

# ITコントロール



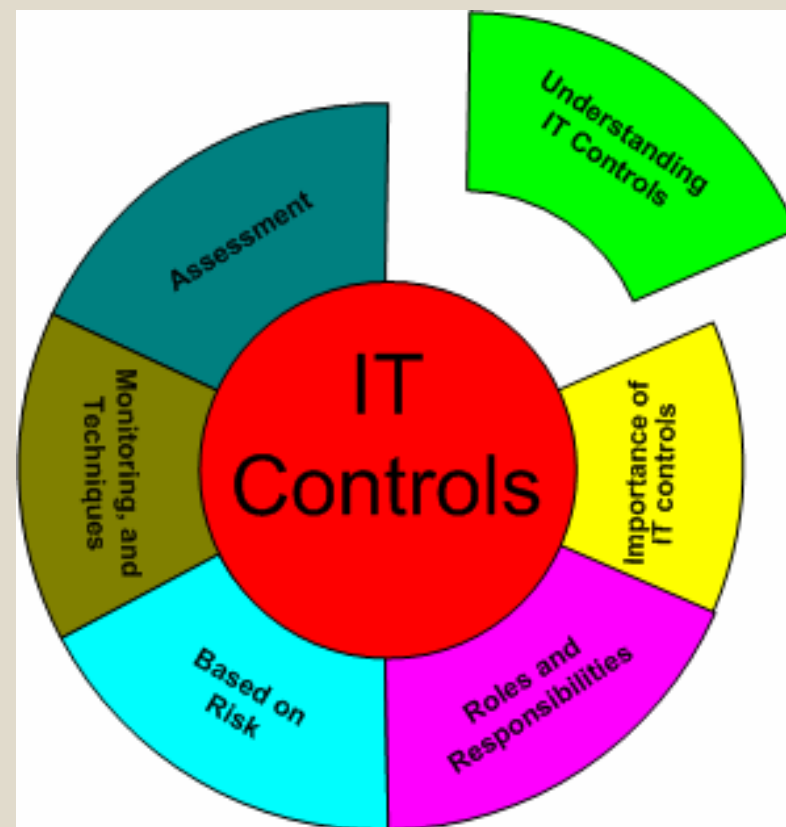
## GTAG1 ( IT監査の国際的ガイダンス 1 )

# 本ガイドの内容

- ITコントロールの理解
- ITコントロールの重要性
- ITコントロールを確実にする組織内の役割  
および責任
- リスクの分析
- モニタリングおよび技法
- ITコントロールの評価

