SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Nejčastější chyby IT governance v praxi

Petr Hujňák
Per Partes Consulting

Agenda

- CHAOS ŘÍZENÍ:
  Co je to IT governance a na co se při governance soustředit?
- CHAOS AKTIV:
  Jak zajistit integritu aktiv a vyhnout se izolovanému řízení aktiv vzniklému z různých zájmových pohledů na systém?
- CHAOS HODNOT:
  O jaké hodnoty se usiluje a jak je konkretizovat až na aktiva?
- CHAOS STANDARDŮ:
  Které standardy aplikovat?

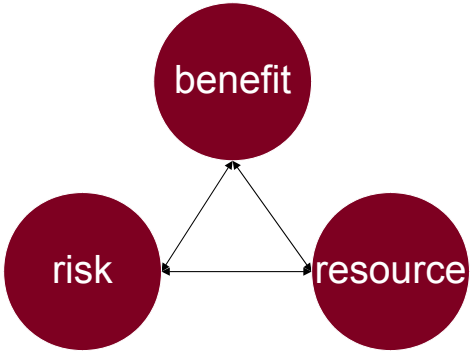
CHAOS ŘÍZENÍ: Na co se vlastně zaměřit při IT Gov?

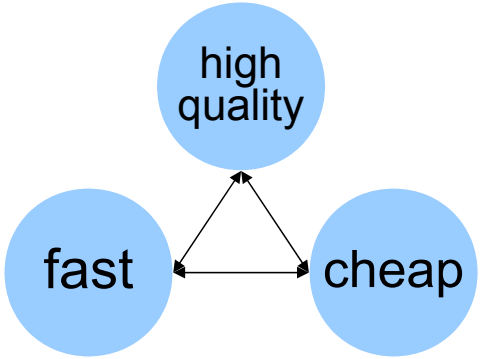
PER PARTES® ATTACKING COMPLEXITY

- IT Governance = vrcholové směrování IT (doslova panování v IT oblasti)

Podle ISACA, která pojem prosadila, do IT governance zahrnuje 3 oblasti:

Ve skutečnosti jde při IT Governance o balancování ve známém trojimperativu

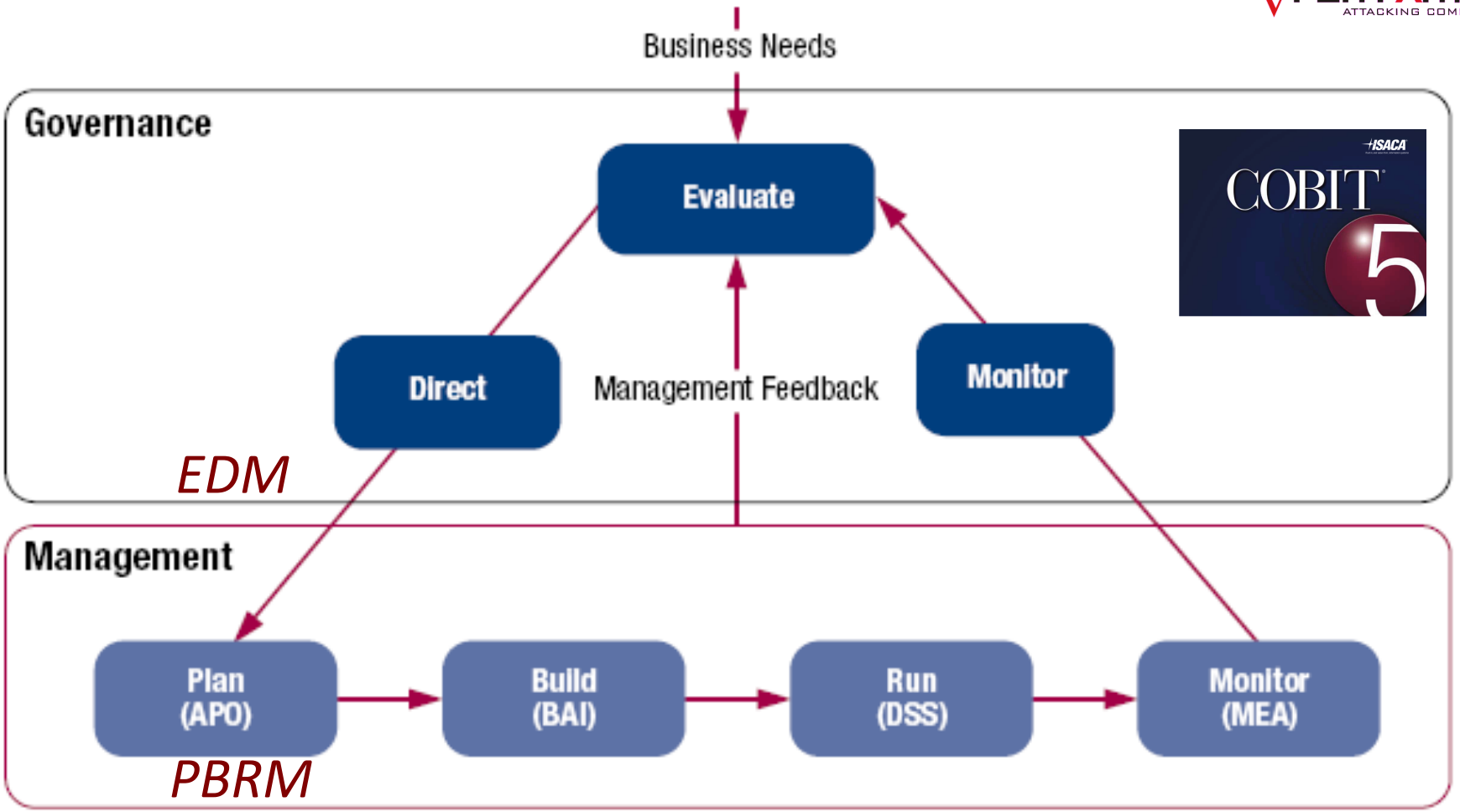




Účelem a přínosem správného vrcholového řízení (IT Governance) je vytváření jasných a udržitelných podmínek pro výkonný management (IT Management). Jde o známou vazbu „dělat správné věci“ a „dělat věci správně“.

