RSAConference2016

Singapore | 20-22 July | Marina Bay Sands

SESSION ID: SDS1-R09

The Journey: From Right Objectives to a Measurable GRC System

Lenka Fibikova

IT Governance, Risk and Compliance
Marina Bay Sands

#RSAC

Introduction—the past

- In the 1990s
  - No legal or regulatory requirements for an ISMS or IT GRC
  - The term IT Governance just emerges
  - Standards start appearing
    - German IT Baseline Security Handbook first published in 1994
    - British Standard BS 7799 first published in 1995
  - Security and IT goveranance driven by a few who understood the importance of organization’s resilience long time before they became buzz words

Introduction—today

- Beginning of the century more and more governments and regulatory bodies releasing their security and governance requirements
- The consequence: From resilience of a few to struggle for compliance by everybody
- The cure:
  1. Relieve the pain (address the hot topics)
  2. Strengthen the body (build organization’s resilience)

Outline

- What we **know**
  - Proper governance is important—standards and best practices exist
  - Metrics are important—various lists of metrics can be found
- What we **don't know**
  - Which best practices and metrics are important to achieve my objectives?
  - Do the best practices and metrics cover my full scope or just an insignificant portion of it?
  - Do I have proper data to feed the metrics? How shall I collect it?
- What you will **learn**
  - How to define a measurable IT GRC system in 5 steps
  - It needs a lot more that just metrics: from objectives to metrics and deliverables

Step 1:
Why do you want an GRC? or Know your pain points

Defining the scope: Requirements

External Compliance

- Requirements of a regulatory body
- SOX
- PCI
- PDPA

Internal Priorities

- Decrease costs of IT
- Clean-up after a recent incident
- Decrease number of incidents
- Protect company’s IP
- Prevent/detect security breaches

Dos and don'ts

Do

- **Diagnose**: Listen to the management, ask questions, understand the circumstances
- **Correlate with what you know**: What causes/could cause the biggest losses
- **Use your professional judgment**: Know the external requirements and standards

Don't

- **National and international standards are not a pain point**—use them as your guidelines, but don't present them unless the management has real motivation to implement them
- **Don't assume you know what the company needs**—you possibly do, but it's not important if the management has other priorities

Step 2:
Where do you need a GRC? or
Know your treasures

Defining the scope: Org structure

Organizational

- Defined business areas (e.g., regulated vs. not regulated)
- Defined legal entities (e.g., high vs. low profit)

Geographic

- Specific countries (e.g., based on local legislation, country-specific risks)

Dos and don’ts

Do

- Consider the following factors:
  - **Criticality of the area**
  - **Level of pain** (areas with a lot of requirements)
  - **Management’s resistance to pain,** (management support)
- Understand your authority in the selected areas

Don’t

- **Don’t rush through this stage**
- If going global, **don’t underestimate power of the local lords**
- **Out of scope should not mean out of sight**—your scope defines your focus, but keep all areas in your peripheral vision; and be ready to pull them in the focus area if needed

Step 3:
What do you want to achieve? or
Word your story

Think big—start small

Start Small

- Define your scope as an onion
  - **Musts**: The areas with the biggest pain
  - **Shoulds**: You see them as critical, but the management doesn't feel the pain
  - **Nice to haves**: Not critical for the set objectives, but would make the life significantly easier or the organization significantly more robust
- **Word stories for the 'musts'**
  - What will be done?
  - By when?

Think Big

- Be like a chess player—think several steps ahead:
  - Is your solution applicable to other areas currently not in the scope?
  - Is your solution flexible and scalable?
  - Where yes? Where not? What would be the strategies when expanding the scope
  - Would any goals set today significantly reduce your handling options tomorrow?