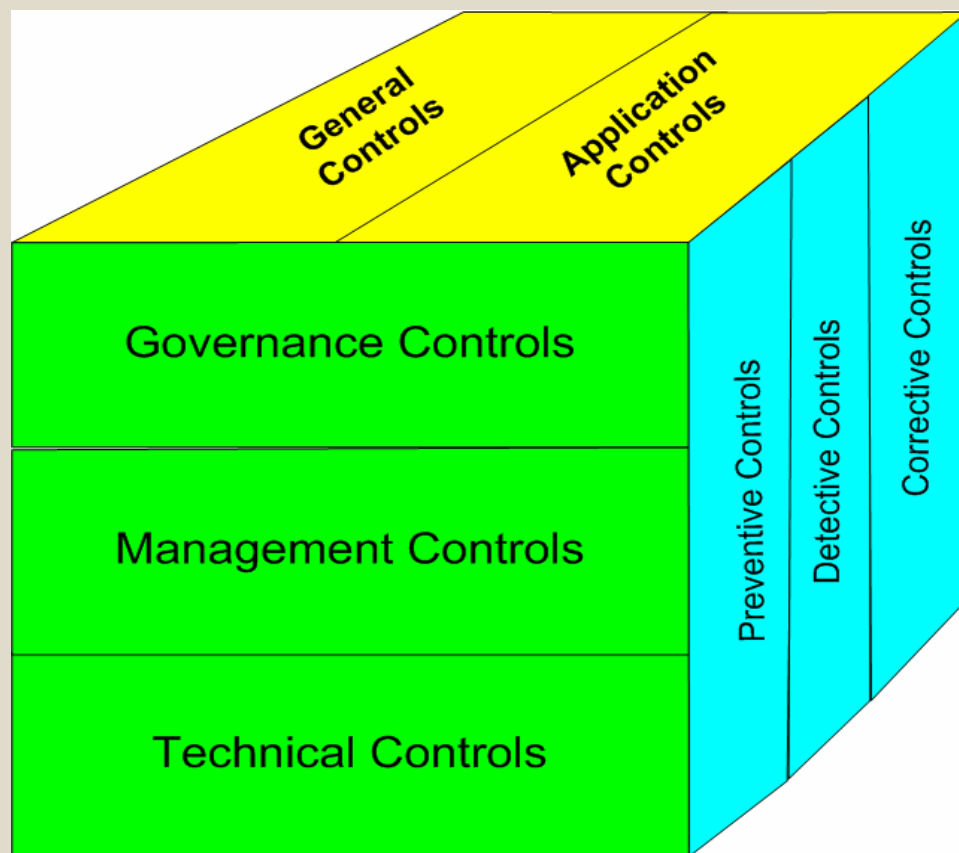
# ITコントロールの理解

- ITコントロールは、情報および情報サービスへアシュアランスをもたらし、テクノロジーの利用にともなうリスクの低減に寄与するプロセスである
- ふたつの構成要素
  - 業務コントロールの自動化
  - ITのコントロール

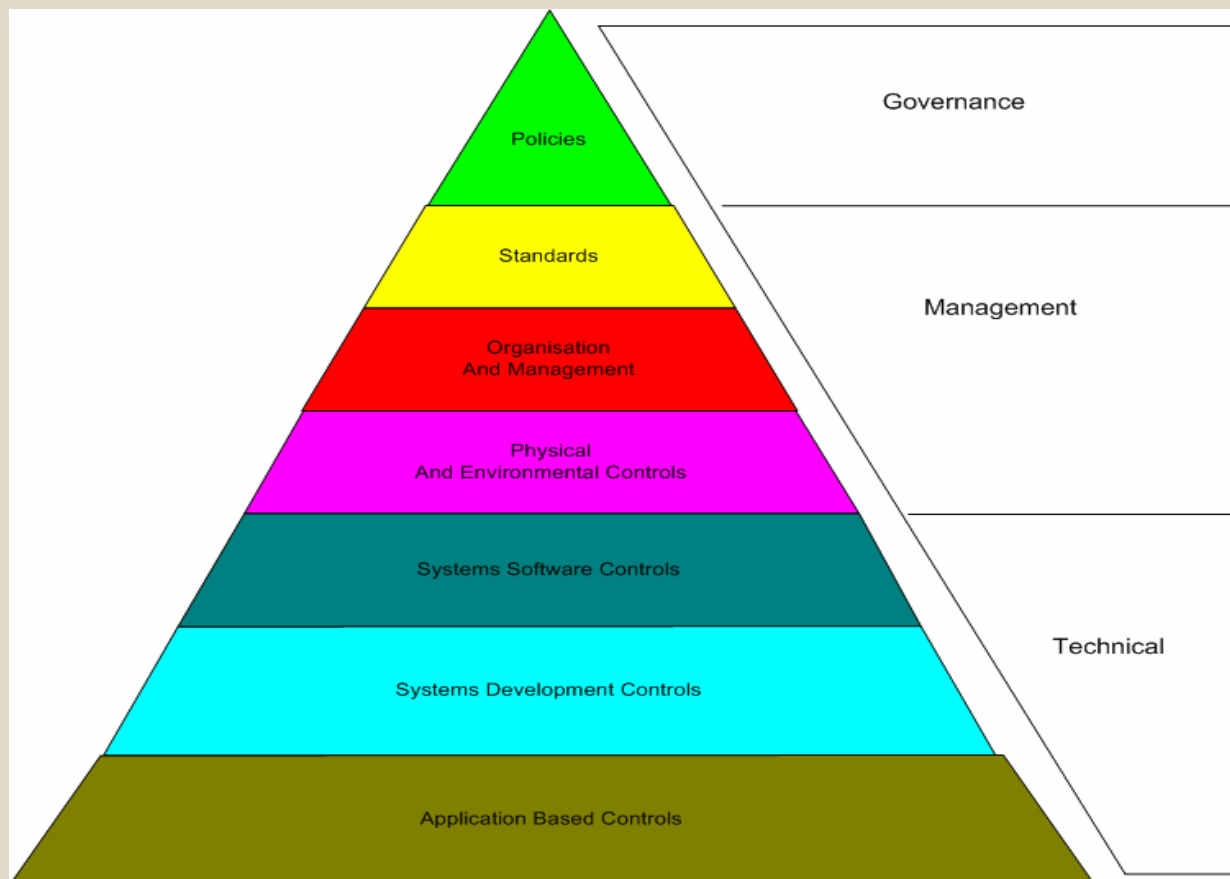


# コントロールの理解

- 種類
  - 全般コントロール(全般統制)
  - アプリケーションコントロール(業務処理統制)
- 種類
  - 防止的
  - 発見的
  - 是正的
- 種類
  - ガバナンスコントロール
  - マネジメントコントロール
  - テクニカルコントロール