CHAOS ŘÍZENÍ: Kdo odpovídá za IT Governance?

PER PARTES ATTACKING COMPLEXITY



ISACA v COBITu 5 (2012) začala striktně odlišovat pravomoc, odpovědnost a procesy pro IT Governance od pravomoci, odpovědnosti a procesů pro IT Management. Praxe totiž - proti předpokladům v COBITu 4 - ukázala, že koncepce „vše v jednom“ nepřináší výsledky.

CHAOS ŘÍZENÍ: Jak na IT Governance?

PER PARTES® ATTACKING COMPLEXITY

CHAOS VRCHOLOVÉHO ŘÍZENÍ V PRAXI
„KDO NEVÍ, KAM MÍŘÍ, TĚŽKO SE STREFÍ“

Doporučené standardy

COBIT 5 AN ISACA® FRAMEWORK

COBIT 5:
The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
01 Ensure governance framework setting and maintenance.
02 Ensure benefits delivery.
03 Ensure risk optimisation.
04 Ensure resource optimisation.
05 Ensure stakeholder transparency.

Je-li v organizaci prováděno vrcholové řízení, tak je také známo, kdo za něj nese odpovědnost, jakou má pravomoc a co (jaké procesy a činnosti) vykonává.

Pro zájemce doporučuji prezentaci Nové metodické myšlení, ke stažení je na www.perpartes.cz (volně v sekci publikace/prezentace a články)

Nové metodické myšlení

Petr Hujňák
CGEIT, CRISC, CSPM
petr.hujnak@perpartes.cz

president ISACA Czech Rep.
ISACA Czech Republic Chapter
CEO Per Partes Consulting
PER PARTES® ATTACKING COMPLEXITY

CHAOS AKTIV: Integrita aktiv v architektuře systému

PER PARTES® ATTACKING COMPLEXITY

- Architekturou rozumíme fundamentální organizaci systému ztělesněnou prvky systému, jejich vzájemnými vazbami vč. vazeb na okolí a principy vedoucími k návrhu a postupnému rozvoji systému.
  [ISO/IEC 42010] [TOGAF]

ISO International Organization for Standardization

TOGAF™ 9

… vedoucími **INTEGRITU** návrhu a postupného rozvoje systému. [Hujňák]

Integritou rozumíme konzistenci *(nerozpornost)* a kompatibilitu *(schopnost fungovat dohromady)* očekávání, hodnot, zásad, principů, měřítek, metod, procesů / činností, technologií, produktů, řešení a aktiv.

- Architekturou rozumíme množinu vytčených zásad a principů užívaných k dosažení integrity dílčích návrhů / řešení přes více vzájemně souvisejících oblastí zájmu vyjádřených v **architektonických pohledech cíli a požadavky na aktiva**. Architektura ovlivňuje individuální řešení vyžadováním společných zásad a principů, poukazováním na vazby k jiným systémům a požadováním zavedení těchto principů a vazeb. [Hujňák]

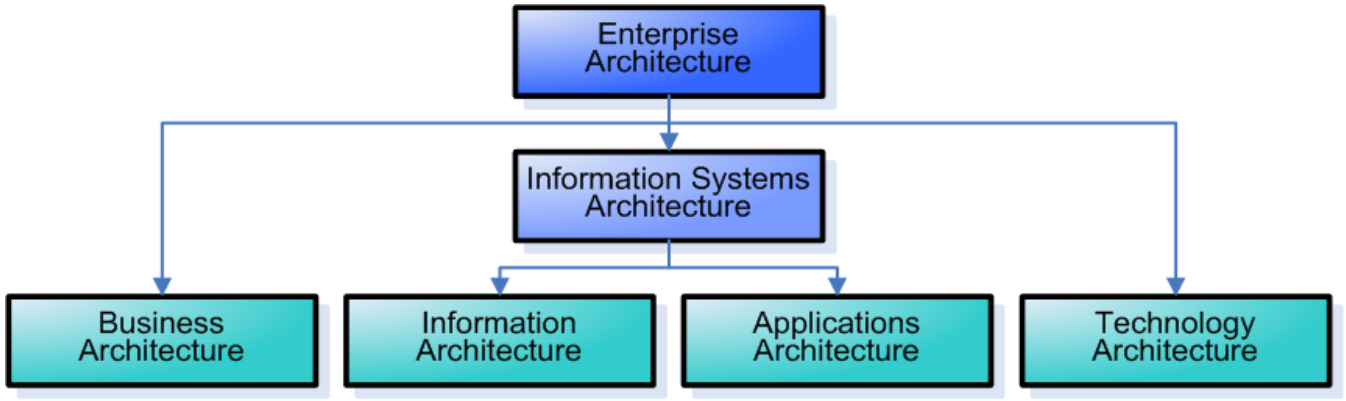
Hlavním motivem architektonického managementu je uřízení **integrity** komplexního systému a architektura systému má tak integritní účinek na řešení všech začleněných oblastí zájmu.

CHAOS AKTIV: Aktiva v pohledech (views) na systém

PER PARTES® ATTACKING COMPLEXITY

Architektonickým **pohledem** (architectural view) rozumíme reprezentaci systému z perspektivy identifikované množiny architektonických zájmů. Obsah architektonického pohledu je znázorněn v architektonickém modelu. [ISO/IEC 4210]

- Zainteresované strany určují zájmy pozorovatelů systému dané zpravidla jejich odpovědnostmi. Typické zájmy zahrnují funkcionalitu, integrovanost, modifikovatelnost, výkonnost, bezpečnost a spolehlivost nebo třeba také náklady, termíny či kvalitu systému.



TOGAF anticipuje zájmy pozorovatelů systému a doporučuje vycházet ze 4 základních pohledů vytvářejících 4 dílčí architektury systému.

