RISK ASSESSMENT FOR EXTERNAL VENDORS

Luciano Ferrari, CISSP, MBA
lferrari@lufsec.com
www.lufsec.com
November, 2013

Risk Assessment is Difficult

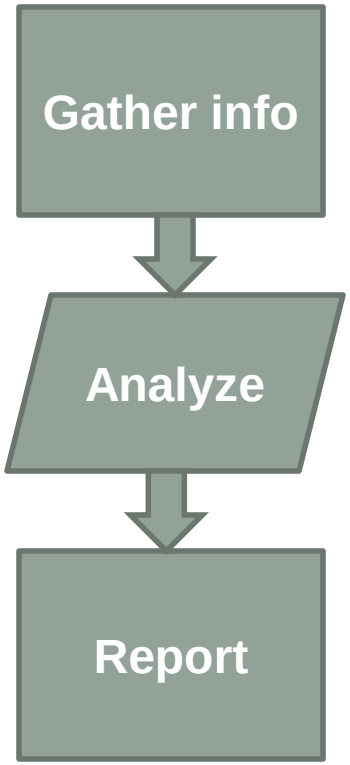
- Multiple scenarios
- Interpreted as a negative activity
- Single method/tool not practical
- Requires key competencies

Categorize your cases

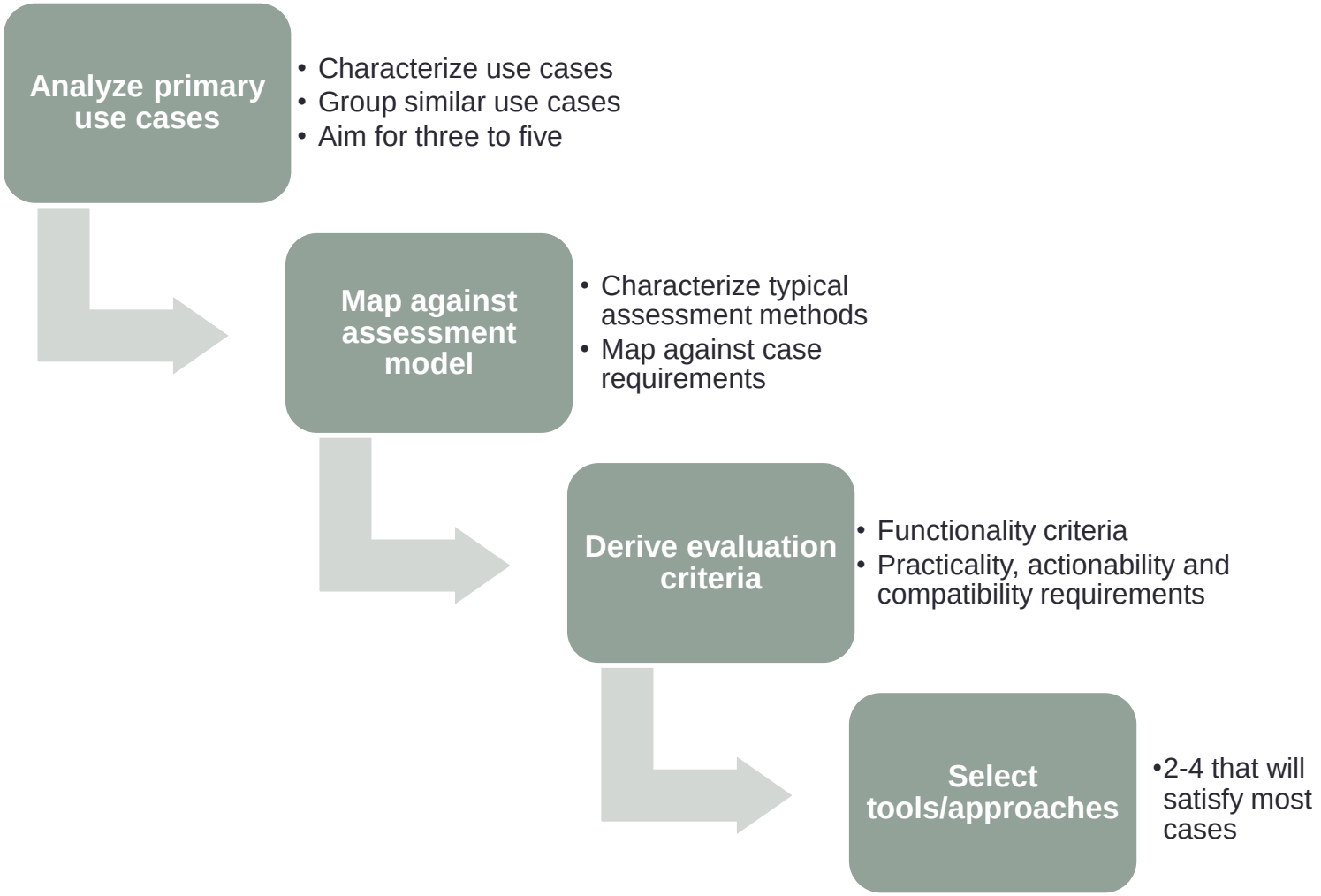
- Standardization/Consistency is good
- Less complexity, less risk
- Experience is a key element