Dos and don’ts

Do

- Picture **how the organization will look in one year**
- Define deliverables small enough to **show progress every month**
- **Prioritize** the high-critical areas
- **Align your approach with the existing best practices and standards**, but…
- Keep in mind that every organization is unique—**take only what fits** to your circumstances

Don’t

- **Don’t ignore ‘shoulds’**: Don’t hide any important findings of your analysis
- **Don’t write a long report**: Nobody has time to read it
- **Don’t request a bit project** taking several years
- Don’t try to **blindly implement a standard**
- **Don’t plan much beyond one year**—everything will be different

Step 4:
How do you want to achieve your goals? or
Build the framework

Governance: Setting up requirements

GRC Framework

- **G**: Policies/Standards/Standard Operating Procedures
- **R**: Risk management objectives, risk assessment methodology
- **C**: Looking for evidence, compliance assessments, handling findings
- Tools? Let’s talk about them later…

1. Set up baselines (requirements)

- For each of your stories, consider:
  - What are the requirements?
  - Do you already have any related policies/standards/procedures?
- Requirements on the GRC vs. requirements on various IT subjects
- Define—modify—align

Compliance: Making things measurable

2. Collect evidence (records)

- For each of your requirements, what are possible evidences for their fulfillment you could find?
  - Automatic vs. manual
  - Continuous vs. repeated vs. ad hoc
- How much evidence is
  - necessary (minimum) vs. efficient (maximum)
- Where will the evidence be stored?
  - Protection against modification

3. Measure (metrics)

- What metrics can be build on the collected evidence?
  - Compliance metrics
  - Performance metrics
- How the metrics will be evaluated
  - Automatic tests vs. manual assessments
  - Notifications vs. reports vs. dashboards

Dos and don'ts

Do

- **Define all 3 elements** (requirements, records, and metrics) for each of your stories
- All elements must be **pragmatic**
- **Balance** between the risk to the organization and needed resources
- **Be a catalyst**—provide the necessary substance to trigger the right reactions

Don't

- **Don't follow a level-by-level implementation using a maturity model**—maturity models are good for evaluation but not for driving progress; an upgrade to a higher level in all already defined areas is too complex and doesn't enable prioritization
- **Don't assume you know the best way to solve the organization's problem**—it's not your journey
- **Don't push in areas where the organization is not ready**—but point out the problems

Tools

Do I need tools?

- Use of tools enables automation and change control which makes
  - The **controls** more efficient ⇒ better acceptance + use of wider spectrum of controls possible
  - The **activities** more transparent ⇒ more understanding of what is happening
  - The **results** more reliable ⇒ more credible GRC system

Oh, the tools…

- Are not quite user-friendly
- Are no panacea: there will not solve your problems, only will help to manage them
- Garbage in—garbage out: The data must be maintained

Step 5:

Are we done now? or

Don’t forget to execute

Execution: Implement and oversee

Deliver and support

- **Deliver** your part
  - GRC Framework need to be delivered and run by you
  - Executing GRC controls is job of the IT teams
- **Awareness** is the key
- **Train** people to execute as expected
- Show that you're there to **support**—but don't do their job

Evaluate and report

- Check whether **data (records) have been created as expected**
  - Automatic: Are there any notifications if the collection fails?
  - Manual: Initial resistance or negligence is usual
- **Evaluate the data**
  - What are the indicators? What are the trends?
  - Are the results plausible?
- **Report the results**
  - Meetings vs. reports vs. dashboards

Execution: Handle risks

Basic: Handle deviations

- Triggers:
  - **Findings**: When metrics show non-compliance or poor performance
  - **Incidents**: When abnormalities in operations occurred
- Questions:
  - What is the risk from the non-compliance/poor performance?
  - What is the risk of re-occurrence of same/similar incident
- Belongs to “relieving the pain”

Advanced: Handling uncertainties

- Trigger:
  - Any situation which is not covered by the Governance Framework yet
- Question:
  - What can go wrong?
- Whereas deviations provide clear boundaries for the risk assessment, handling uncertainties is more fuzzy
- Belongs to “building resilience”