Znáte své zainteresované strany a jejich sílu vlivu? Jaké pohledy na systém jsou ve vaší organizaci vytvářeny? Dochází u vás ke konfliktu zájmů zainteresovaných stran? Jsou tyto pohledy provázány přes společná aktiva systému?

CHAOS AKTIV: Integrita aktiv v architektuře systému

Aktivem nazývá norma ISO 27001 cokoliv, co má pro organizaci nějakou hodnotu. Aktiva mohou mít hmotnou i nehmotnou povahu (schopnost vykonávat službu či znalost) a je potřeba je řídit. Podle COBITu jsou aktiva (asset) předmětem „IT governance“ (doslova v překladu a významu „panování“), právě proto, že mají pro organizaci hodnotu.

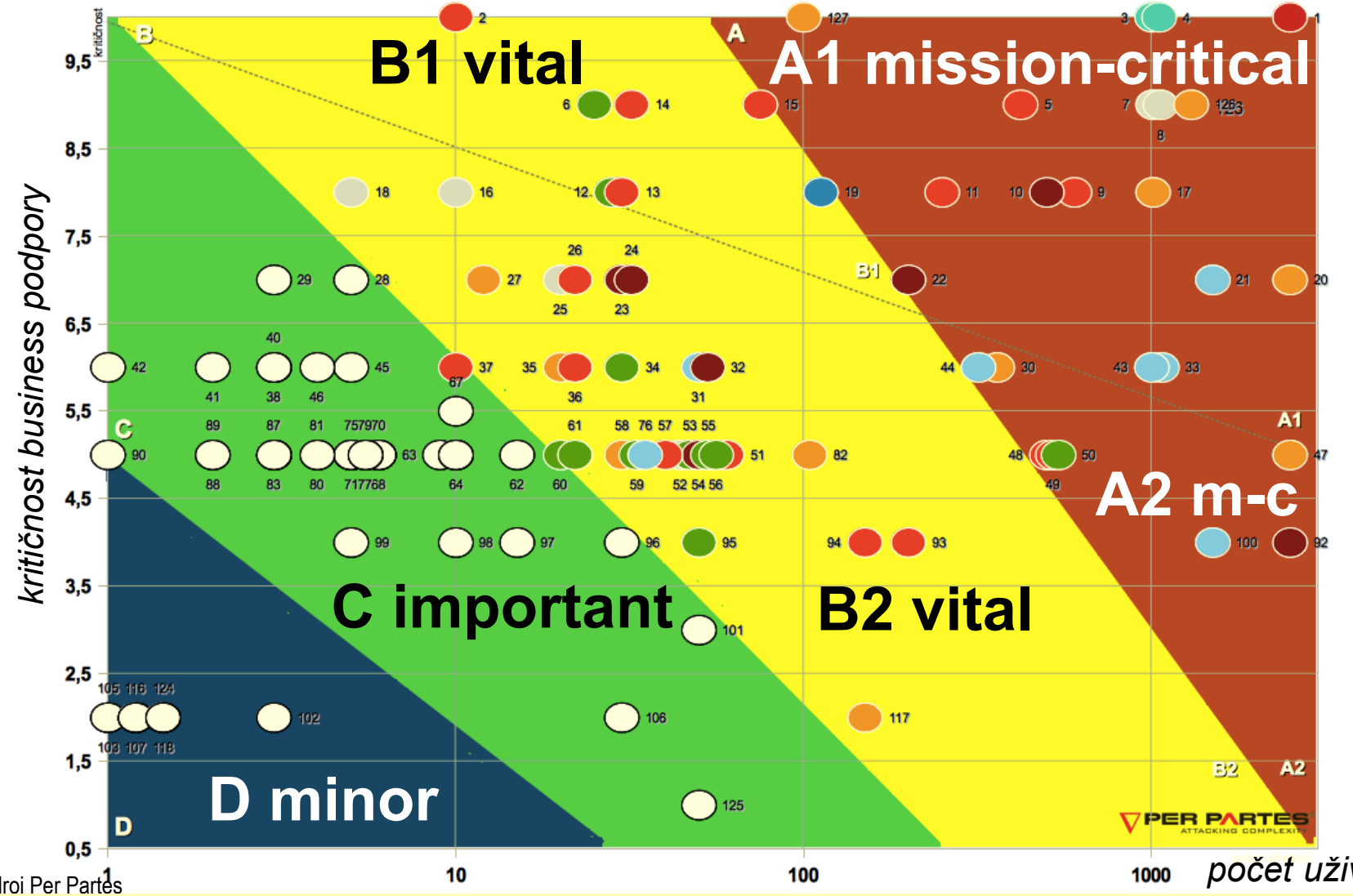
- Má-li aktivum pro organizaci hodnotu, je předmětem zájmu zainteresovaných stran a je pro systém zobrazeno v pohledech.
- Architektonickým aktivem nazvěme ty komponenty architektury systému, které jsou zobrazeny v architektonických pohledech a současně mají význam (jsou relevantní) pro architektonický management. [Hujňák]

Ne všechny komponenty pohledů však musí mít architektonický význam a proto nemá cenu komponenty, které nepřispívající a neovlivňují architekturu systému, dále dekomponovat a zkoumat. Proto architektura může obsahovat nevyrovnanou dekompozici z hlediska granularity rozpadu.

Tam, kde by mohlo dojít k nejasnostem či variantám ovlivňujícím celkovou architekturu systému, je potřeba zvětšit podrobnost dekompozice a na detailní úrovni popsat a řídit právě ty komponenty, které mají architektonický význam.

