

14th to 15th Oct - Lisbon -PT

IT GRCmeeting

Governance, Risk & Compliance

2011



Business Oriented Risk Management Approach

2nd IT GRC Meeting
2011 - Lisbon

1. The problem
2. State of the Art
3. Business Oriented Risk Management Approach
4. Enlightenment starts here and now
5. Prioritizing investments
6. Ensuring repeatability
7. A Global Risk Framework
8. Conclusions
9. Q & A

Modern organizations, which want to ensure information security of their assets, need to establish and maintain effective information security management systems. These systems, in turn, must integrate a well balanced set of safeguards selected on the basis of the existing risks and business needs.

What are your organization's most pressing IT Risk issues? The answer probably depends somewhat on your job and the perspective it gives you.

It's always about managing risk at some cost. In the absence of metrics, we tend to over-compensate and focus on risks that are either familiar or recent.

Risk management needs to be business-oriented.

Identify assets and processes that are critical to business and determine what must be done to protect them.

The problem

1. That's too generic – I don't see how it can work.

E.g. “new version will be released late” it says nothing about the real problem – potential reason why there can be a slip.

A reason should be named, not a result.

2. That's too detailed – I don't understand the problem.

E.g. “problems with multithreading in new API function will result in overrunning code complete milestone”, that's something no one understands.

Either make it understandable or throw it away.

3. Where's the avoidance plan?

Usually it's easy to name the threat and rather not difficult to find an emergency plan. But when you don't equip your risk with a good avoidance plan it's almost worthless.

Of course sometimes no matter how hard you try you won't come up with anything reasonable. Then you just accept the risk is going to materialize.

4. I don't see any change ...

In the top 5 list there's always the same set of risks, the same set of people responsible for them and the same things told. "This week nothing changed."

If really nothing changed person responsible for the risk should be "ashamed". Usually something has changed but it's not reported because it doesn't seem important.

The problem

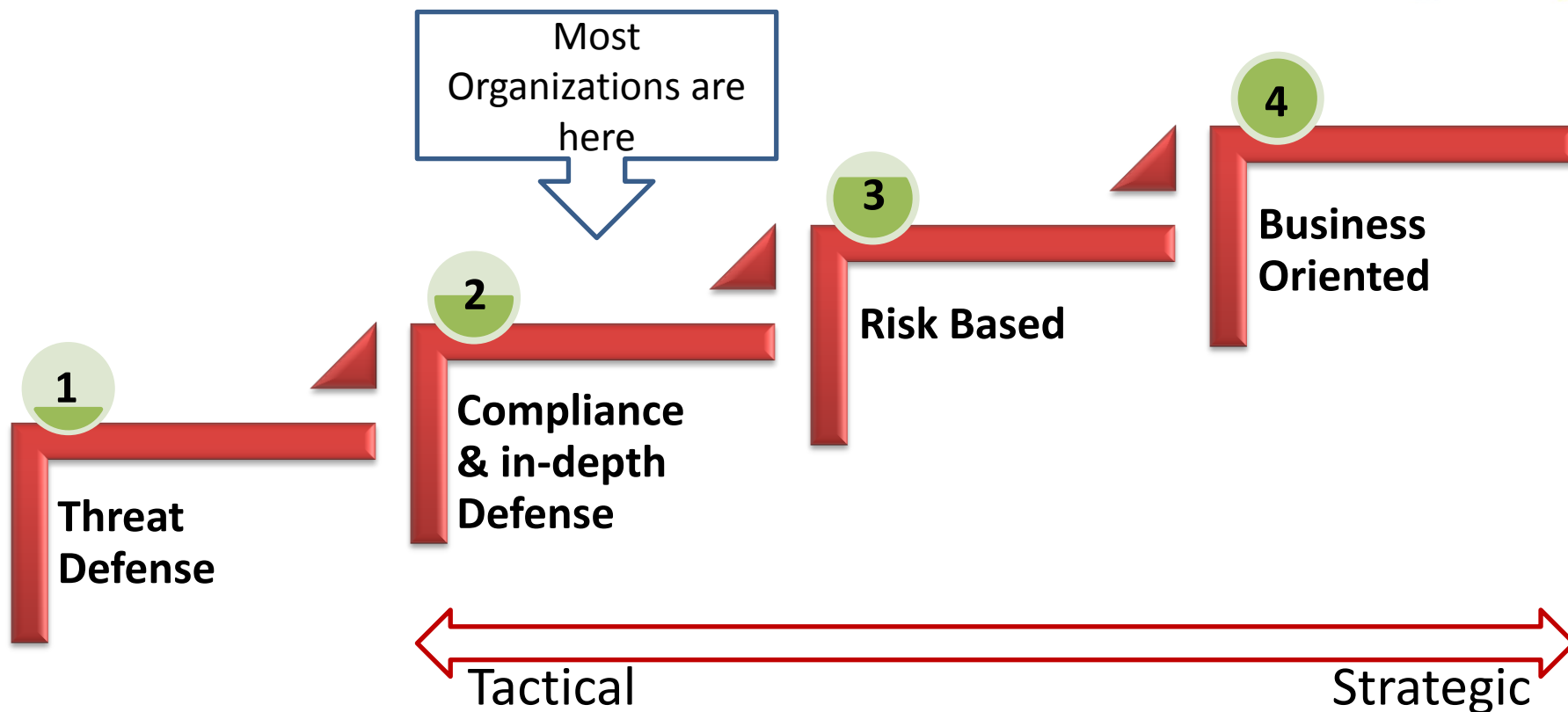
5. Hey, that's yet another thing I have to do!