Prerequisites for selection a toolbox

- Typical use cases for Risk Assessment
- The various approaches for risk assessments
- The characteristics of available methods/tools



Selecting the tools/methods



Examples – functionality assessment

Cases	Project/ Procurement	DRP/BCP	ERM Rollup/ Compliance	Security Prioritization
Explore: People	One-to-one interviews and scenario planning	Survey questionnaire	Scenario planning and collective brainstorm	Survey questionnaire and one-to-one interviews
Explore: Systems	Risk inventory	Vulnerability analysis and threat inventory	Threat inventory	Threat inventory
Assess: Qualitative	-	What-if-modeling	Deviance and intuitive	Ranking and intuitive
Assess: Quantitative	Automated calculation		-	-
Express	Absolute/ scalar ALE	Scenarios	Dashboard and heat map	Heat map and projects/ actions

Tools/Methods

	Explore	Assess	Express
FRAP	Collective brainstorm (facilitated workshop)	Intuitive/discussion/ranking Deviance	Scenarios and actions
ISF SARA and SPRINT	Questionnaires/scorecards	Quantitative: Intuitive/discussion, deviance from controls/standards	Scorecards
ISF IRAM	Workshops	Qualitative: Scenario-based discussion/brainstorm	Status reports and controls
Citicus ONE	Questionnaires/scorecards	Qualitative: Intuitive, deviance from controls/standards	Status/heat maps, action plan
OCTAVE	Collective brainstorm (facilitated workshop)	Qualitative: intuitive against threat profile, catalog of vulnerabilities	Action Scenarios, projects/actions
GRAM	Scenario planning	Qualitative: Delphic what-if modeling	Scenarios
RiskWatch	Survey Questionnaire	Qualitative: Deviance from standards. Quantitative: Monte Carlo simulation	Risk status reports, absolute ALE, return on investment, actions
CRAMM	Asset register, threat/vulnerability inventory,questionnaire, workshop	Qualitative: deviance, what if modeling, automated calculation. Qualitative: BIA	Actions: Scenarios: controls, risk profile, register, risk score

