ISO 9000, 20000, 27000

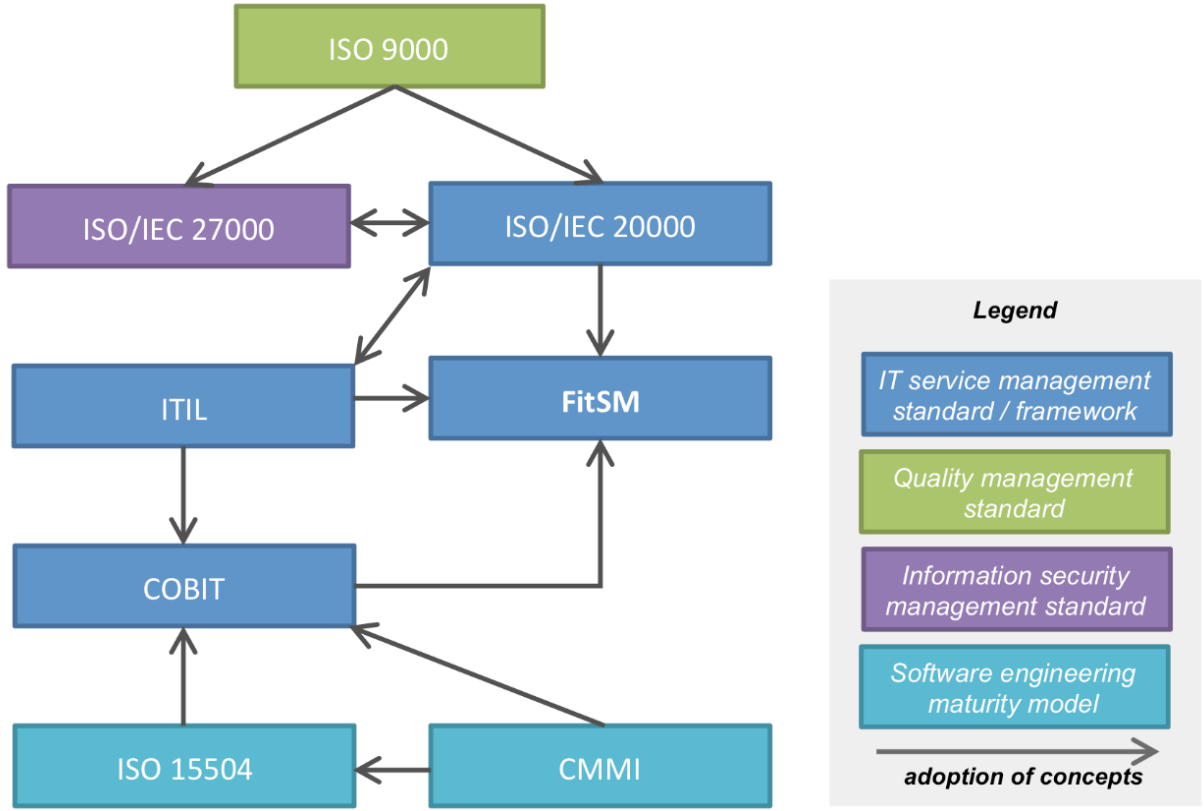
Informační management VIKMA07

Mgr. Jan Matula, PhD.