CHAOS AKTIV: Prioritizace aktiv

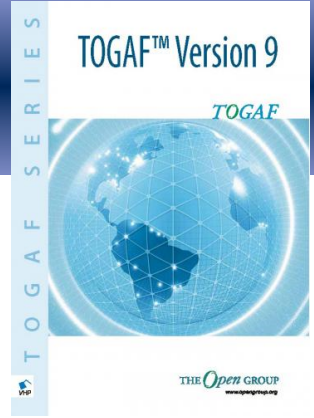
Příklad zařazení cca 130 aplikací v dané organizaci do zón podle jejich významnosti



zdroi Per Partes

Prioritní aplikace jsou v centru pozornosti IT Gov a tvoří jádro apl. architektury.

CHAOS AKTIV: architektonické principy



Business Principles	9
Data Principles	6
Application Principles	2
Technology Principles	4
	21

Data Principle 10: Data is an Asset

Statement: *Data is an asset that has value to the enterprise and is managed accordingly.*

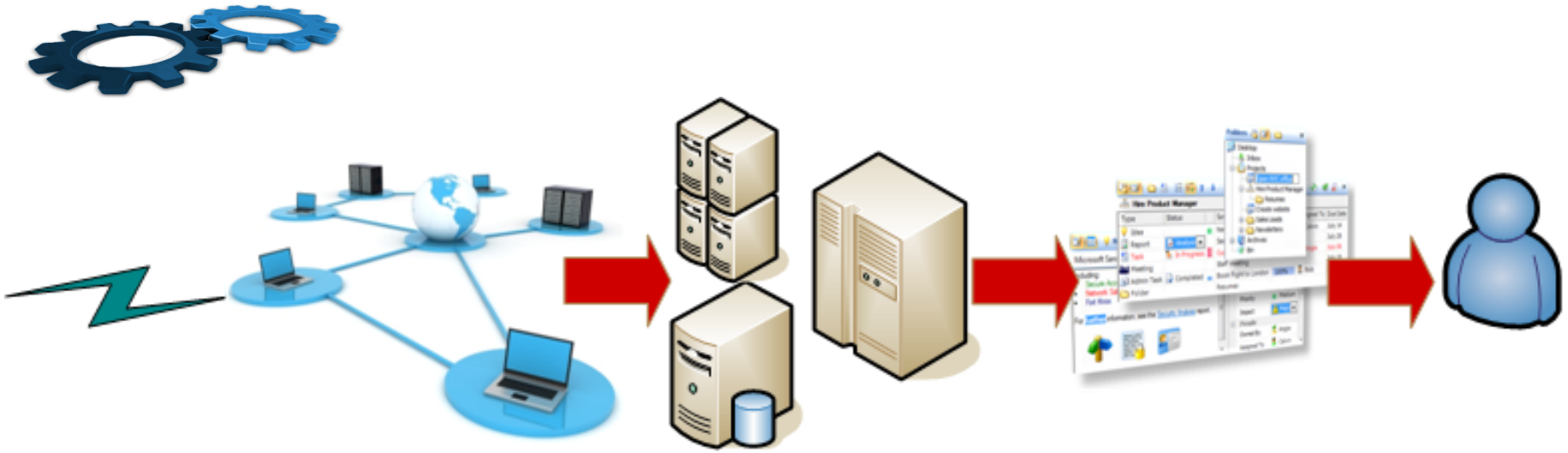
Rationale: *Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decisionmaking, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.*

Implications:
This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. ...
Data quality will need to be measured and steps taken to improve data quality — it is probable that policy and procedures will need to be developed for this as well. …
A security policy, governing human and IT actors, will be required that can substantially improve protection of IP. ...

Pohled na data (informace) jako aktivum zavádí TOGAF jako jeden ze základních principů a je tak ve shodě s filozofií norem ISO řady 27000.

CHAOS AKTIV: řetězení aktiv / superaktiva

PER PARTES® ATTACKING COMPLEXITY



„Superaktivum“ zahrnuje všechny prvky na end-to-end cestě od ICT infrastruktury až k uživateli. [Hujňák]

Řetězení aktiv do superaktiv. Cesta od infrastruktury je protažena přes aplikace a data až na aplikační služby a jejich SLA parametry pomocí architektonických superaktiv. SLA parametry služeb nejsou přáním ICT útvaru, ale „business“ potřebou konkrétní skupiny interních a/nebo externích uživatelů.

CHAOS AKTIV: Jak zajistit integritu aktiv?

CHAOS AKTIV V PRAXI „KAŽDÝ PES JINÁ VES“

Doporučené standardy

TOGAF™ 9

ISO 42010 27000

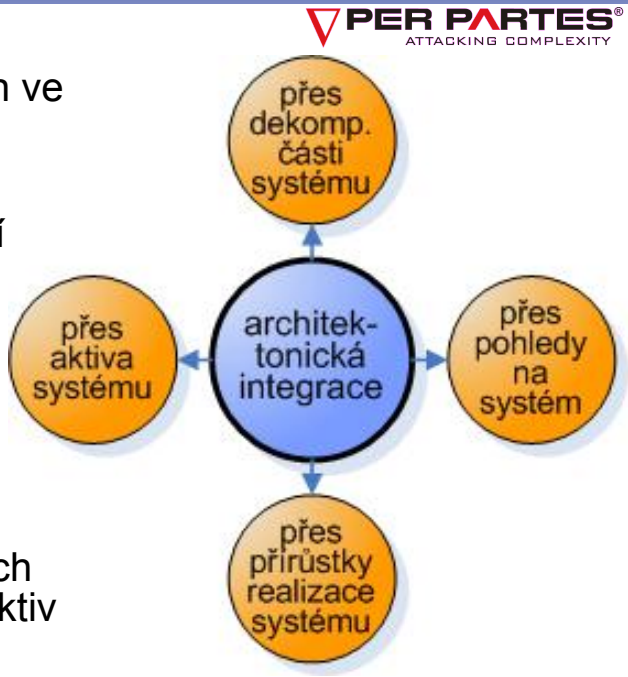
Architektonický integrační management je v praxi prováděn ve čtyřech rovinách:

a) při dekompozici systému k zajištění integrity částí (vertikální integrace do hloubky systému),

b) při pohledech na systém vedených z různých hledisek / zájmů zainteresovaných stran (horizontální integrace architektonických pohledů),

c) při identifikaci architektonických aktiv a jejich integraci do superaktiv (integrita aktiv),

d) při realizaci přírůstkových segmentů systému na cestě od přechodových stavů k cílovému systému (integrita přírůstků).