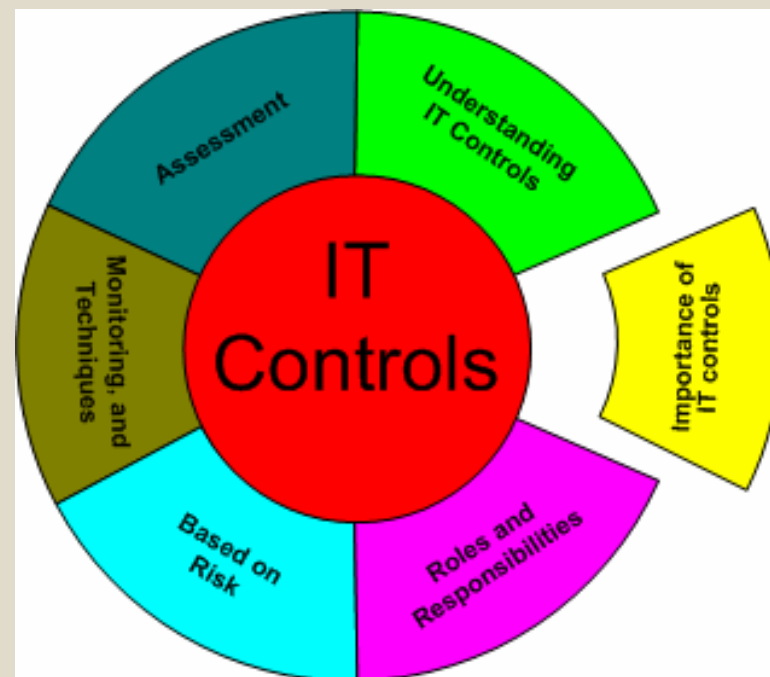
# ITコントロールの理解



- 実施するコントロールの検討と重点分野の決定時にトップダウンアプローチを使用

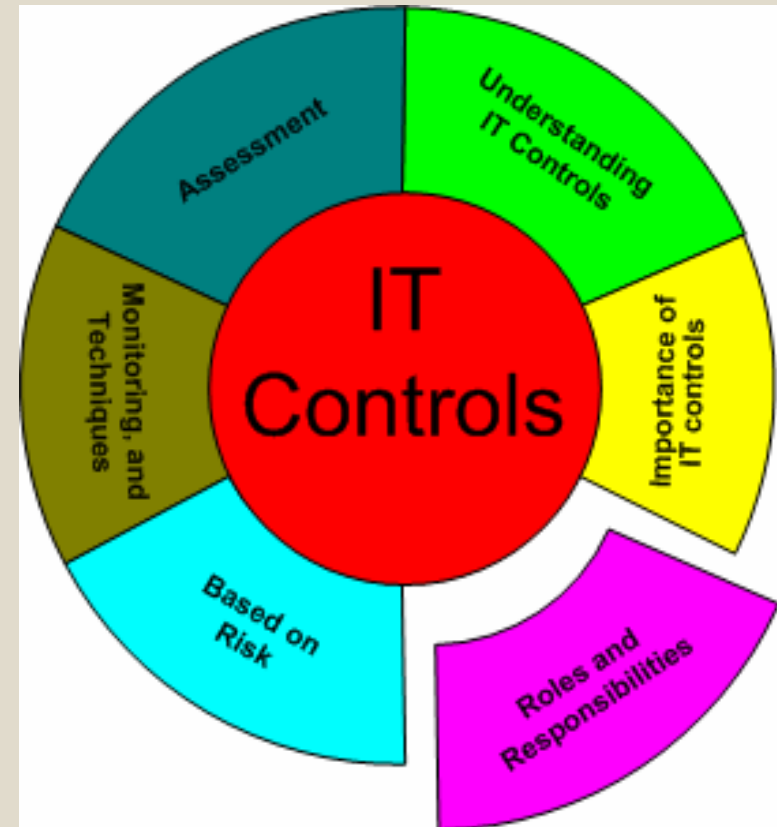
# ITコントロールの重要性

- 次のようなITコントロールが必要
  - コストコントロール
  - 競争力の維持
  - 情報資産の保護
  - 法律・規制への準拠
- 効果的なITコントロールの実施は  
アシュアランス証拠の効率性、信頼性、柔軟性、可用性を促進



