A new framework for CYBERSECURITY GOVERNANCE in large organizations

Dr. George Popescu

- Zero-Day – 15.11.2018 -

Governance

"Ensures that **stakeholder needs**, conditions and options are evaluated to determine balanced, agreed-on **enterprise objectives** to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on **direction and objectives**." *

Examples:

- Commercial effectiveness
- Extensive use of IT capabilities
- Cyber-security initiatives

* COBIT5 - A Business Framework or the Governance and Management of Enterprise IT

Governance vs. Management

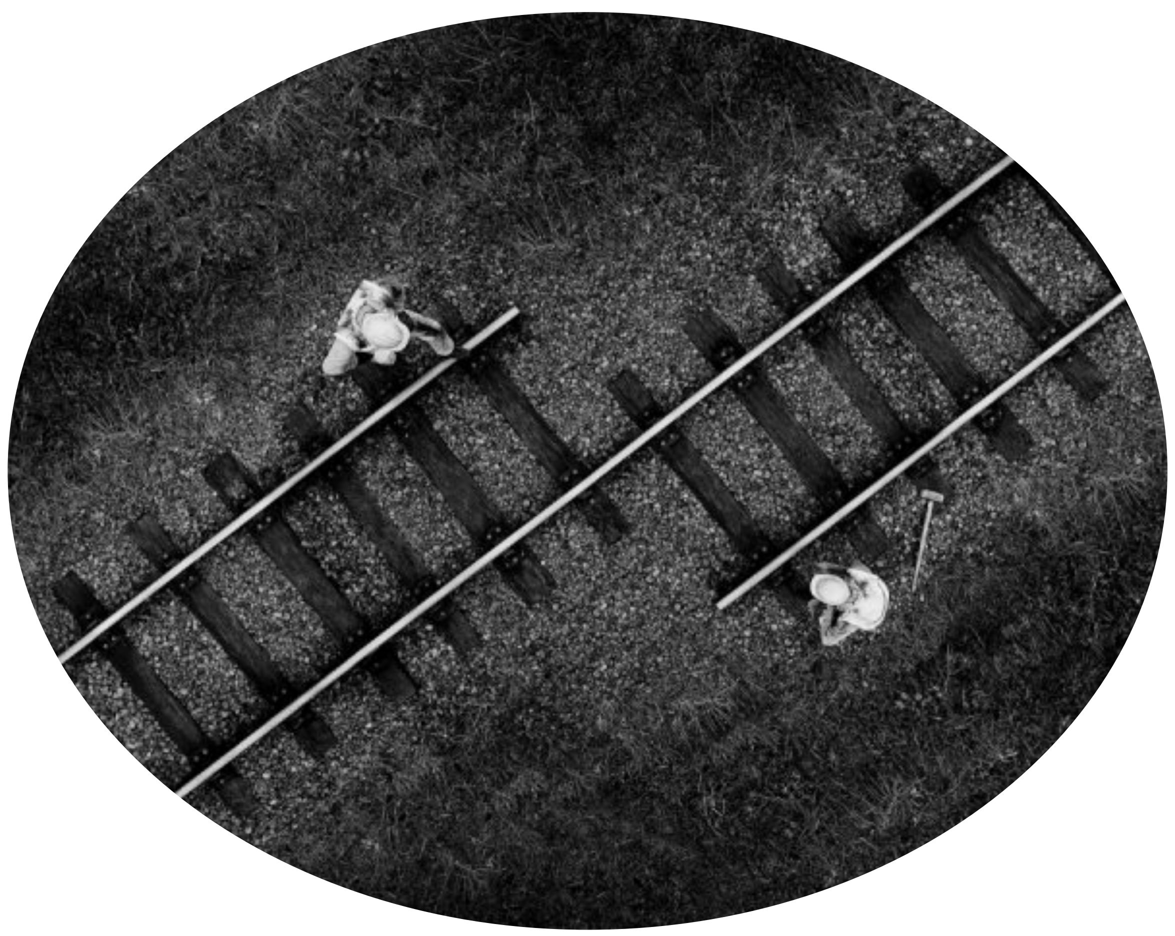
Provide direction

- Evaluate / Direct / Monitor

Execute on the direction

- Plan: Align / Plan / Organize
- Build: Build / Acquire / Implement
- Run: Deliver / Service / Support
- Monitor: Monitor / Evaluate / Assess

