nacional de La Pampa, **Argentina**

Elena **Pesotskaya**

School of Software Engineering, HSE at National Research University, **Russia**

Summary of the Paper/Presentation Aim

- Преодоление разрыва между методами оценки рисков/безопасности и методами оценки качества

  Bridging the gap between …

- In the present work, we discuss the added value of supporting the **IT Security** and **Risk Assessment areas** with a **Measurement and Evaluation Strategy**, which includes **methods** that strongly relies on Metrics and Indicators.

Summary of the Paper/Presentation Aim

- An IT security vulnerability (attribute) can be considered as a potential weakness in a target system (target entity) that could be exploited by a threat source (source entity).

- Most vulnerable attributes of a target system can be identified for instance with *security controls* in order to evaluate *the level of their weaknesses* (acceptability level).

- Thus, ***understanding*** the current quality acceptability level achieved for vulnerable attributes can help in turn assessing the risk and planning actions for treatment (***improvement***) from the impact (consequence) standpoint.

Summary of the Paper/Presentation Aim

- The underlying hypothesis in our proposal is that each identified attribute associated with the target entity to be controlled should show the highest quality satisfaction level (acceptability level)as an elementary indicator.

- The higher the quality indicator value achieved per each attribute, the lower the vulnerability indicator value and therefore the potential impact.

Summary of the Paper/Presentation Aim

- The entrance gate to **IT Security** and **Risk Assessment areas** is based on identifying vulnerable attributes of a target entity, which can be quantified by metrics and interpreted by indicators.
  - **Metrics** and **indicators** are **organizational assets** and should be seen as designed, versioned and stored **by-products**

- Hence, by using an evaluation-driven strategy (as GOCAME) we can apply for quality and risk assessment its *Multi-Criteria (attribute) Decision* methods

Risk value for Attribute Ai = Probability of Event occurrence for Ai * Vulnerability Indicator value for Ai

Vulnerability Indicator value Ai = 100 – Quality Indicator value Ai

Summary of the Paper/Presentation Aim

- **Risk evaluation** assists in the decision about **risk treatment**, which is defined as “the process to modify risk”.
- Usually **risk treatment** can involve:

i) ….;

ii) ….;

iii) removing the risk source;

iv) changing the likelihood (probability);

v) changing the consequences;

vi) sharing the risk with another party or parties; and

vii) ….

Summary of the Paper/Presentation Aim

- Ultimately, without the well-established support of **metrics** and **indicators** and their values, **Software Risk Management** could be more craftwork than engineering!
  - Metrics and indicators are organizational assets which provide useful **data** and **information** for analyzing, recommending, controlling and ultimately making decisions

- The proposed approach of looking at (security) vulnerabilities as attributes of target entities and then using metrics and indicators for their measurement and evaluation is illustrated in the following slides, considering also the **W5H** mnemonic rule!

GOCAME M&E Strategy: An Overview

- **GOCAME** is an integrated **Measurement & Evaluation strategy** which follows a **goal-oriented** and **multiple-attribute (criteria) evaluation** approach.

GOCAME has its **terminological base** defined as an **ontology** from which the **conceptual framework** emerges

GOCAME process embraces the following activities:

i) Define Nonfunctional Requirements (Features/Attributes);

ii) Design the Measurement (Metrics);

iii) Design the Evaluation (Indicators);

iv) Implement the Measurement (measure values/data);