Information Classification

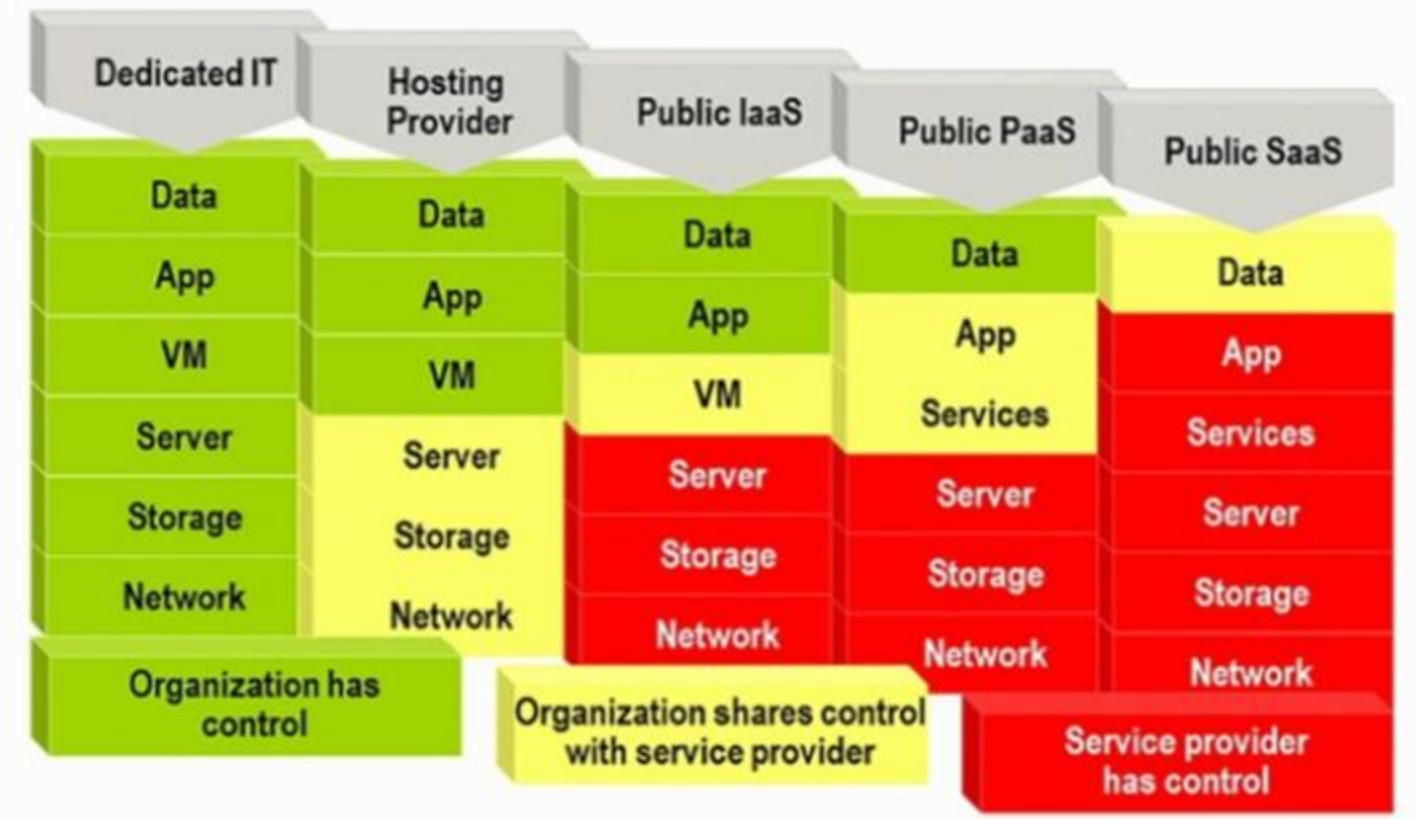
- If you don’t know what to protect and where it is how can you protect?