jan.matula@fpf.slu.cz

III. blok

ITSM & Security management standard



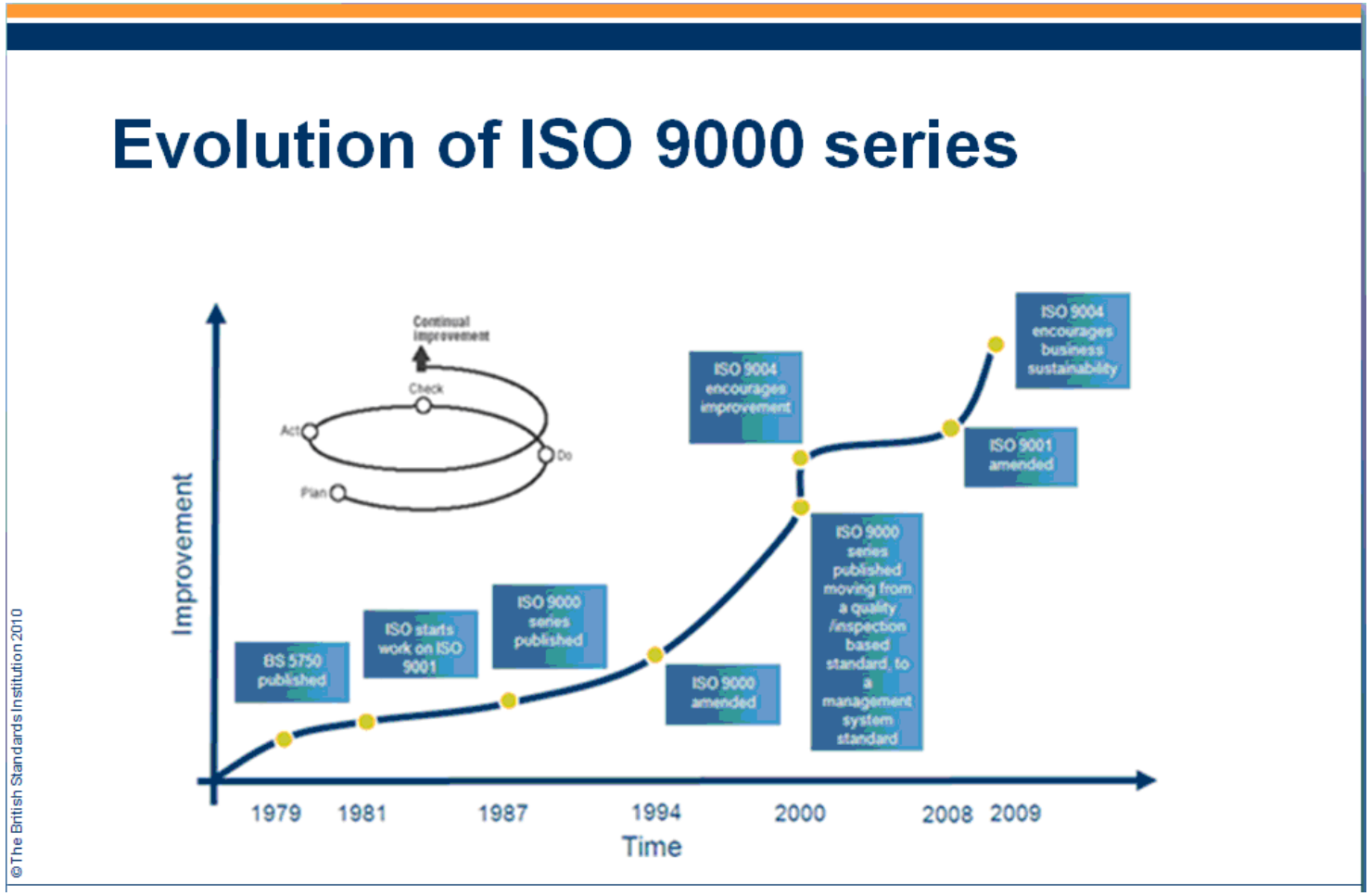
ISO 9000-1

- ISO 9000:2015 Quality management systems – Fundamentals and vocabulary (Zavedena v ČSN EN ISO 9000:2016 (01 0300) Systémy managementu kvality – Základní principy a slovník)
- SO 9001:2015 Quality management systems – Requirements (Zavedena v ČSN EN ISO 9001:2016 (01 0321) Systémy managementu kvality – Požadavky)

Historie ISO 9000

- Normy ISO 9000 byly poprvé zveřejněny v roce 1987 a vzešly z řady norem BS 5750 (British Standard). Určité úpravy a revize proběhly v roce 1994, ale až v roce 2000 vznikla nová ucelená řada ISO 9000, která sloučila tři standardy (ISO 9001, ISO 9002, ISO 9003). V roce 2008 byl systém doplněn o normu ISO 9004, která pouze rozšiřuje již fungující systémy.

Vývoj normy ISO 9000



Použitelnost ISO 9000:2015

- organizace, které usilují o udržitelný úspěch prostřednictvím zavedení systému managementu kvality;
- zákazníky, kteří usilují o získání důvěry ve schopnost organizace trvale poskytovat produkty a služby vyhovující jejich požadavkům;
- organizace, které usilují o získání důvěry v jejich dodavatelském řetězci, že požadavky na produkt a službu budou splněny;
- organizace a zainteresované strany, které usilují o zlepšení komunikace prostřednictvím společného porozumění slovní zásobě používané v managementu kvality;
- organizace provádějící posuzování shody podle požadavků ISO 9001;
- poskytovatele výcviku/školení, posuzování nebo poradenství v managementu kvality;
- zpracovatele příslušných norem.