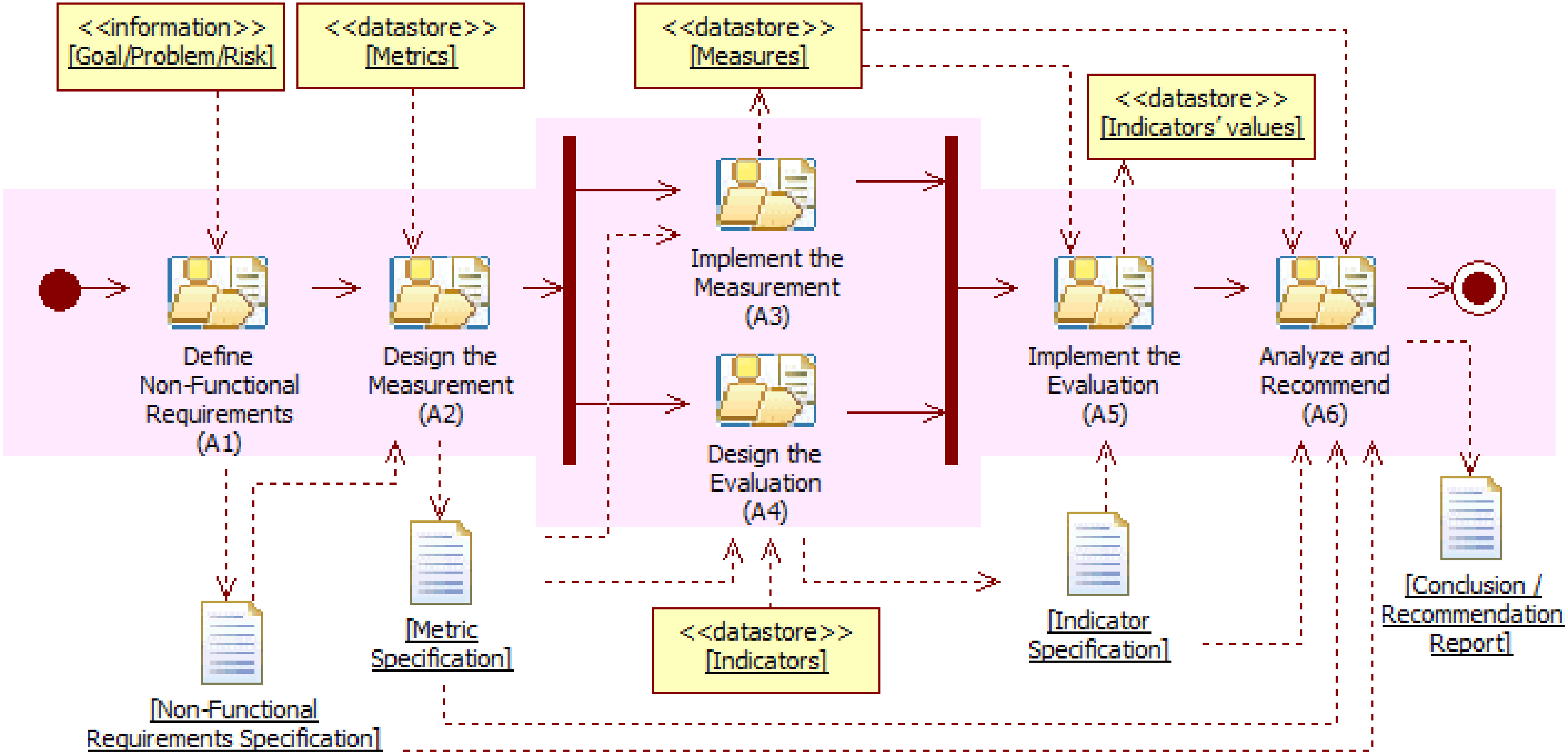
v) Implement the Evaluation (indicator values / information);

vi) Analyze and Recommend

WebQEM methodology provides a multi-criteria evaluation approach, relying on experts and/or end users to evaluate and analyze different views of quality for software/web applications