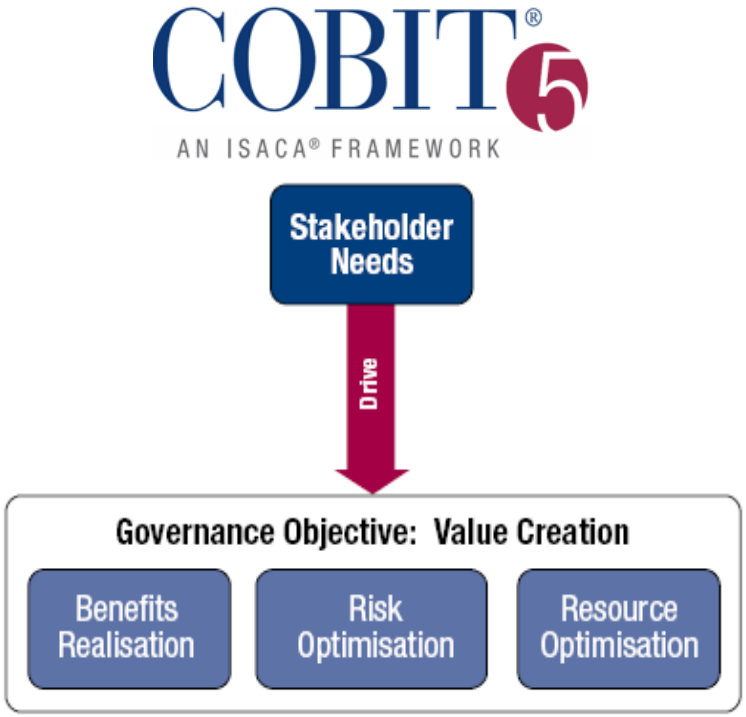
Základním znakem provádění IT Governance je architektonická integrace aktiv.

Pro zájemce doporučuji nezávislou studii Architektura komplexních systémů, architektonická aktiva & integrační management (30 stran), ke stažení je na www.perpartes.cz

(heslo ke stažení zdarma sdělím na přednášce)

CHAOS HODNOT: O jaké hodnoty se usiluje?

O jaké hodnoty se při IT Gov usiluje?
„Organizace existují proto, aby vytvářely hodnotu pro zainteresované strany (stakeholders). Každá organizace, bez ohledu na to, zda je komerční či nikoliv, má vytváření hodnoty jako svůj hlavní vrcholový (governance) cíl. [COBIT 5]



Interní zainteresované strany
představenstvo, generální ředitel (CEO), finanční ředitel (CFO), ředitel pro informatiku (CIO), byznys manažeři, vlastníci procesů, rizikoví manažeři, bezpečnostní manažeři, servisní manažeři, manažeři pro lidské zdroje (HR), interní auditoři, ICT uživatelé, ICT manažeři apod.

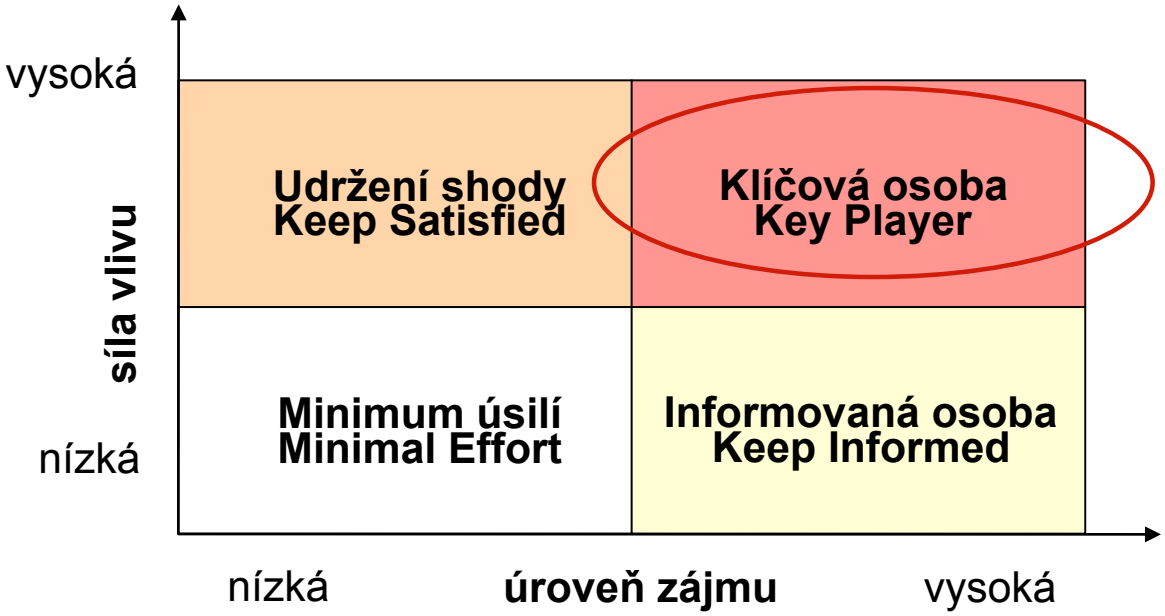
Externí zainteresované strany
externí uživatelé, zákazníci, partnerské organizace, dodavatelé, vlastníci, standardizační organizace, externí auditoři, poradci, regulatorní orgány a vláda, úředníci pro ochranu osobních údajů apod.

Problémem řízení hodnoty jsou konfliktní zájmy zainteresovaných stran. Při ICT governance je nezbytné vyjednávání a rozhodování s cílem balancování zájmů různých zainteresovaných stran.