ISO 9001:2015

- V této normě jsou specifikovány požadavky na systém managementu kvality v případech, kdy organizace potřebuje prokázat svoji schopnost trvale poskytovat produkt nebo službu, které splňují požadavky zákazníka a příslušné požadavky předpisů, a kdy má v úmyslu zvyšovat spokojenost zákazníka, a to efektivní aplikací systému, včetně procesů pro jeho neustálé zlepšování.
- Požadavky normy jsou aplikovatelné v jakékoliv organizaci bez ohledu na její typ nebo velikost nebo na produkty a služby, které poskytuje. Norma používá rámec vypracovaný ISO s cílem zlepšit sladění mezinárodních norem systémů managementu.

ISO 9001:2015

- Norma využívá procesní přístup a zvažování rizik. Procesní přístup, který zahrnuje cyklus PDCA, umožňuje organizaci ujistit se, že jsou pro její procesy zajištěny a řízeny odpovídající zdroje, jsou stanoveny příležitosti ke zlepšování a jedná se podle nich.
- Zvažování rizik umožňuje organizaci určit faktory, které by mohly způsobit odchýlení jejích procesů a jejího systému managementu kvality od plánovaných výsledků, dále zavést preventivní nástroje řízení s cílem minimalizovat negativní účinky a maximálně využít příležitosti, které nastanou.