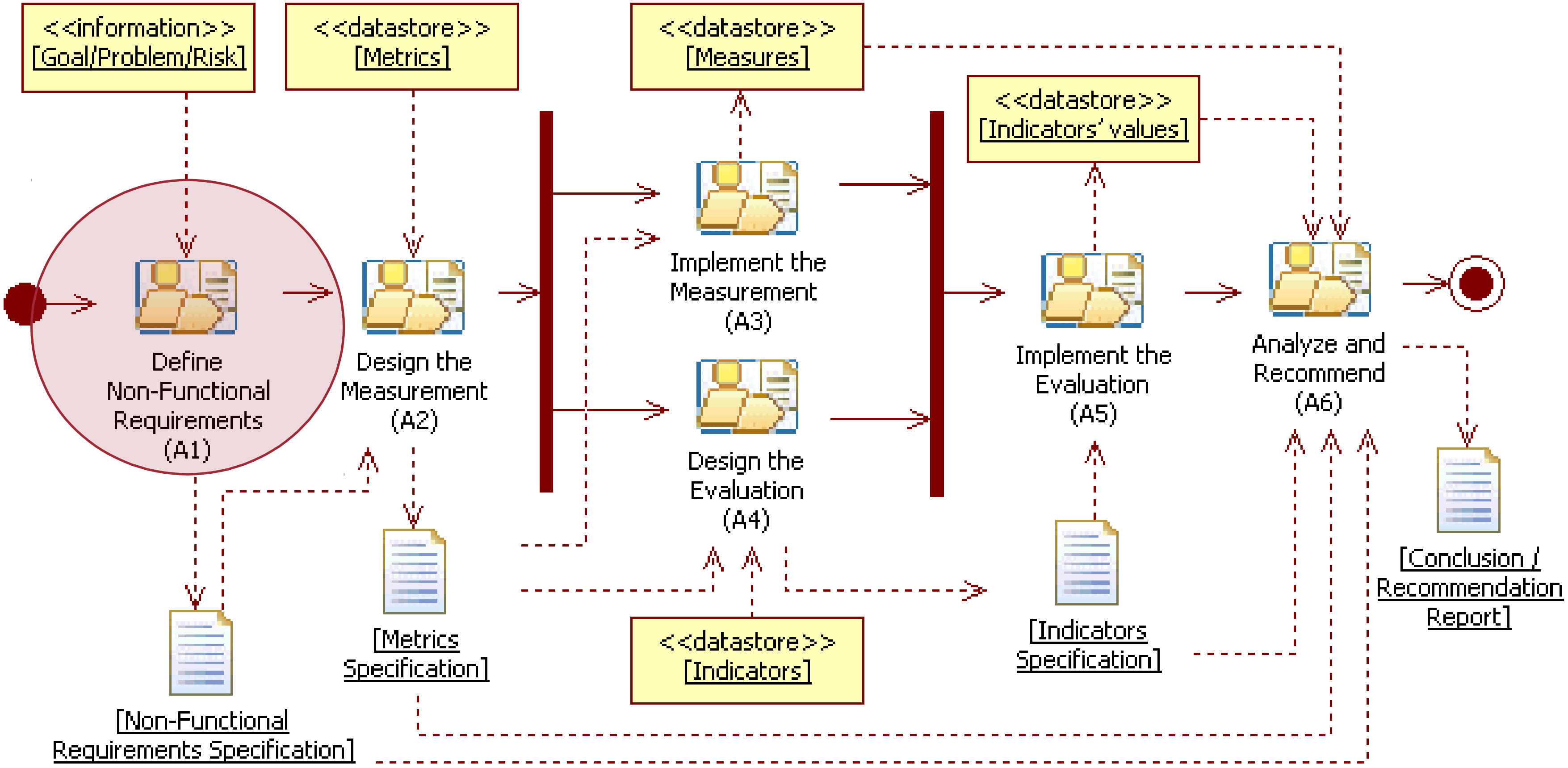
GOCAME Process: *Overview*

W5H mnemonic rule: ***Why, What, How, Who, When, Where?***


<<information>>
[Goal/Problem/Risk]
<<datastore>>
[Metrics]
<<datastore>>
[Measures]
<<datastore>>
[Indicators' values]
Define Non-Functional Requirements (A1)
Design the Measurement (A2)
Implement the Measurement (A3)
Design the Evaluation (A4)
Implement the Evaluation (A5)
Analyze and Recommend (A6)
[Non-Functional Requirements Specification]
[Metric Specification]
<<datastore>>
[Indicators]
[Indicator Specification]
[Conclusion / Recommendation Report]