CHAOS HODNOT: Konflikt zájmů

PER PARTES® ATTACKING COMPLEXITY

Zkoumání síly zainteresovaných stran (stakeholders) podle The Open Group Architecture Framework, version 9 / TOGAF

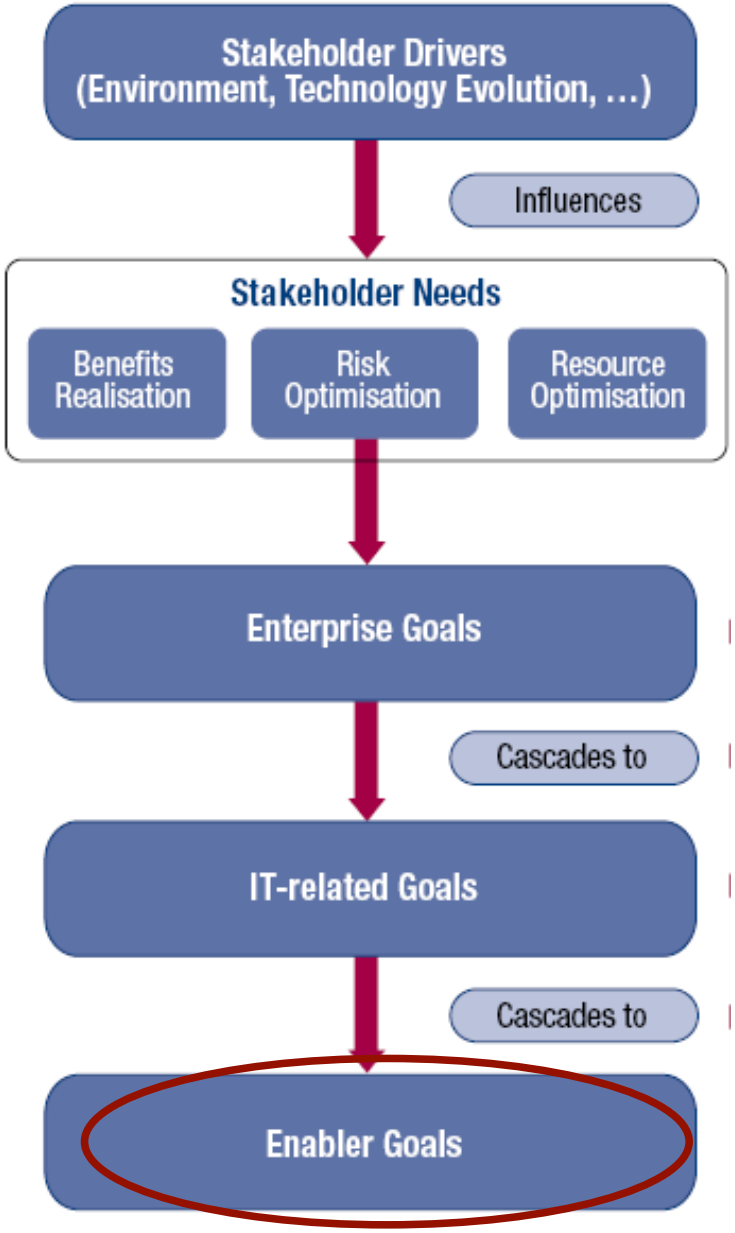


TOGAF - The Open Group Architecture Framework, version 9

Konfliktní požadavky

TOGAF doporučuje klasifikovat zainteresované strany podle pozice a síly, kterou mohou v dané organizaci nařídit, změnit či blokovat směrování architektury a podle toho, zda je v jejich zájmu se do prací v dané oblasti aktivně zapojit či nikoliv. PMBOK® Guide Fifth Edition nově zahrnuje oblast Project Stakeholder Management jako klíčovou oblast řízení.