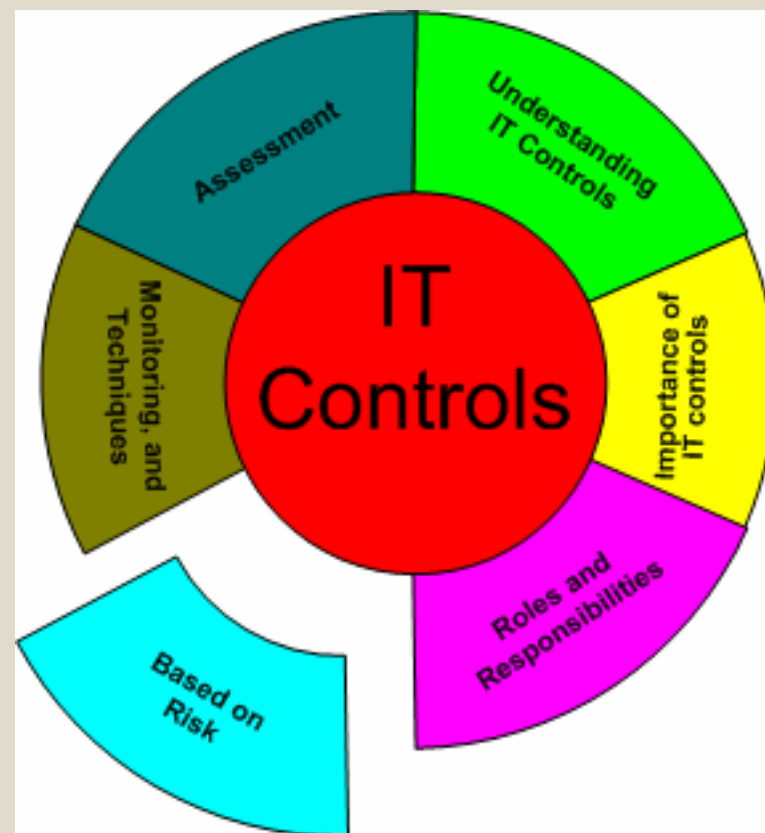
# 役割と責任

- 取締役会／理事会
- マネージメント
  - ITコントロールの定義、承認および実行、もしくはITコントロールの利用への理解
- 監査人
  - 内部監査人- アシュアランス
  - 外部監査人- 定期的監査



# リスクベース

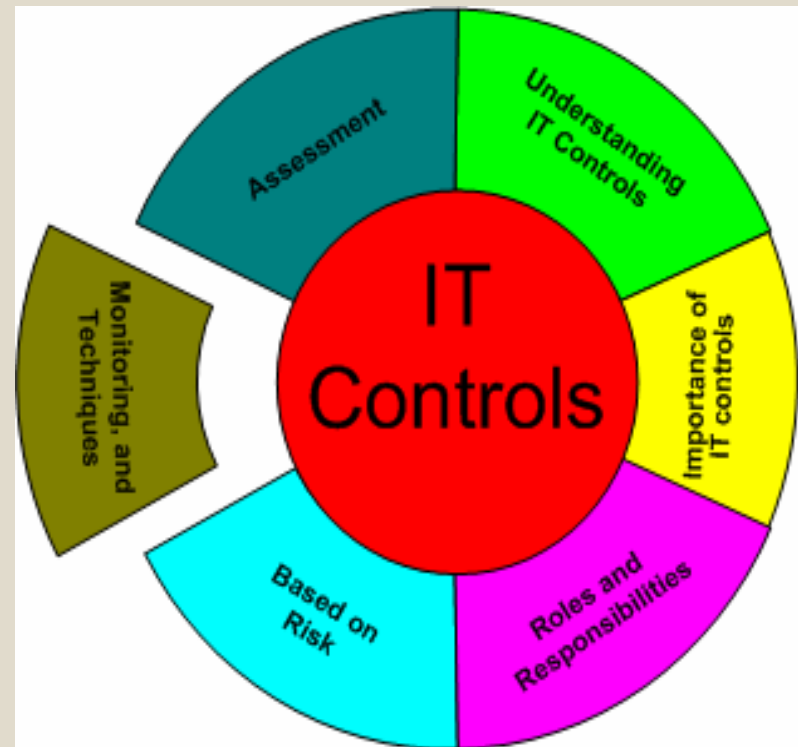
- リスクの分析
  - リスクの識別
  - ITコントロールの適切性判断に際し、リスクを考慮
  - リスク低減戦略の決定 – 受容/除去/共有/統制/低減
  - ITコントロールのベースラインを検討





# モニタリングと技法

- モニタリング & ITコントロールの評価
  - コントロールフレームワークの選択
  - 適切な監査メソッドロジの利用
  - 継続的モニタリング/特別なレビュー/自動化された継続的監査



# 評価

- ITコントロールの評価は、継続的なプロセスである。なぜならビジネスプロセスは絶え間なく変化するから。
- テクノロジーは進化し続ける
- 新たな脆弱性の出現にともない脅威も拡大
- 監査方法は改善し続ける