Dos and don’ts

Do

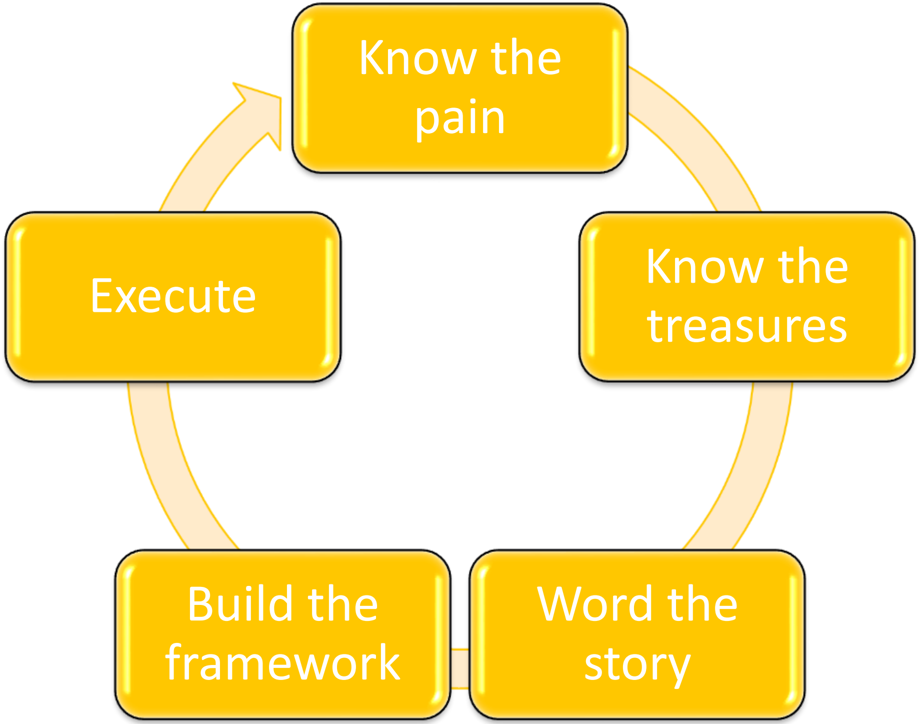
- **Deliver** your part on time
- **Respond** to all concerns and questions
- **Distinguish providing support and doing job of others**
- **Start working on the next cycle** (analyzing the pain points) as soon as you enter this phase

Don’t

- **Don’t assume that everything will run by itself and smoothly**
- **Don’t hesitate to stop activities** if they don’t bring the expected value

Summary

Summary


Know the pain

Know the treasures

Word the story

Build the framework

Execute

Apply

- **Next week** you should:
  - Set up your schedule for the first 3 steps (1. know the pain, 2. know the treasures, and 3. word the story)
- **In the first three months** following this presentation you should:
  - Analyze the status quo
  - Word the stories and get the senior management feedback
  - Set up your implementation plan (steps 4. build the framework, and 5. execute)
- **Within six months** you should:
  - Deliver the first results
  - Improve your stories and plans if necessary

Thank you for your attention…

Questions ?

Example scenario (Steps 1 and 2)

1. Know your pain

- SOX audits show repeating issues especially in removal of access control

2. Know your treasures

- The organization has 3 main entities (the HQ in Europe, one in the USA and one in Asia) generating the most profit and several small entities
- Two of the organizations—the HQ and in Asia—use a centralized ticketing system, the third one has a proprietary system

Example scenario (Steps 3 and 4)

3. Word your story

- **Must**: Proper access control procedures
- **Should**: SLAs for business department for requesting access removal
- **Nice to have**: Contractors on- and off-boarding via HR; automation and tool standardization across the organization

4. Build the framework

- Set up a policy (company-wide) that all access rights have to be removed within 24 hours
- Set up an SOP to ensure that—might be slightly different in the subsidiaries depending on the ticketing systems
- Use the ticketing systems as the evidence collector
  - In the HQ and A, the system can automatically send notification upon the SLA failure
  - In the USA manual reviews will be done by the staff till a notification built in the system
  - Rollout in other subsidiaries would require bringing them on the same platform otherwise too much admin overhead

Example scenario (Step 5)

5. Execute

- Time to time run a report in the HQ ticketing system
- Regularly check that the review are executed in the USA subsidiary