CHAOS HODNOT: Kaskáda cílů



PER PARTES ATTACKING COMPLEXITY

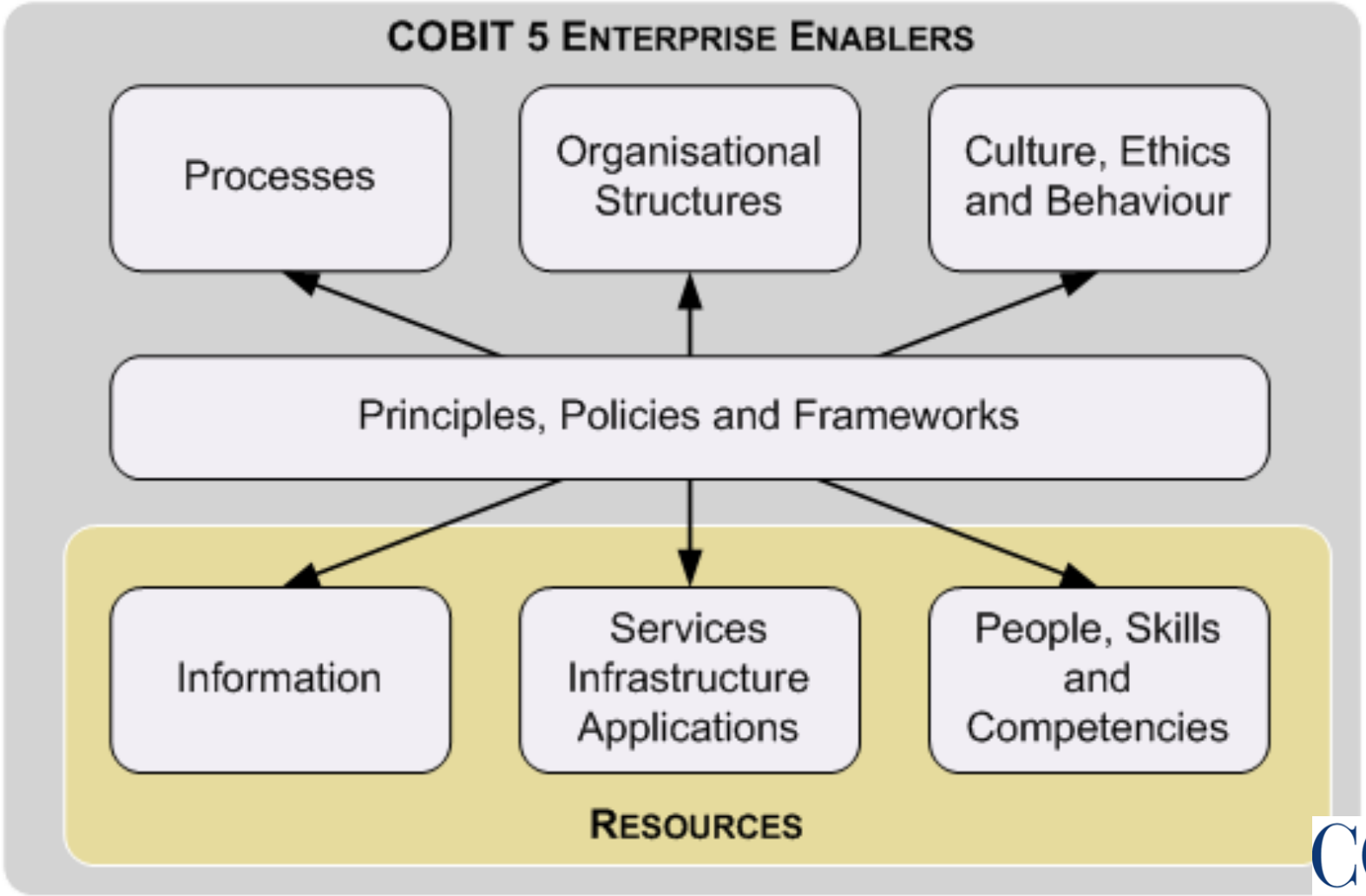
The COBIT 5 goals cascade

"Stakeholder needs have to be transformed into an enterprise's actionable strategy."
"The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals."

Úkolem IT Governance je za každou cenu „udržet v lajně" cestu od hodnot ke konkrétním cílům!

CHAOS HODNOT: Přílišná orientace na procesy

PER PARTES® ATTACKING COMPLEXITY



COBIT® 5 AN ISACA® FRAMEWORK

Přílišná orientace na procesy odsunuje další důležitá aktiva z pozornosti vedení a evokuje paradox „ dělat věci správně“ versus „dělat správné věci“.

CHAOS HODNOT: Jak řídit cíle ve vazbě na hodnoty?

PER PARTES ATTACKING COMPLEXITY

CHAOS HODNOT V PRAXI „SMETÍ DOVNITŘ, SMETÍ VEN“

Koncepce COBIT 5 „enablers“ dává návod, jak v rámci vrcholového řízení (governance) nastavit kaskádu cílů od potřeb zainteresovaných stran až na cíle pro oblasti řízení, které umožní je prosadit a zrealizovat („umožňovače“). Aktiva jsou pak logicky architektonickými prvky v oblastech pokrytých „umožňovači“.

Doporučené standardy

COBIT 5 AN ISACA® FRAMEWORK

Val IT BASED ON COBIT®

ITIL®

Základním znakem řízení hodnot v rámci IT Governance je je řízení cesty od požadavků zainteresovaných stran až ke konkrétním cílům na aktiva.

Pro zájemce doporučuji prezentaci Hodnocení přínosů IT pro business, ke stažení jse na www.perpartes.cz (volně v sekci publikace/prezentace a články)

CHAOS STANDARDŮ: Které standardy aplikovat?

PER PARTES
ATTACKING COMPLEXITY

THE Open GROUP
Making standards work®
TOGAF™ 9

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

Val IT™
BASED ON COBIT®

BPMN

IASA

COBIT® 5
AN ISACA® FRAMEWORK

Risk IT
BASED ON COBIT®

VRM
Value Reference Model

CMMI®

ITIL®

PRINCE2

TRANSLATING STRATEGY INTO ACTION
The BALANCED SCORECARD
Robert S. Kaplan
David P. Norton
"A LANDMARK ACHIEVEMENT."
—Michael Hammer

INTERNATIONAL STANDARD

ISO/IEC/ IEEE

ISO International Organization for Standardization

IEC International Electrotechnical Commission

PMI

IPMA International Project Management Association

IDEF Integrated DEFinition Methods

CHAOS STANDARDŮ: Jsou standardy kompatibilní?

PER PARTES® ATTACKING COMPLEXITY

Vezměme si jako příklad oblast řízení rizik. Přijdeme aplikováním různých standardů k různým rizikům nebo budou identifikována rizika stejná?

Každý standard vztahuje rizika k jiné základně

- k hodnotám, cílům, aktivům, procesům, produktům či interakci zainteresovaných stran …

Každý standard má svůj přístup k identifikaci rizik / scénáře

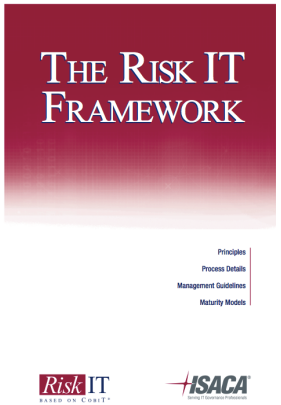
- přístupem shora-dolů, při kterém se zahajuje identifikace rizikových scénářů od všeobecných business cílů a provádí se analýza nejdůležitějších a nejpravděpodobnějších událostí
- přístupem zdola-nahoru, při kterém se zahajuje identifikace rizikových scénářů analýzou seznamu generických scénářů vzniklých ze zkušenosti, které se konkretizují a přizpůsobují na specifické podmínky.