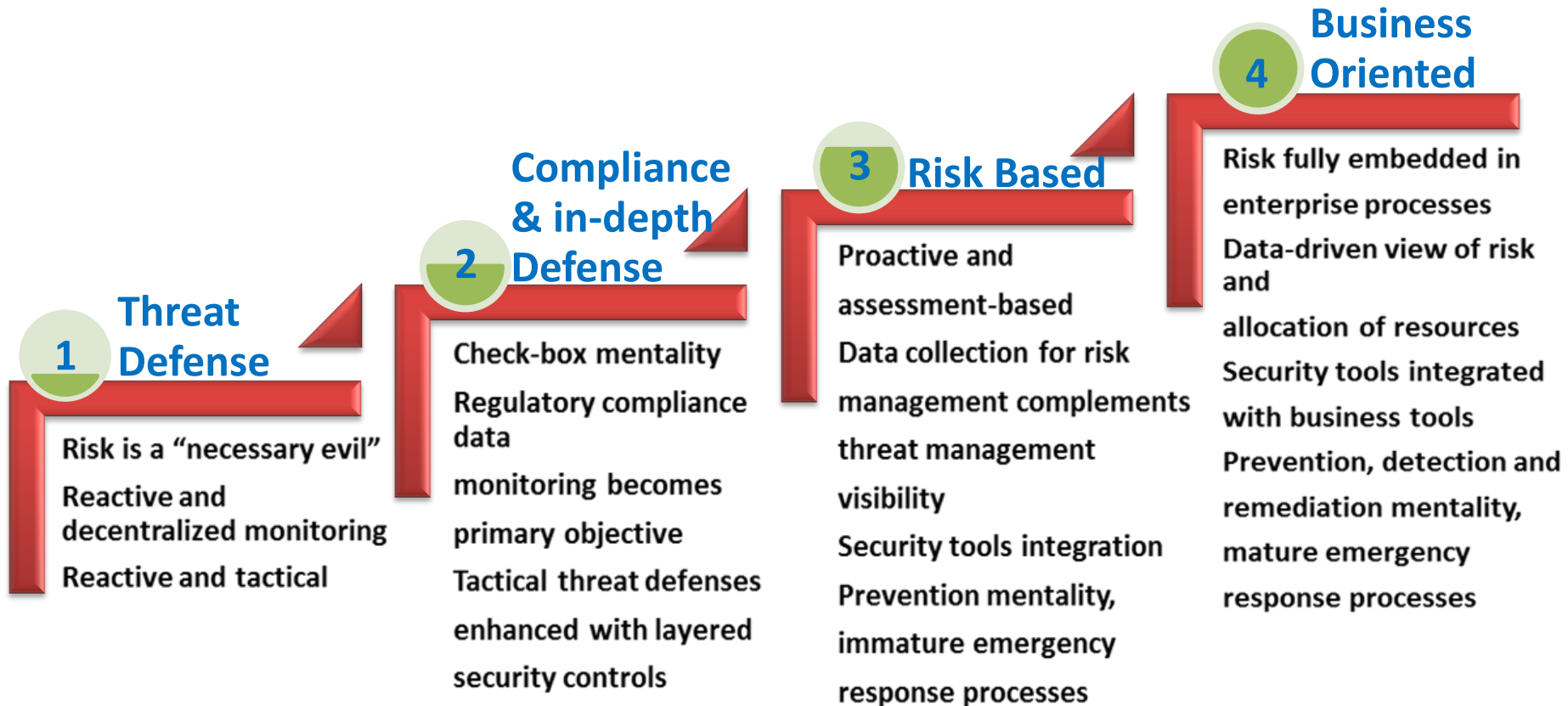
Unless people believe that it really works it'll always be something they do because they have to.