GOCAME Process: *Define NFR*

W5H rule: ***Why, What.***


<<information>>
[Goal/Problem/Risk]
<<datastore>>
[Metrics]
<<datastore>>
[Measures]
<<datastore>>
[Indicators' values]
Define Non-Functional Requirements (A1)
Design the Measurement (A2)
Implement the Measurement (A3)
Design the Evaluation (A4)
Implement the Evaluation (A5)
Analyze and Recommend (A6)
[Non-Functional Requirements Specification]
[Metrics Specification]
<<datastore>>
[Indicators]
[Indicators Specification]
[Conclusion / Recommendation Report]

Define Non-Functional Requirements

The M&E information need **goal** is to understand the current quality satisfaction level achieved, particularly for non-vulnerabilities regarding the Security characteristic, from the security administrator user viewpoint, for a student management system widespread used in Argentinean national universities.

M&E Information Need:

Purpose: *Understand* (and later *Improve*)

User Viewpoint: *IT Security Administrator*

Entity Category (Target) **:** *IT System*

Entity (Target)**:** *SIU Guarani register system*

Quality **Focus:** *Security (Confidentiality/Integrity/Authenticity)*

Quality ***View:*** *External Quality*

Context: *Engineering School, UNLPam …* **Entity** (Source): *Attacker*

Define NFR: Requirements Tree

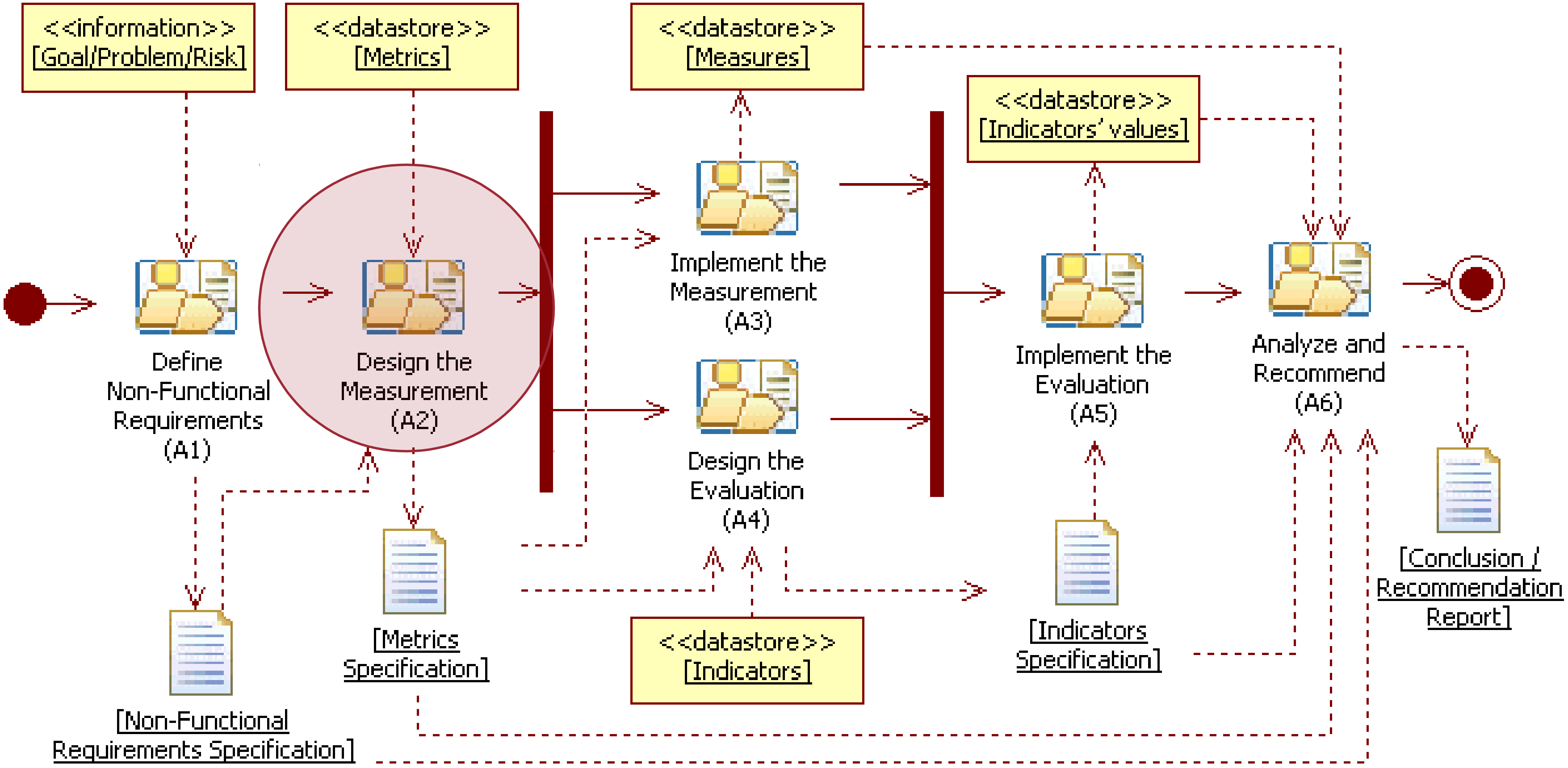
1. Security
   1.1. Confidentiality
      1.1.1. **Access Schema Protectability**
         1.1.1.1. Authentication Schema Bypass
         1.1.1.2. Password Aging Policy
         1.1.1.3. String Password Robustness
   1.2. Integrity
      1.2.1. **Cross-Site Scripting Immunity**
         1.2.1.1. Reflected Cross-Site Scripting Immunity
         1.2.1.2. Stored Cross-Site Scripting Immunity
         1.2.1.3. DOM-based Cross-Site Scripting Immunity
         1.2.1.4. Cross-site request forgery Immunity
   1.3. Authenticity
      1.3.1. **Session Impersonation Protectability**
         1.3.1.1. Session Data Disclosure Protectability
         1.3.1.2. Session ID Disclosure Protectability
         1.3.1.3. Session Non-Replay Protectability