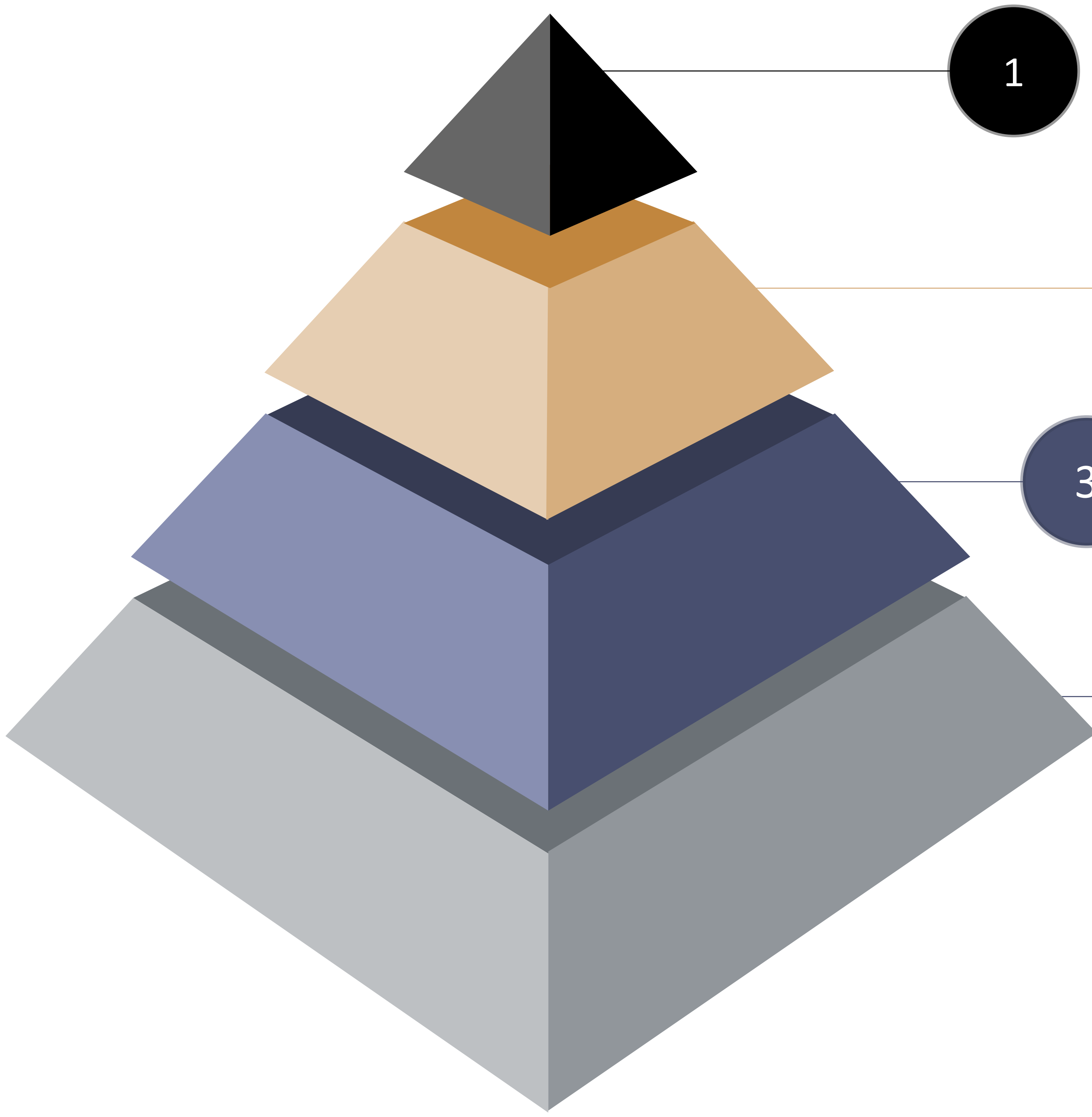
COBIT® 5
AN ISACA® FRAMEWORK



The Challenge

One of the most strategic challenges that organizations worldwide face is the **setup** of a suitable governance framework.

Strategic Alignment



1. Stakeholder needs
   - Business development
2. Governance objective
   - Value creation through risk optimization
3. Business goals
   - Business continuity and availability
4. IT goals
   - Information security

Adapted from: COBIT® 5 AN ISACA® FRAMEWORK

The 4 pillars of a Governance Framework

Governance relies at its core on the alignment between business strategy and IT capabilities

LEADERSHIP

Governance is directed by the board of directors, who set the direction for IT governance.

BIZ ⇔ IT

Business and IT need to be well aligned to commonly meet the organization's overall strategy.

GOALS

Each IT goal must be derived from at least one business goal, e.g., cyber-security initiatives need to link to business development.

AUDIT

Audit provide independent assurance on the effectiveness of controls with regard to IT governance.

Thank you

popescugeorge.com

linkedin.com/in/
popescugeorge