The R in GRC: Managing Risk in Times of Crisis

1st ISACA Conference Athens 2011

Rolf von Roessing
CISA, CISM, CGEIT, CISSP, FBCI

FORFA AG Holding

Global Crisis: IT Under Heavy Fire

ISACA
Serving IT Governance Professionals

- Economic and financial crises spark local / regional recession
- Cost pressure and austerity on the business side, secondary impact on IT
- Renewed interest in outsourcing / outtasking as a defensive move
- Cost cutting round tables with 3rd parties, primarily in IT and other support services
- Removal of external consultants as a typical first move in corporate austerity programmes
- Increased legislative and regulatory activity

FORFA AG Holding

Global Risks in IT: They´re Out There and They Know Where We Live

ISACA
Serving IT Governance Professionals

- Cyber Warfare , Cyber Crime and targeted attacks
- Cloud Computing and systemic issues
- Identity and access management, identity theft
- Social media and related risks

- All of these risks set new challenges for users and IT management – particularly where users are exposed to complexity and direct attack

Global Issues: Game Changers

- Governments cling to the illusion of maintaining control over cyberspace – the last stand of the Old Guard
- New groupings, such as the Pirates, have set a liberalist agenda, seriously challenging the traditional government view on national laws and regulations
- Younger individuals regard free cyberspace as part of human rights
- The timeline has gone beyond Digital Natives: „Generation iPhone“ no longer knows what IT is and what it does

Global Issues: Writing on the Wall

ISACA
Serving IT Governance Professionals

- Shift in user behaviour: complex chains of interaction through social networks and other web services
- Shift in business paradigms: removal of (traditional) fallback solutions, e. g. paper-based
- Increasing number of security incidents and data losses in service supply chains
- Clustering of critical services in major public clouds
- Increasing number of links between widely used service offerings and critical infrastructures (e. g. utilities)

Global Trends: We Can See It Coming

ISACA
Serving IT Governance Professionals

- Bundling of products and services around individual identities create multiple vulnerabilities
- Security, information risk management are still underfunded, but their importance is growing
- Democratisation of social media and related services may require a different mindset
- Protecting individuals, and individual participative rights, is key

How to Prepare: Basics in Times of Crisis

- Legislators, regulators and supranational agencies provide ecosystem controls, linked to more traditional individual rights
- Commonly accepted frameworks and agreed best practice add flexibility to the abstract legal and regulatory context
- New security paradigm and related developments will enable intelligent prevention and defence
- Risk mindset must address individual protection, not just corporate interest

How to Prepare: The R in GRC

- Compliance has been identified as one of the top issues in corporate thinking – but how about individual compliance?
- Governance is catching up with compliance – doing the right things creates new links between the corporate environment and individuals as stakeholders
- **Risk management assists in closing the gap between the expected and the unexpected – and that gap has been growing!**

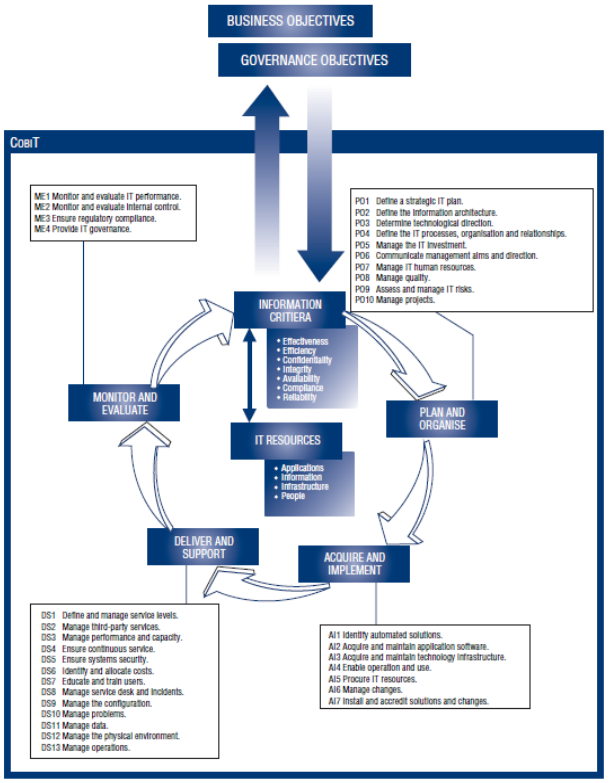
How to Prepare: The R in GRC

- Ideal World vs. Real World: cost cuts, headcount reductions, transferring IT out create breaking points, gaps and weaknesses
- The risk position shifts to the right: more expected (residual) risk, higher likelihood of unexpected risk events
- As business and IT resilience erodes, risk management as 2nd line of defence is becoming more important
- Holistic risk view: in times of crisis, triage is inevitable. **BUT (!!!) low budgets and pressure are not an excuse for leaving your flanks open.**