Degree to which a product or system ensures that data are accessible only to those authorized to have access

calling an internal page that is supposed to be accessed only after authentication has been performed.

GOCAME Process: *Design the Measurement*

W5H rule: ***How***



Selected Metric for the Attribute 1.1.1.1

Attribute: ***Authentication Schema Bypass*** *(Coded 1.1.1.1)*

Attribute: ***Amount of successful attempts to access protected***

Attribute: ***Amount of attempts to access protected pages***

Per each **attribute** of the **requirements tree**, a **Metric** (either direct or indirect) should be selected from the ***Metrics*** *Repository*

Direct Metric:

Name: Total number of attempts to access protected pages (#TPP)
Objective: The total number of protected pages (i.e. the given population) to be attempted for access by a given technique
Author: Covella G. and Dieser A.
Version: 1.0

Measurement Method:

Specification: As precondition, log into the website with a valid user ID and password. Browse the site looking for the URL population of protected pages, which are those that must be accessed only after a successful login. Add one per each protected page URL selected.
Type: Objective

Numerical Scale:

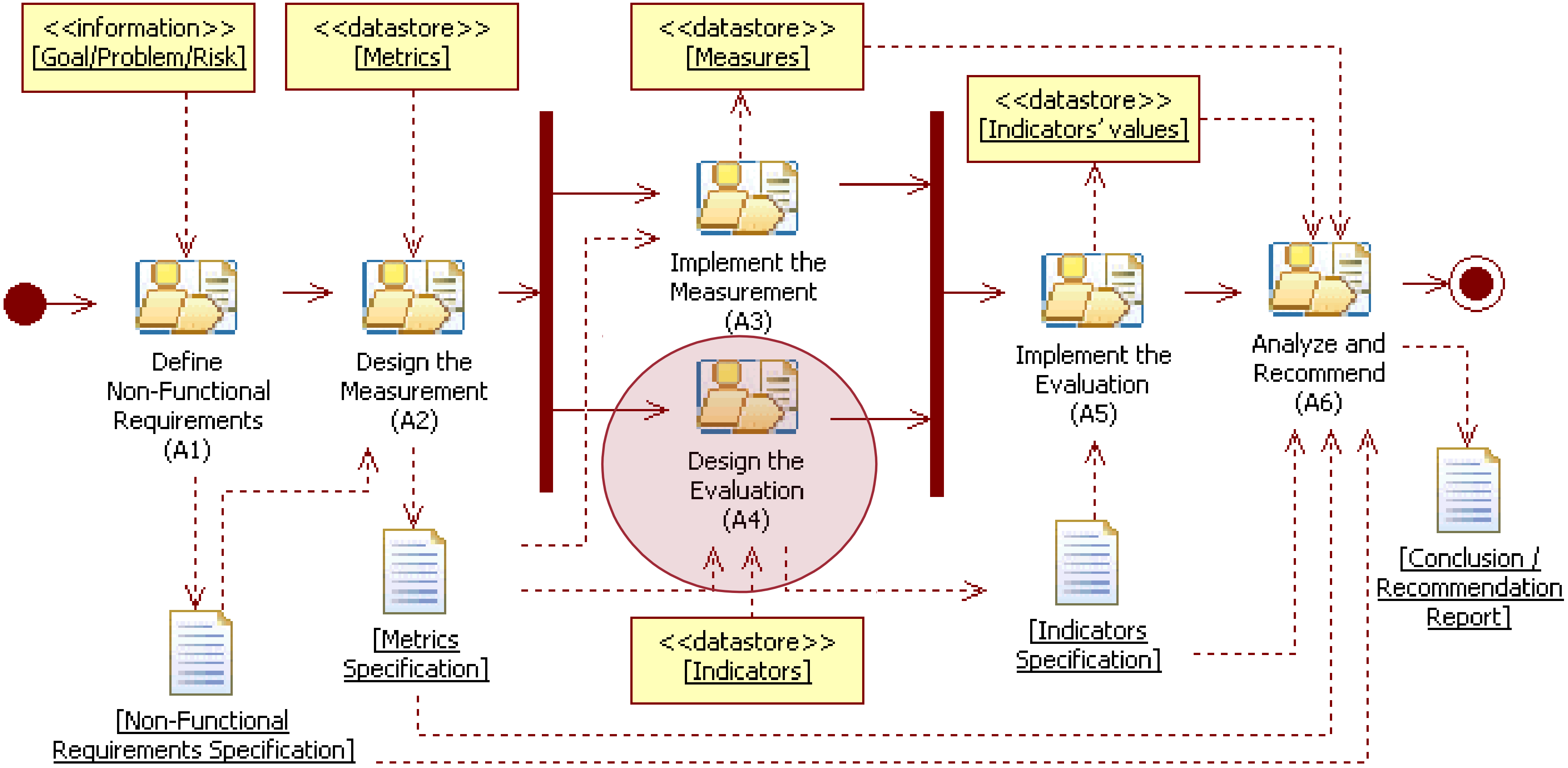
Representation: Discrete
Value Type: Integer
Scale Type: Absolute

Unit:

Name: Protected pages
Acronym: Pp

GOCAME Process: Design the Evaluation

W5H rule: *How*



<<information>>
[Goal/Problem/Risk]
<<datastore>>
[Metrics]
<<datastore>>
[Measures]
<<datastore>>
[Indicators' values]
Define Non-Functional Requirements (A1)
Design the Measurement (A2)
Implement the Measurement (A3)
Design the Evaluation (A4)
Implement the Evaluation (A5)
Analyze and Recommend (A6)
[Non-Functional Requirements Specification]
[Metrics Specification]
<<datastore>>
[Indicators]
[Indicators Specification]
[Conclusion / Recommendation Report]

Design the Evaluation: *Elementary Indicator*

Attribute: ***Authentication Schema Bypass***

Elemental Indicator:

Name: Performance Level of the Authenticatio

Author: Covella G. and Dieser A. **Version:**

Elementary Model:

Function Name: P_ASB function

Specification: the mapping is:

P_ASB = 100 iff %PPA < %PPAMIN ;

P_ASB = 80 iff %PPAMIN <= %PPA < %PPAMAX;

P_ASB = 0 iff %PPA >= %PPAMAX where %PPA is the indirect metric specified in Table III.