Každý standard jinak chápe vztah riziko - příležitost

- hrozba je nejistá událost s negativním a příležitost s pozitivním efektem na cíle
- riziko negativně a příležitost pozitivně ovlivní dosažení cílů

Každý standard jinak přistupuje k agregace rizik

- rizika včetně jejich dopadu na aktiva se posuzují ve stejné škále individuálně
- na základě vzájemné provázanosti rizik (podle společných zranitelností, příčin, aktérů, času dopadu, aktiv, …) se vytváří shluky působící agregovaně v celkovém rizikového profilu

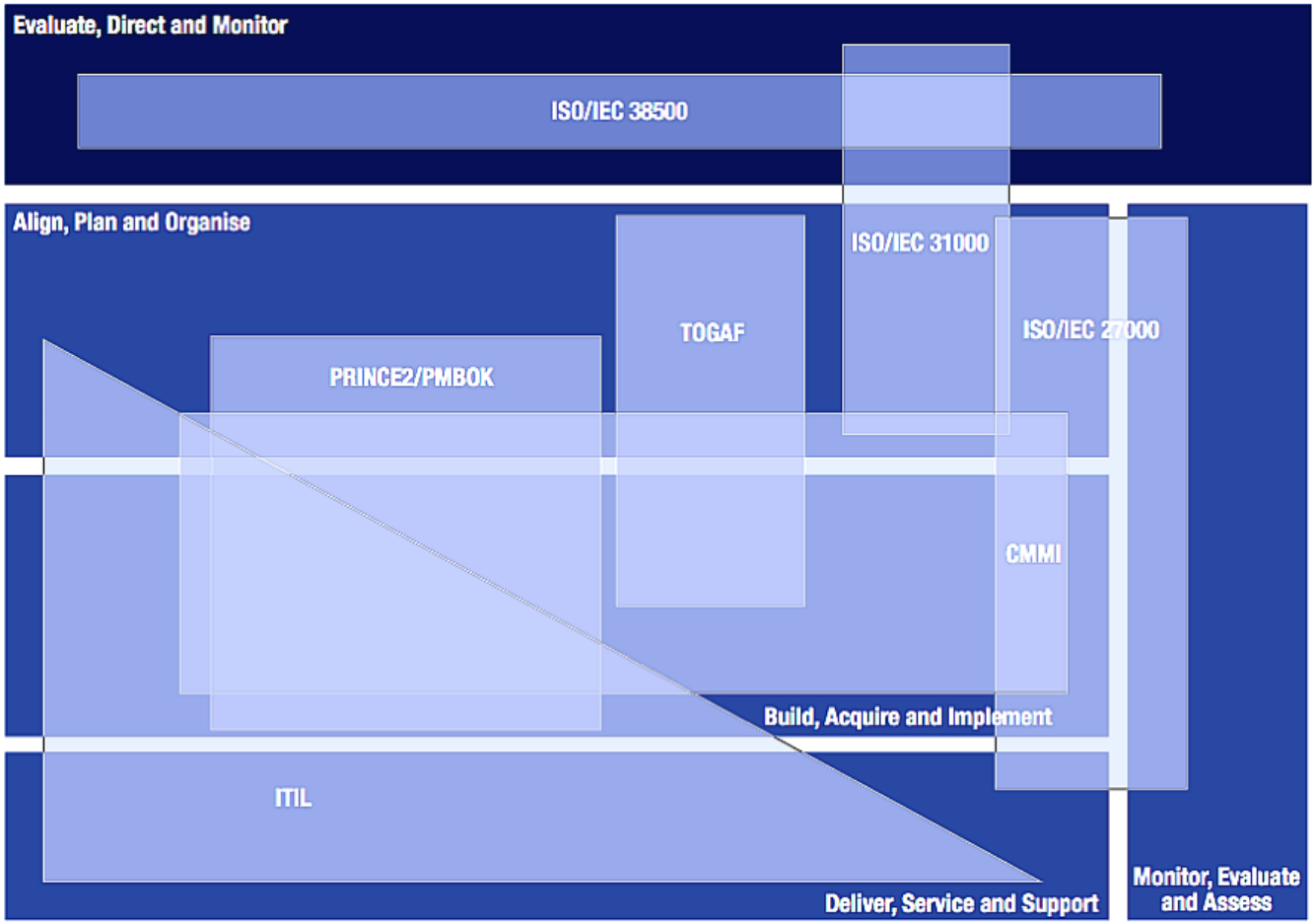


RISK IT obsahuje celkem 36 generických rizikových scénářů pro oblast IT

Základním znakem provádění IT Governance je správné řízení rizik.

CHAOS STANDARDŮ: Aplikujte jeden metod. rámec

PER PARTES® ATTACKING COMPLEXITY



COBIT® 5
AN ISACA® FRAMEWORK

C5 Principle: Applying a Single Integrated Framework:

COBIT 5 is aligned with other major frameworks and standards in the marketplace, such as ITIL®, TOGAF, PMBOK), PRINCE2® and the ISO standards.

Vrcholové řízení IT (ITG) musí stanovit rámec, kterým definuje využití dílčích metodických standardů tak, aby se vzájemně nepřekrývaly s různými nekompatibilními přístupy (jako je např. oblast řízení rizik a příležitostí).

CHAOS STANDARDŮ: Jaké standardy aplikovat?

PER PARTES® ATTACKING COMPLEXITY

CHAOS STANDARDŮ V PRAXI
„MNOHO PSŮ, ZAJÍCOVA SMRT“

COBIT 5:
A single integrated framework will help stakeholders understand how various frameworks, best practices and standards are positioned relative to each other and how they can be used together and could augment each other.

Doporučené standardy

COBIT® 5
AN ISACA® FRAMEWORK

Základním znakem provádění IT Governance je výběr a aplikace vhodných metodik a standardů.

Pro zájemce o oblast řízení rizik doporučuji nezávislou studii Řízení rizik a příležitostí probírající standardy RISK IT, PMI, ISO 27005/31000/10006 a IPMA. Ke stažení je na www.perpartes.cz (heslo ke stažení zdarma sdělím na přednášce)

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Petr Hujňák
Per Partes Consulting
petr.hujnak@perpartes.cz