How to Prepare: Tools of the Trade

- Controls, processes and full integration of security with GRC: COBIT 5
- Risk in the underlying information systems and infrastructures: Risk IT
- Sanity check, and strategic alignment: Val IT
- Holistic security, including wider societal systems and relationships with business: BMIS (now including the new publication on culture)
- Drill-down: further publications on aspects of risk and security

From COBIT 4.1...



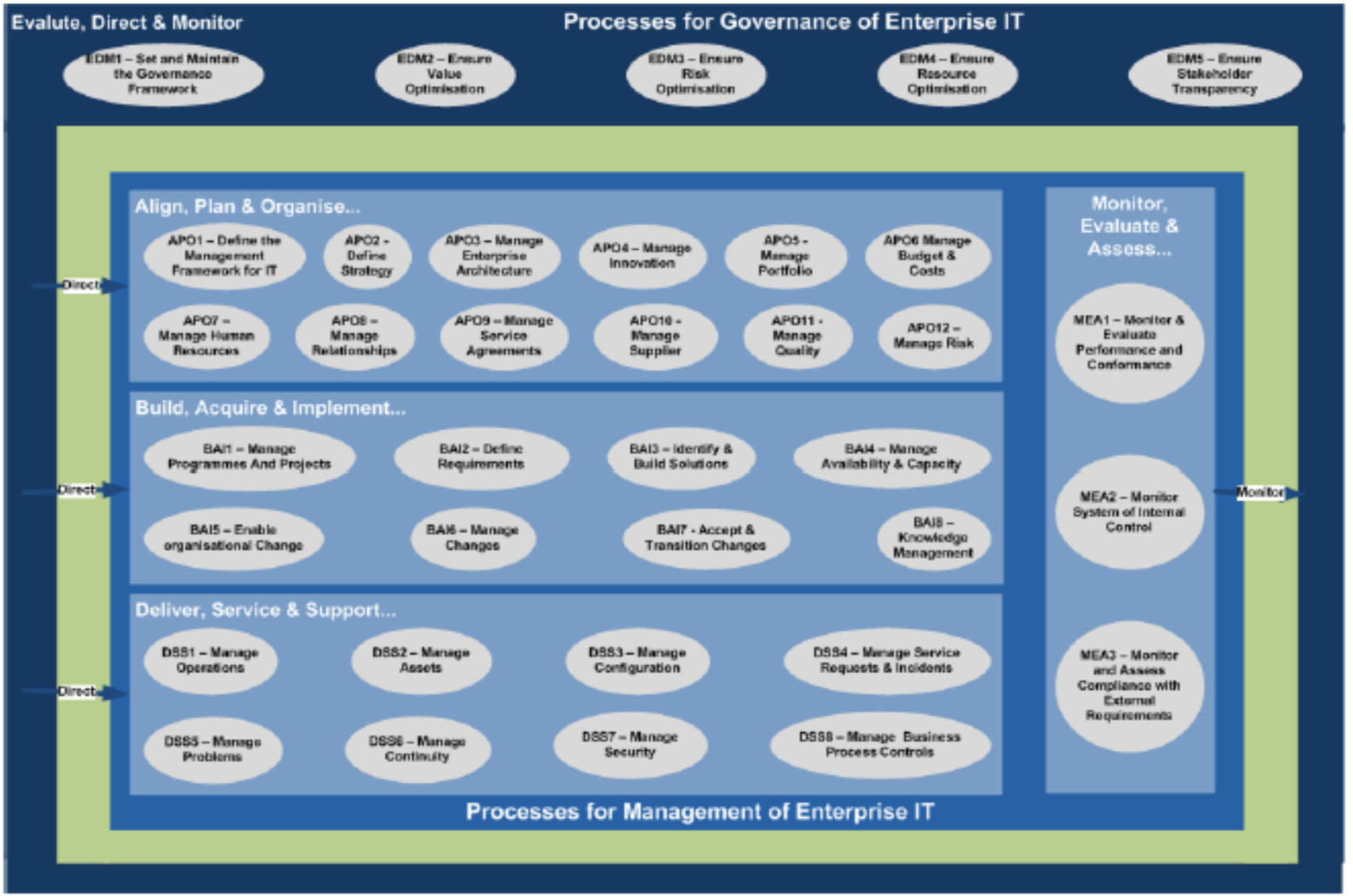
MAPPINGS

- COSO ERM
- Basel II
- NIST Pubs
- ISO 27000
- etc.