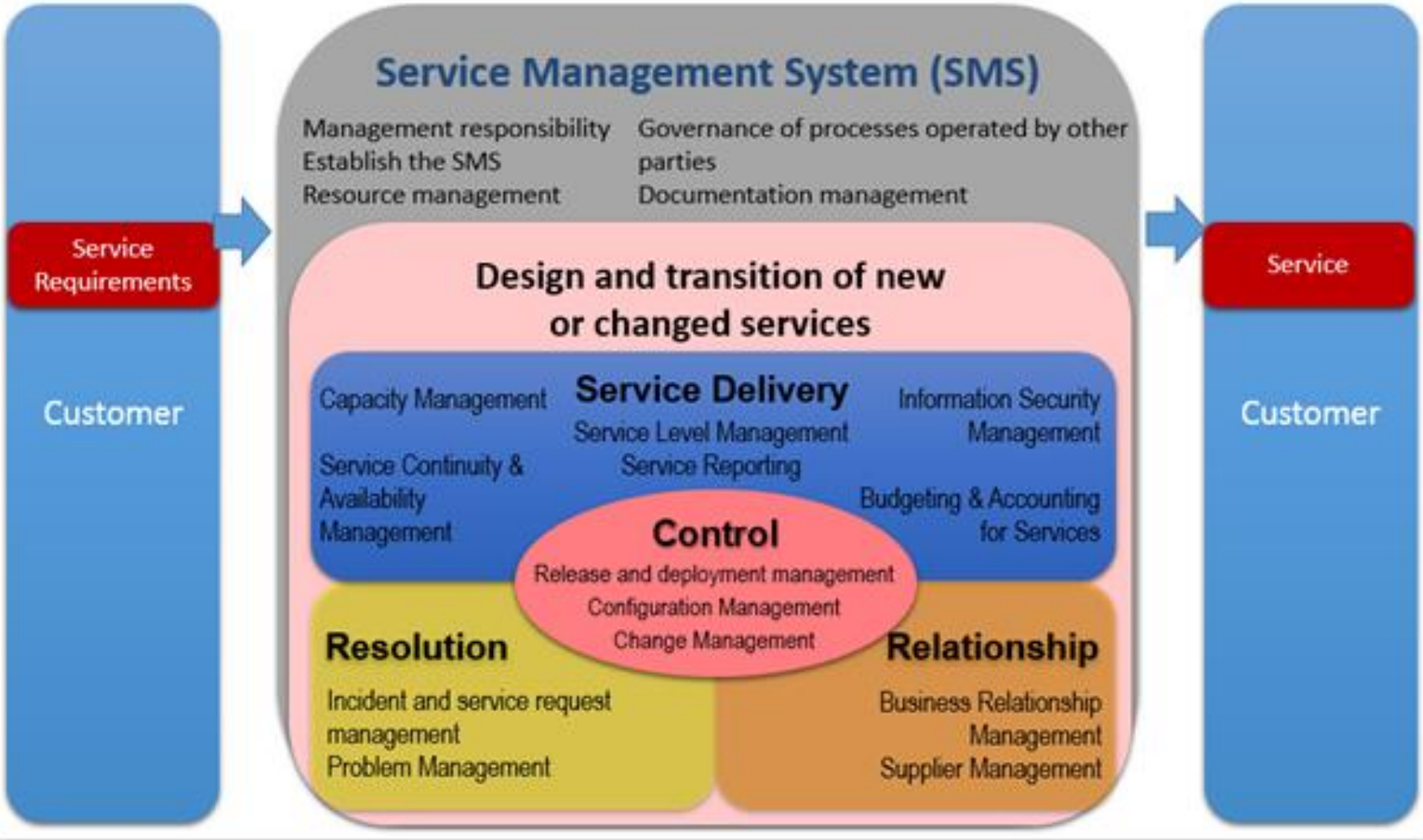
ISO 20000

- ISO 20000 Management služeb pro informační technologie (IT service management) se zaměřuje na zlepšování kvality, zvyšování efektivity a snížení nákladů u IT procesů, popisuje procesů řízení pro poskytování služeb IT a obsahově se řídí úspěšnými ustanoveními IT Infrastructure Library (ITIL) a ITSM.
- Standard ISO 20000 vychází z britského standardu BS 15000, který řeší certifikaci systému řízení IT služeb - ITSM.

ISO 20000

- Norma je orientovaná na IT služby, obsahuje referenční procesy (jak mají procesy řízení IT služeb vypadat).
- Stejně jako ostatní normy ISO vyžaduje následnou certifikaci zavedeného systému řízení (zavedených procesů) v organizaci.
- Výsledkem je certifikát, který je mezinárodně uznávaný a je předpokladem určité zralosti a vyspělosti organizace.