Information Security is not an island

- Formal engage with other areas is key
- Risk Management
- Legal
- HR
- Procurement

Risk Assessment for Cloud Providers

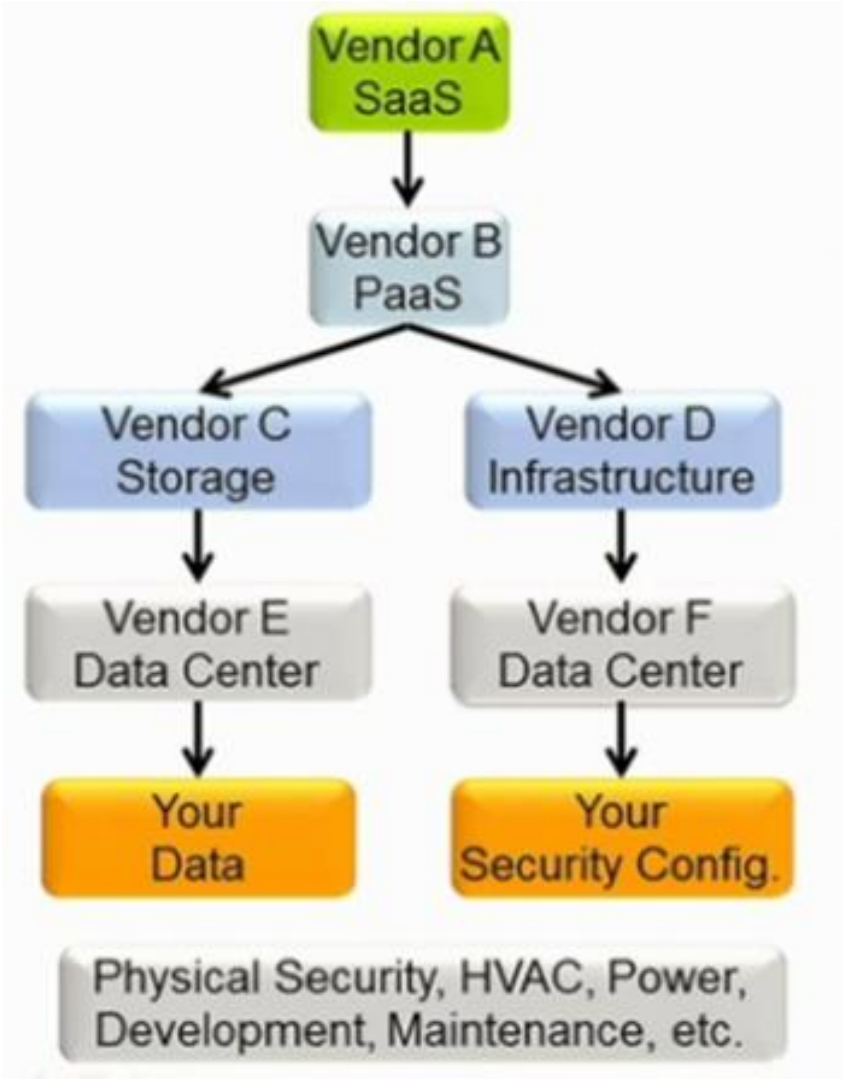
Control implications of different models



Accountability cannot be outsourced

Master Agreement / SLAs

Tree of Provider Chains



- Are you aware of all the parties?
- Will you be notified when parties change?
- Does your contract require all parties to comply with it?
- Do you force clauses applying to the entire chain of providers?
- How visible are the finances of the parties?

What service level to look for?

- Planned Downtime
- Service Availability
- Support/Mean time to restore service
- Data recovery
- RTO/RPO

Risk Assessment on Social Media

Top Social Media issues

- Employee productivity
- Record Retention
- Company reputation/image
- Inappropriate content posted by employees
- Compliance with regulation/laws
- Discovering and assessing social media risks

How and what to monitor?

- Analysis
- Assessment
- Mitigation

Action Plans

- Don’t wait for a call from marketing to get involved.
- Think of social media as your most popular cloud platform.
- Integrate social media processes and drivers into risk assessment processes.
- Accept the reality that your enterprise has social risks to manage.

Regulation

- HIPAA
- PII
- PCI
- GBA
- SOX

- Use the new grouping model
- Engage other areas or your organization
- Promote Risk Assessment Awareness
- Use it for vendor selection criteria
- Continuous Improvement