

## References for Marek Pióro

Hereby I wish to warrant, that Mr Marek Pióro worked for Polkomtel from 1998 to the end of 2006 year. Recently Marek worked as IT Audit main Auditor. In 2000 year he provided process information security policy preparation. In the period from 2001 to the end of 2006 years Marek was attended in all IT and telecommunication area audits. This time he was responsible eg for risk identification, management and for elaborating strategy prevention risks, but first he was attending in building IT Governance framework closely collaborating with CIO and with Polkomtel's Board members responsible for operational Issue. Marek also was member of IT – business Committee.

According to my Attestations dated 2008-10-25, as verifier in Marek Pióro Application for CGEIT Certification, I warrant, that Mr Marek Pióro performed task in

### 1. IT Governance Framework

- Define the requirements and objectives for, and drives the establishment of, IT Governance in an enterprise, considering Value, philosophy, management style, IT awareness, organization and policy,
- Define the requirements and objectives for, and drive the establishment of, IT governance in an enterprise, considering values, philosophy, management style, IT, awareness, organization, standards and policies.
- Ensure that an IT governance framework exists and is based on a comprehensive and repeatable IT process and control model that is aligned with the enterprise governance framework
- Establish appropriate management governance structures, such as an enterprise investment committee, IT strategy committee, IT steering committee, technology council, IT architecture review board, business needs committee and IT audit committee.
- Confirm that the IT governance framework ensures compliance with applicable external requirements and ethical statements that are aligned with, and confirm delivery of, the enterprise's goals, strategies and objectives.
- Obtain independent assurance that IT conforms with relevant external requirements; contractual terms; organizational policies, plans and procedures; generally accepted practices; and the effective and efficient practice of IT.
- Apply IT best practices to enable the business to achieve optimal value from implementation of IT services and IT-enabled business solutions.
- Ensure the establishment of a framework for IT governance monitoring (considering cost/benefits analyses of controls, return on investment for continuous monitoring, etc.), an approach to track all IT governance issues and remedial actions to closure, and a lessons-learned process.
- Ensure that appropriate roles, responsibilities and accountabilities are established and enforced for information requirements, data and system ownership, IT processes, and benefits and value realization.

## 2. Strategic Alignment:

- Identify and take action on barriers to strategic alignment..
- Ensure that effective communication and engagement exists between business and IT management regarding shared strategic initiatives and performance.
- Ensure business and IT goals cascade down through the enterprise into clear roles, responsibilities and actions
- Identify and monitor the interdependencies of strategic initiatives and their impact on value delivery and risk.
- Monitor, evaluate and report on the effectiveness of the alignment of IT and enterprise strategic initiatives.
- Monitor and assess current and future technologies and provide advice on the costs, risks and opportunities that they bring.

## 3. Value Delivery

- Recognize that different categories of investments need to be evaluated and managed differently.
- Ensure that all IT solutions are developed and maintained effectively and efficiently through the development life cycle to deliver the required capabilities.
- Ensure that all IT services are delivered to the business with the right service levels.
- Ensure that IT investments, solutions and services are aligned with the enterprise strategies and architecture.

## 4. Risk Management:

- Ensure that IT risk identification, assessment, mitigation, management, communication and monitoring strategies are integrated into business strategic and tactical planning processes.
- Define risk management strategies, and prioritize responses to identified risks to maintain risk levels within the appetite of the enterprise.
- Ensure that risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels.
- Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate).

## 5. Resource Management:

- Ensure that the requirements for trained resources with the requisite skill sets are understood and are assessed appropriately.
- Ensure the existence of appropriate policies for the training and development of all staff to help meet enterprise requirements and personal/professional growth.
- Undertake gap analyses to determine shortfalls against requirements to ensure that the business and IT resources (people, application, information, infrastructure) are able to meet strategic objectives.
- Ensure that people, hardware, software and infrastructure procurement policies exist to effectively and efficiently fulfill resource requirements.
- Ensure that IT assets are managed and protected through their economic life cycle and are aligned with current and long-term business operations requirements to support cost-effective achievement of business objectives.



6. Performance Measurement;

- Evaluate IT process performance, track IT investment portfolio performance, and measure IT service delivery through the use of outcome measures and performance drivers.
- Use maturity models and other assessment techniques to evaluate and report on the health of the enterprise's performance level.

Marek is a very competent professional in IT Governance and Telcommunication area. But first of all he is very effective in all area connected with risk management (also as an internal auditor). He fully understands principles of process based organization, governance rules, standards and best practices. He helped a lot building new IT governance model and making internal processes more effective and safe. Over the time of our collaboration he has constantly worked on improving his professional and personal skills.

Wojciech Dylewski

  
Management Board Member

Operations Director