FORFA AG Holding

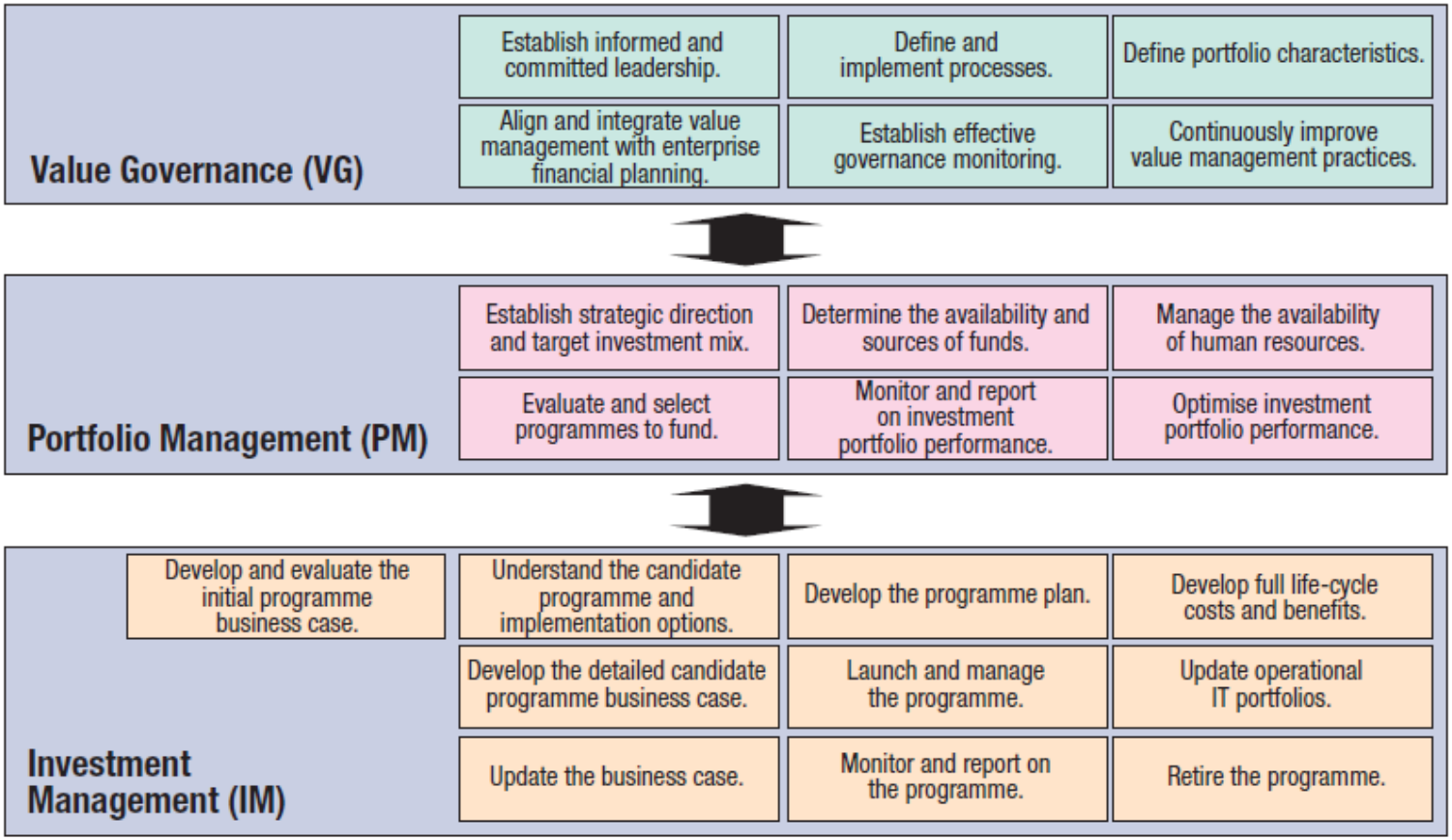
… to COBIT 5

ISACA
Serving IT Governance Professionals

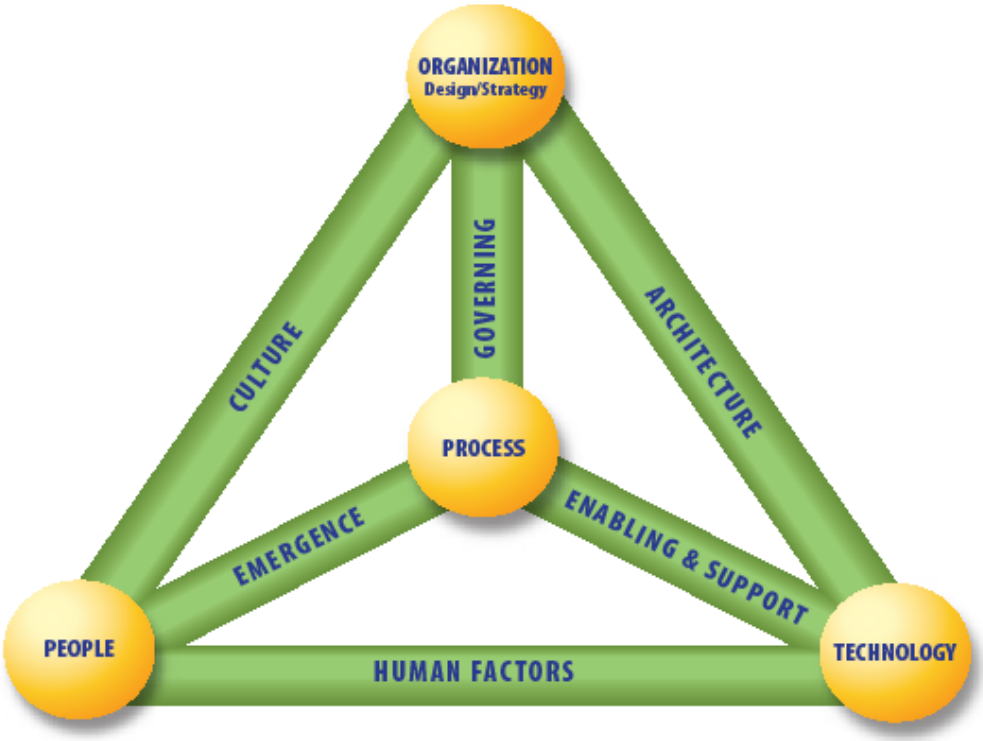


Managing Risk Hands-on: RiskIT

Making Business Sense in Times of Crisis: ValIT



Advancing Security: BMIS



BMIS will be complemented by the forthcoming COBIT for Security publication

The R in GRC: Weak and Strong Signals in Times of Crisis

- Bounded Rationality: if there are „things better not said“, the 2nd and 3rd lines of defence must speak up and provide an impartial risk assessment.
- Storming, crunching, do more with less: the more often the organisation has „barely made it“, the stronger the signals. Beware the crisis-prone organisation!
- Escalating commitment: where doing more of the same does not achieve the goal, people need re-orientation.
- Overcontrol: more policies, procedures and controls may not be the answer
- Cutting Corners: where people don´t like the written rules, they will make their own

Thank you very much indeed for your kind attention.
Your questions and comments are highly appreciated.

FORFA AG Holding

GRC, Audit, Quality Assurance

controllit
Business Continuity Management

Business Continuity, BCM Academy, ICT Continuity

JANUS Consulting GmbH
Erhalt und Entwicklung des unternehmerischen Erfolges

Security, Investigation, Forensics

Rolf can be reached at +49-172-6712322, rvr@scmltd.com, skype: rvrscm and through the Forfa Alliance companies.

ISACA®
Serving IT Governance Professionals