6. I don't believe in that!

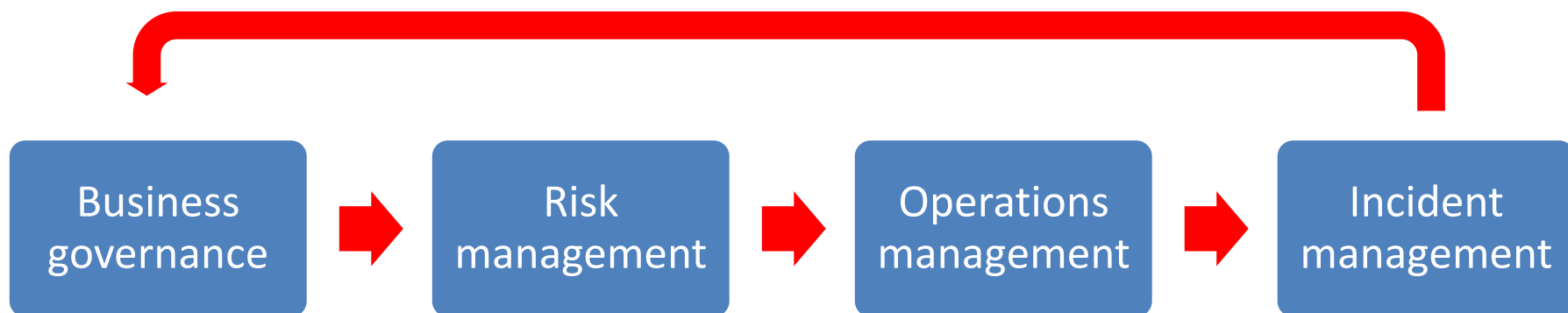
Unless people believe that it really works it'll always be something they do because they have to. Even when it starts working, results are usually seen from the management level but most of the team doesn't see a difference.

They have to see it work!

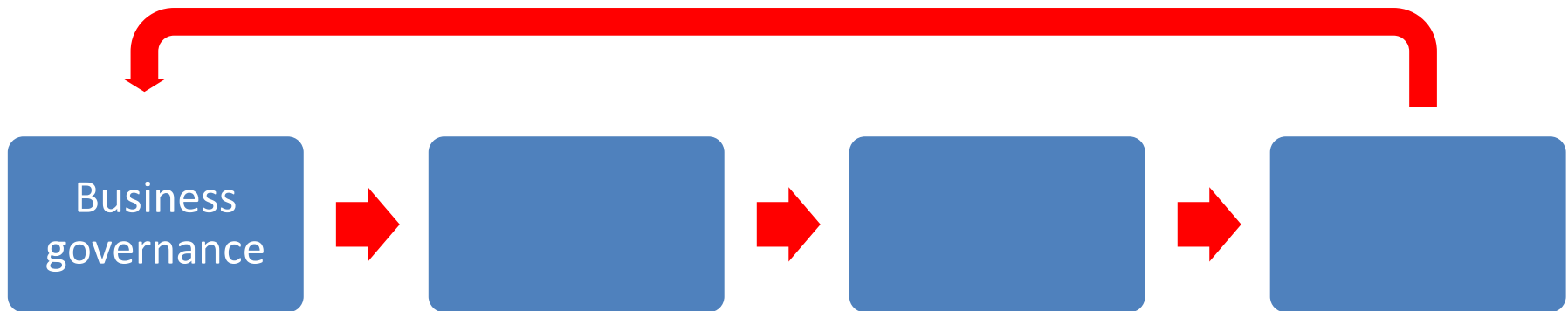




... Oriented Risk Management Approach:

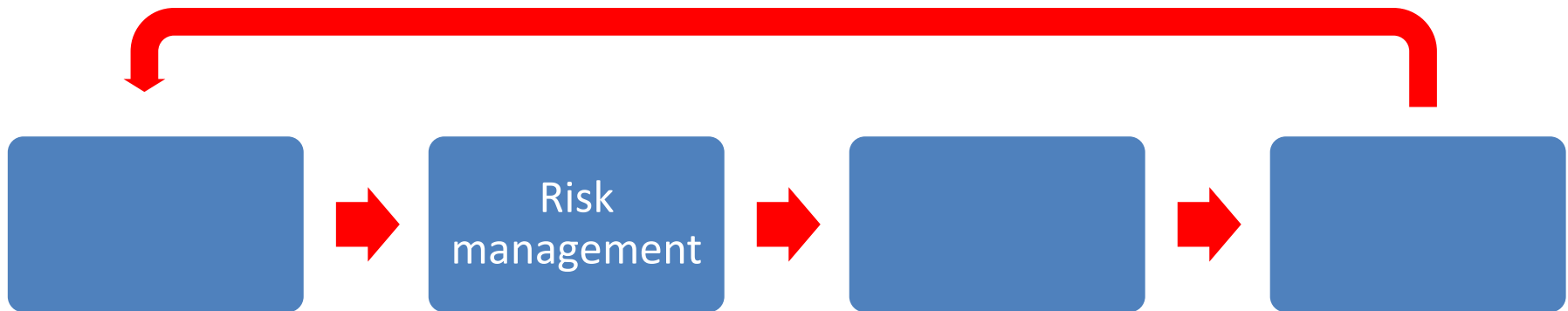


... Oriented Risk Management Approach:



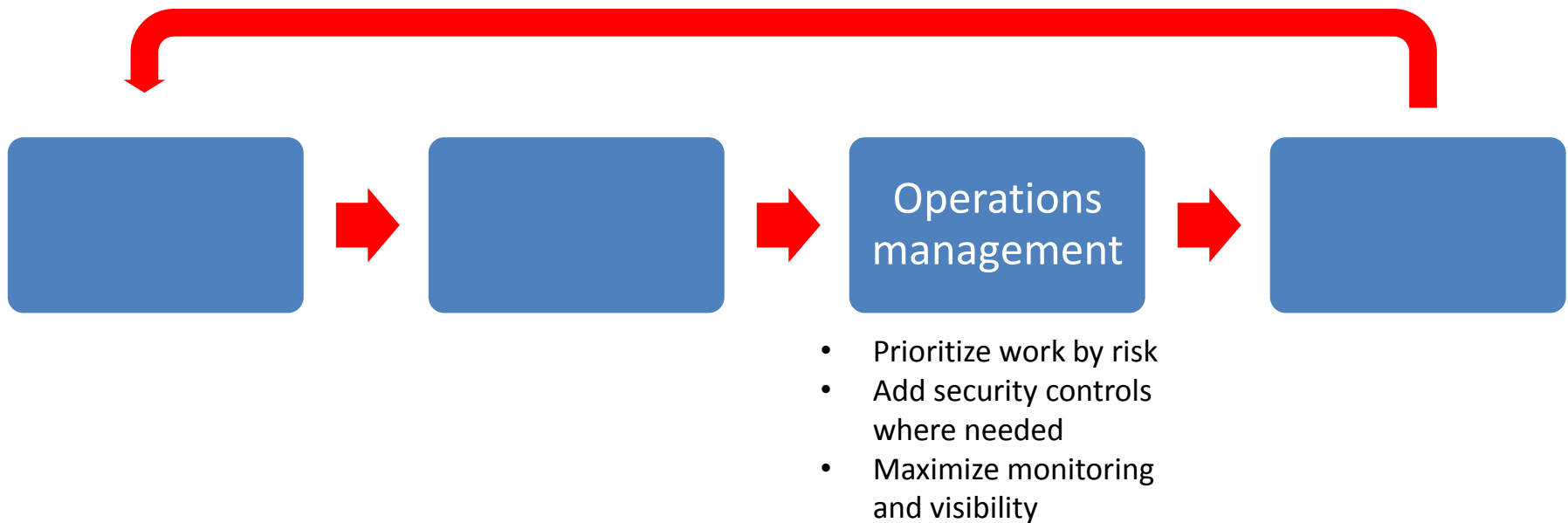
- Define business objectives
- Define business-level risk targets
- Define business-critical assets

