



Analyzing Risks in Organization through Goal-Oriented Approach

Yudistira Asnar

yudis.asnar@dit.unitn.it



Outlines

- ⇒ Motivations
- ⇒ Objectives
- ⇒ Tropos Goal-Risk Modeling Framework
 - ↳ Using Loan Originating Process
- ⇒ Risk Analysis
 - ↳ Actual Risk
 - ↳ Perceived Risk
- ⇒ Applications
- ⇒ Remarks



Motivation

- ⇒ Information systems (ISs) are critical for business
 - ↳ E.g., corporate images, customer loyalties, business continuity, etc.
- ⇒ Development IS starts by defining requirements
 - ↳ "Things" that the stakeholders intend to be achieved
- ⇒ How about things that are undesirable things ?
 - ↳ Let's deal later with some safeguards; in the phase of design or even more (e.g., implementation)
- (-) consequence:
 - ↳ requirements might be need to be revised to adopt safeguards
 - ↳ safeguards may conflict with some requirements



Motivations (2)

- ⇒ An enterprise is composed by many roles that are played by many agents
- ⇒ Risk management is done following the interest of enterprise.
- ⇒ An enterprise is only one of the stakeholders
- ⇒ How about the risks that is perceived by other stakeholders?
 - ↳ may perceive a higher/lower risk than the actual one
 - ↳ Over-react
 - ↳ Under-react

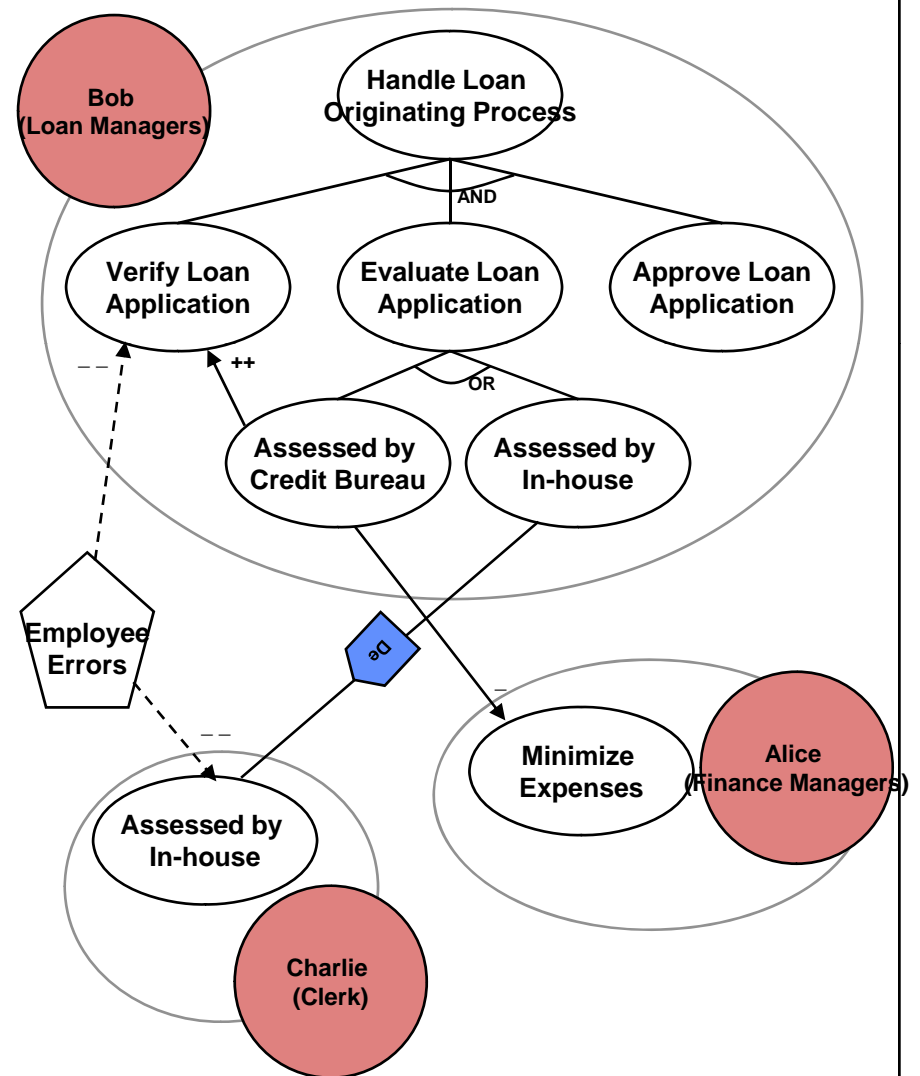


Objectives

- ⇒ Risk is an uncertain event that impacts (negatively) to the goals of stakeholders - (ISO Guide 73, 2002)
- ⇒ Analyzing **risks in the earlier phase** of IS development (requirement phases) and analyze also the **organizational- setting** where the IS will be operated
- ⇒ Providing modeling framework that:
 - ↳ operate using: **subjective and objective** input
 - ↳ assess **actual risk and perceived risk**