ISO 20000 - Procesy



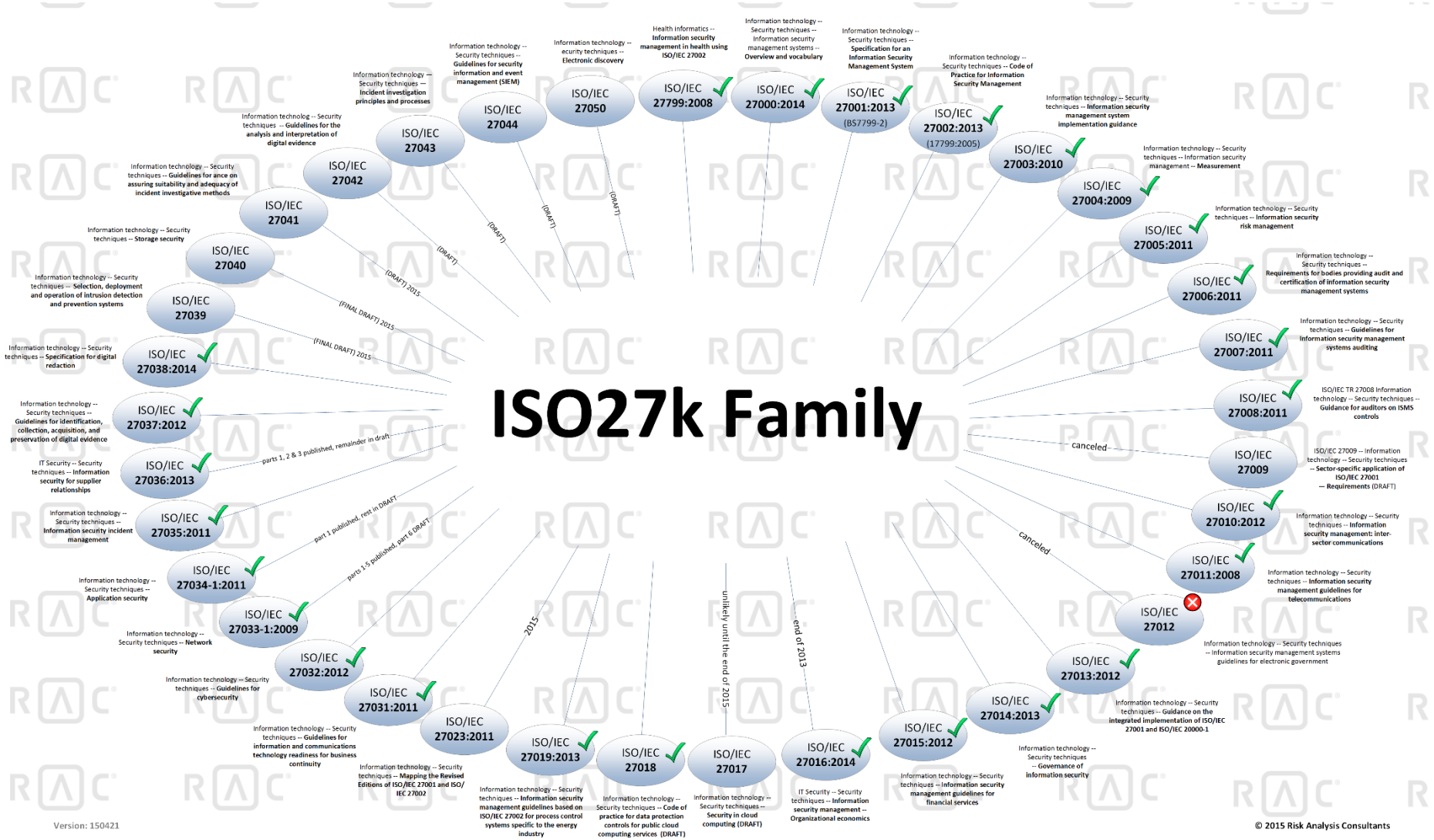
ISO 20000

- Norma ISO 20000 je použitelná ve všech sektorech a odvětvích, ale větší význam má u firem, které dodávají IT nebo poskytují IT služby.
- Vlastnictvím certifikátu ISO 20000 organizace prokazuje vysokou úroveň řízení svých IT procesů a zvyšuje tím důvěryhodnost u zákazníků a partnerů.
- Je zaměřená na řízení IT procesů, tedy na procesy v rozsahu odpovědnosti manažera IT (CIO).

ISO 27000

- ISO 27000 (ISO/IEC 27000) je rodina mezinárodních standardů zaměřená na řízení informační bezpečnosti v organizacích.
- Všechny standardy rodiny ISO 27000 jsou vydávané Mezinárodní organizací pro standardizaci ISO.
- Jednotlivé standardy cílí na různé aspekty informační bezpečnosti v organizacích. Poskytují praktické nástroje pro ty organizace, které chtějí identifikovat a řídit environmentální dopad svého chování a trvale udržovat a zlepšovat environmentální výkonnost.

ISO 27000 Family



Rodina normy ISO 27000

- ISO 27000 je pouze zastřešující rodina, organizace si musí vybrat vždy jednu konkrétní normu pomocí které vyřeší svoje konkrétní potřeby. Klíčová a nejpoužívanější je norma ISO 27001.

ISO 27001 - hlavní norma pro Systém řízení bezpečnosti informací.

ISO 27002 - seznam nejlepších praxí pro řízení informační bezpečnosti

ISO 27003 - návod na zavedení systému řízení informační bezpečnosti (ISMS)

ISO 27004 - řízení informační bezpečnosti - Měření

ISO 27005 - návod pro řízení informační bezpečnosti v organizaci (ISMS).

Rodina normy ISO 27000 (pokračování)

ISO 27006 - požadavky na auditory a certifikační autority informační bezpečnosti v organizaci

ISO 27007 - Informační technologie - bezpečnostní techniky - Návod pro audit systému řízení informační bezpečnosti

ISO 27008 - Informační technologie - bezpečnostní techniky - Návod pro řízení systému řízení informační bezpečnosti

ISO 27010 - Informační technologie - bezpečnostní techniky - Řízení informační bezpečnosti pro komunikaci uvnitř organizace a uvnitř sektoru

ISO 27011 - Informační technologie - bezpečnostní techniky - Návod systému řízení informační bezpečnosti pro telekomunikační společnosti založený na ISO 27002