... Oriented Risk Management Approach:

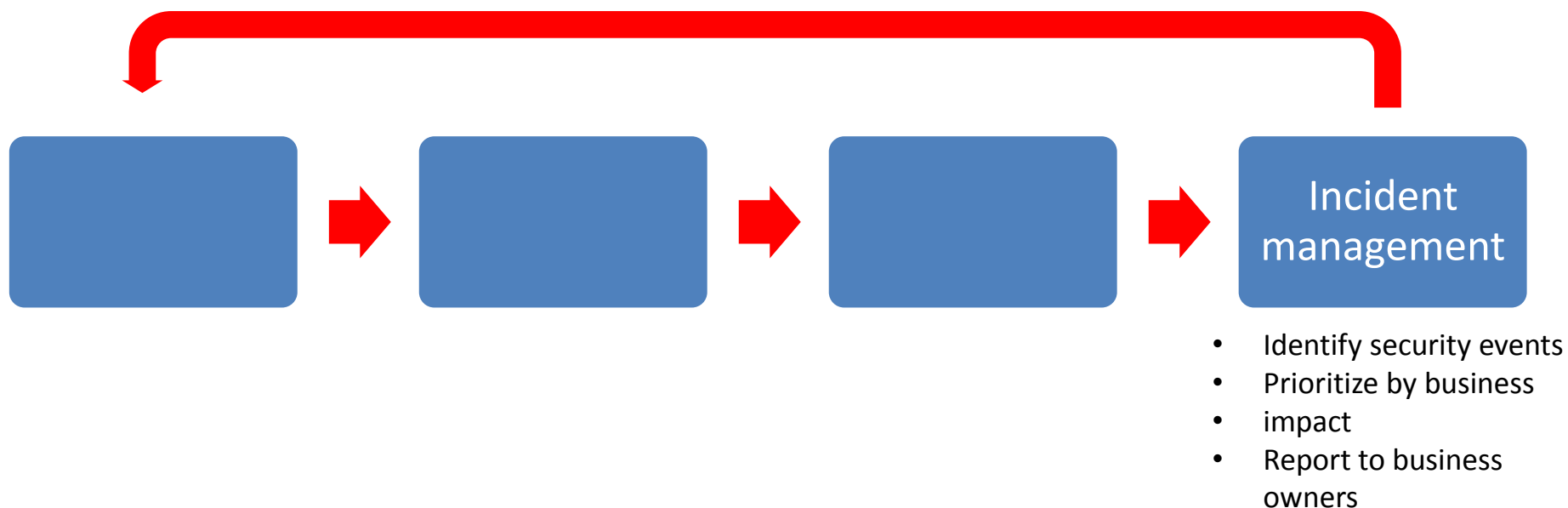


- Understand external and internal threat landscape
- Identify vulnerabilities
- Classify high-value assets

... Oriented Risk Management Approach:



... Oriented Risk Management Approach:



... Oriented Risk Management Approach:



- Define business objectives
- Define business-level risk targets
- Define business-critical assets



- Understand external and internal threat landscape
- Identify vulnerabilities
- Classify high-value assets



- Prioritize work by risk
- Add security controls where needed
- Maximize monitoring and visibility



- Identify security events
- Prioritize by business impact
- Report to business owners

... starts here and know!

There is a process of enlightenment that organizations need to go through to effectively manage risk.

... investments ...

... based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organization's appetite for risk.

... repeatability.

Once enterprise information has been located and a risk assessment was made, the next step is to implement controls — including policies, technologies and tools — to mitigate that risk.

... Risk Framework.

For critical data, a global risk framework should provide an holistic view of risk across lines of business and operations.

Are enterprises ready to embrace risk management as a business accelerator?

Roughly 20 percent of enterprises already 'get it'!

Another 60 percent are ready for that message but are not fully on board ...

and the remaining 20 percent are still back in the mindset that risk management is an inhibitor.

Q & A

Luís Martins

luis.martins@glintt.com