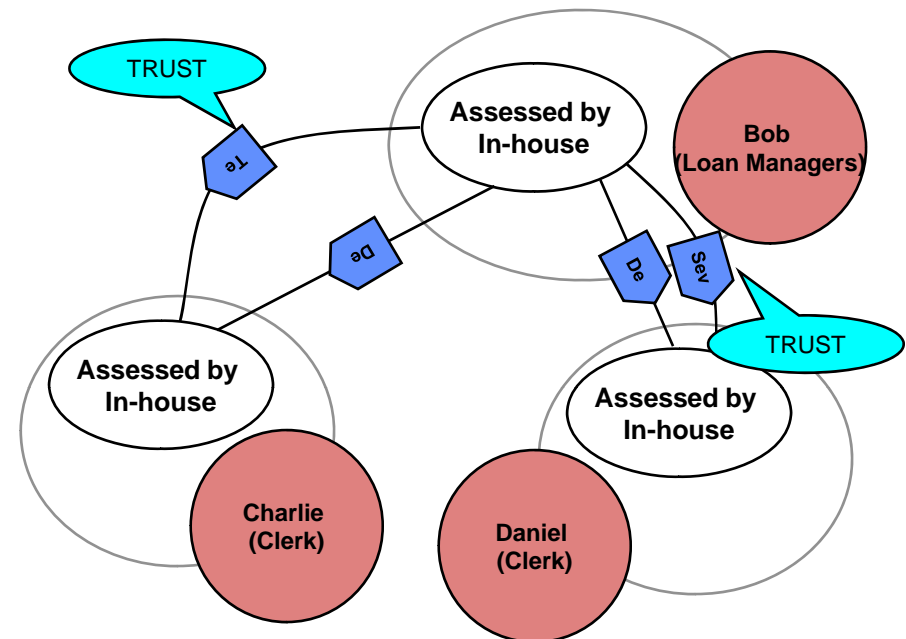
Tropos Goal-Risk Modeling Framework

- ⇒ Define **strategic-interests** of stakeholders
 - ↳ Stakeholders: Bank, Bank Manager, Clerk
 - ↳ Interests: Handle Loan Application, Minimize Expenses
- ⇒ Analyze strategic interests
 - ↳ Refinement
 - ↳ Alternative
 - ↳ Delegation
 - ↳ Side Effects/Contributions
- ⇒ Define **events** that may impact the stakeholders
 - ↳ E.g., Employee Errors



Analysis - Perceived Risk

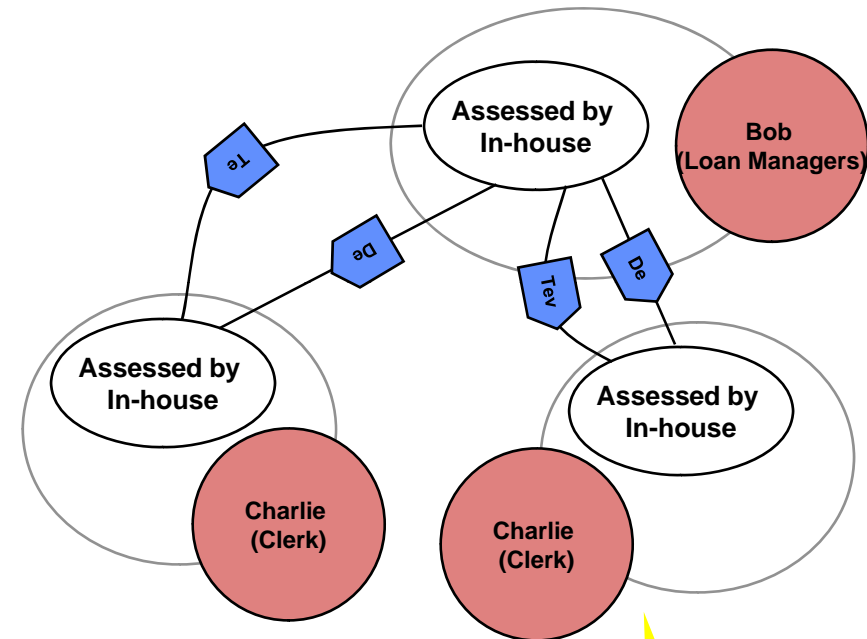
- ⇒ Perceived Risk - the belief of actors about the risk that exists in a delegation
- ⇒ Important!!
 - ↳ **Under-react**: if an actual risk is high and the actor doesn't perceive it
 - ↳ **Over-react**: the actor believes that s/he is exposed to high risk though the system is secure and dependable enough
- ⇒ Trust and loss are key factors to shape the perceived risk of an actor