Decision Criterion: [Acceptability Levels]

Name 1: Unsatisfactory **Range:** if 0 ≤ P_ASB ≤ 60

Description: indicates change actions must be taken with high priority

Name 2: Marginal **Range:** if 60 < P_ASB ≤ 90

Description: indicates a need for improvement actions

Name 3: Satisfactory **Range:** if 90 < P_ASB ≤ 100

Description: indicates no need for current actions

Numerical Scale:

Representation: Continuous

Value Type: Real **Scale Type:** Proportion

Unit:

Name: Percentage **Acronym:** %

Per each **attribute** (*elementary NFR*) of the **requirements tree**, an **Elementary Indicator** should be selected from the ***Indicators** Repository.*

It uses data coming from the measure, interpreting it by means of the **Elementary Model**

Design the Evaluation: Global I

Global (Aggregation) Model:

Function:

Name: LSP (Logic Scoring of Preference)

Specification:

P/GI (r) = (W1 * I1r + W2 * I2 r + ... + Wm * Im r)

It aggregates **Elementary Indicators** into **Partial Indicators** and **Global Indicator** (regarding ***sub-characteristics*** and ***characteristics*** of the requirements tree).

Numerical Scale:

Scale Type: absolute **Unit name:** Percentage (%)

Decision Criteria/Acceptability Levels:

if 0 ≤ X ≤ 60: **"unsatisfactory"** →indicates change actions must take high priority.

if 60 < X ≤ 90: **"marginal"** →indicates a need for improvement actions.

if 90 < X ≤ 100: **"satisfactory"** →indicates satisfactory quality of the analyzed feature.

Summary of Work Contributions (1/3)

- "the awareness of the added value of supporting the IT security/risk assessment area with quality M&E methods and strategy, which are based on metrics and indicators"

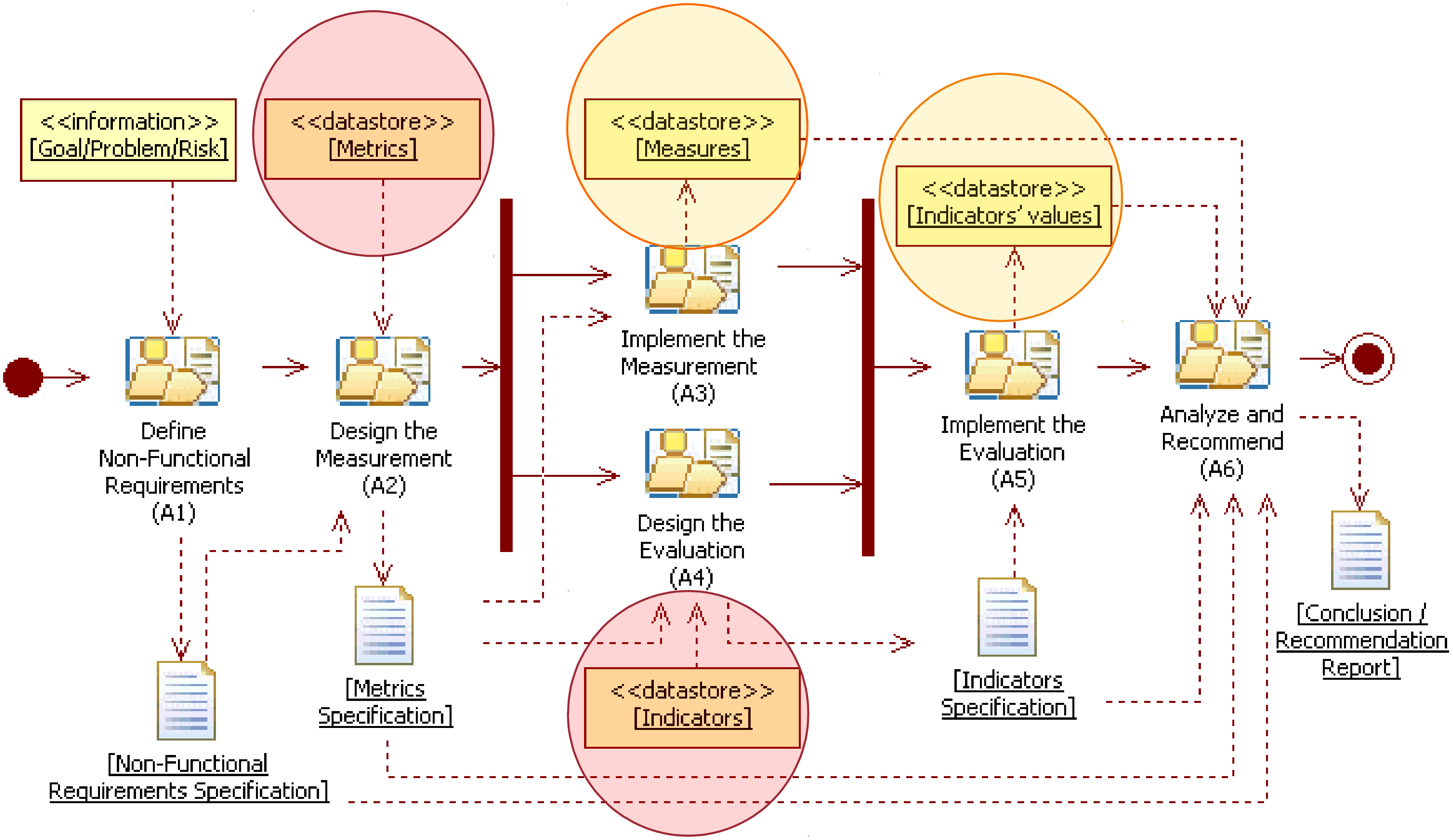
- The entrance gate is based on identifying vulnerable attributes of a target entity, which can be quantified by metrics and interpreted by indicators.
  - by using an evaluation-driven strategy as GOCAME, we can apply for security and risk assessment its **multi-criteria (attribute) decision analysis methods**

