

Governance Standards and Control Frameworks

Dr. Shahzada Khurram

Governance Standards and Control Frameworks

- **PCI-DSS** - Payment Card Industry Data Security Standard (While a standard it is required: more on this one later).
- **OCTAVE®** - Operationally Critical Threat, Asset, and Vulnerability Evaluation.
 - **Self-Directed** Risk Management.
- **COBIT** - Control Objectives for Information and related Technology.
 - **Goals** for IT – Stakeholder needs are mapped down to IT related goals.
- **COSO** – Committee Of Sponsoring Organizations.
 - **Goals** for the entire organization.
- **ITIL** - Information Technology Infrastructure Library.
 - IT Service Management (**ITSM**).
- **FRAP** - Facilitated Risk Analysis Process.
 - Analyses one business unit, application or system at a time in a roundtable brainstorm with **internal** employees. Impact analyzed, threats and risks prioritized.

ISO 27000 series

- **ISO 27001:** Establish, implement, control and improvement of the ISMS. Uses PDCA (Plan, Do, Check, Act)
- **ISO 27002:** (From BS 7799, 1/2, ISO 17799) Provides practical advice on how to implement security controls. It has 10 domains it uses for **ISMS** (Information Security Management Systems).
- **ISO 27004:** Provides metrics for measuring the success of your ISMS.
- **ISO 27005:** Standards based approach to risk management.
- **ISO 27799:** Directives on how to protect PHI (Protected Health Information).



Thank you