- ⇒ An activity is perceived as risky:
 - ↳ Its failure results in high disadvantages/loss
 - ↳ The managing actor is untrustworthy
 - ↳ Information provided by non-trusted actors

Analysis - Perceived Risk (2)

- ⇒ Define threshold of **Risk-Factor** for each actor
- ⇒ In case of perceived risk is **too high/low** in Bob rationale
 - ↪ It is not always **real**
 - ↪ OK? Treatments need to be adopted to deal with such issue



Qualitative
vs
Quantitative



Applications

- ⇒ Assessing risks (actual and perceived) in organizations [CRITIS-06,ARES-07]
 - ↳ E.g., Loan Originating Process, London Ambulance Service, ATM
- ⇒ Eliciting requirements with considering risk analysis [CRITIS-06,EEDC-06]
 - ↳ Requirements = Intentions + Treatments of Risks
 - ↳ E.g., ATM, Car Manufacturer
- ⇒ Forming organizational-setting [AOSE-06]
 - ↳ Considering: trust among actors, capability
 - ↳ E.g., Forming Partial Delegation Airspace
- ⇒ Specifying and Verifying Secure and Dependable Patterns [RE-07]
 - ↳ Context-Requirement-Solution
 - ↳ E.g., ATM, Smart-Items, e-Business, e-Government
- ⇒ Implementing Intelligent Agent [AOSE-07]
 - ↳ Unmanned Aerial Vehicle using JACK



Conclusions

- ⇒ Analysts can introduce some safeguards as part of requirements even without defining the system architecture
- ⇒ Tropos GR model can be used for assessing **actual-risk** and **perceived-risk**
- ⇒ Tropos GR model is able to assist analysts in **developing** business-critical systems (e.g., Loan Originating Process) or **assessing** the existing system



Future Works

- ⇒ Derive/Assess architectural design following the result of Tropos Goal-Risk analysis
- ⇒ Assessing availability-reliability of systems through the goal models of the business
- ⇒ Moving towards next phases of Risk Management
 - ↳ Risk Planning, Risk Monitoring-Controlling, Risk Reporting
 - ↳ Ideally, risk reporting complies with any particular standard (e.g., ISO 16085) or regulation (e.g., SOX)



Thank You

This work has been partially funded by
EU Commission: SENSORIA and SERENITY projects
FIRB program of MIUR: ASTRO and TOCAI projects
Provincial Authority of Trentino: MOSTRO project

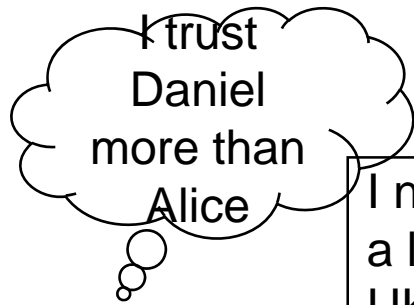


References

- ⇒ [**CRITIS-06**] Asnar, Y. & Giorgini, P., Modeling Risk and Identifying Countermeasures in Organizations, *CRITIS '06*
- ⇒ [**EDCC-06**] Asnar, Y. & Giorgini, P., Ensuring Dependability in Socio-Technical System by Risk Analysis, *EDCC '06*
- ⇒ [**AOSE-06**] Asnar, Y.; Bryl, V. & Giorgini, P., Using Risk Analysis to Evaluate Design Alternatives, *AOSE '06*
- ⇒ [**ARES-07**] Asnar, Y.; Giorgini, P.; Massacci, F. & Zannone, N. From Trust to Dependability through Risk Analysis, *ARES '07*
- ⇒ [**AOSE-07**] Asnar, Y.; Giorgini, P. & Zannone, N., Implementing Risk Reasoning in Jadex Agents, *AOSE '07*
- ⇒ [**RE-07**] Asnar, Y.; et. Al., Secure and Dependable Patterns in Organizations: An Empirical Approach, *RE '07* (to appear)



Example for Forming Organization



Boss

I need to write
a letter to the
UK embassy

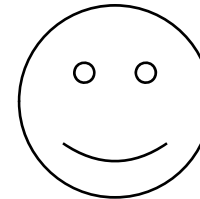
...to write a letter means:
type, print and certify it with
stamp and boss's signature

I can only
sign letters...



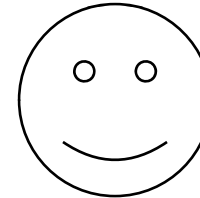
Daniel

I know
English



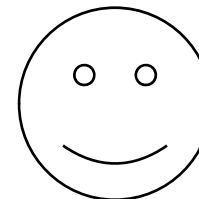
Alice

I know
English



Bob

I can use
printer



Charlie

I have an
official stamp

Taken from V. Bryl's Presentation