Summary of Work Contributions (2/3)

- “a thorough discussion about the specification of metrics and indicators as resources (work products) for measurement and evaluation process descriptions…”

- They are key organizational assets for providing suitable data and information for analyzing, recommending, controlling and ultimately decision-making processes
  - importance for **consistency** and **comparability** reasons recording not only **data sets** and **information** but also the associated **metadata**

GOCAME Process: *Data/Info* ***and*** *Metadata*



<<information>>
[Goal/Problem/Risk]
<<datastore>>
[Metrics]
<<datastore>>
[Measures]
<<datastore>>
[Indicators' values]
Define Non-Functional Requirements (A1)
Design the Measurement (A2)
Implement the Measurement (A3)
Design the Evaluation (A4)
Implement the Evaluation (A5)
Analyze and Recommend (A6)
[Non-Functional Requirements Specification]
[Metrics Specification]
<<datastore>>
[Indicators]
[Indicators Specification]
[Conclusion / Recommendation Report]

See example of **inconsistency of analysis** in Section III.C, 2nd and 3th paragraphs of the paper

Summary of Work Contributions (3/3)

- “the illustration of metrics and indicators from excerpts of an actual IT security and risk evaluation case study”

- The first goal is to understand the current quality (non-vulnerability) satisfaction level achieved to the *Security* characteristic for the SIU target entity ...
  - Once its current state is understood, the following purpose is to improve the SIU system in those weakly performed indicators; that is, to reduce its security risks.

Risk value for Attribute Ai = Probability of Event occurrence for Ai * Vulnerability Indicator value for Ai

Questions ?

Thank you for your attention!

2012
CEE-SEC(R)
Software Engineering
Conference in Russia

For further questions send an E-mail to: olsinal@ing.unlpam.edu.ar

Dr. Luis **Olsina**

GIDIS_Web

Departamento de Informática – Facultad de Ingeniería – Universidad Nacional de La Pampa

General Pico – La Pampa – Argentina