Rodina normy ISO 27000 (pokračování)

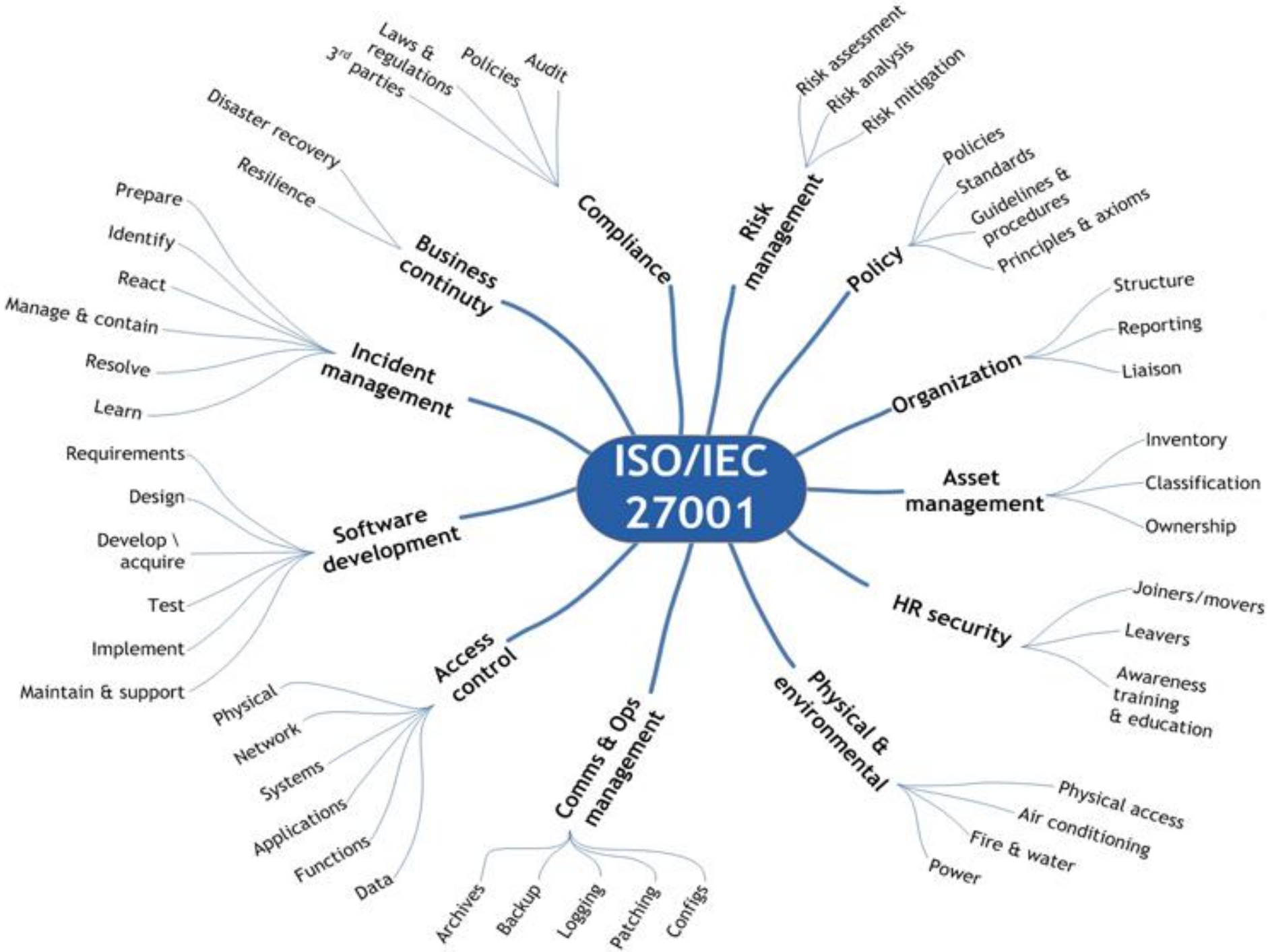
- ISO 27031 - pokyny pro připravenost ICT na business continuity
- ISO 27032 - pokyny pro cybersecurity.
- ISO 27033 - norma zaměřená na bezpečnost sítí
- ISO 27034 - pokyny pro bezpečnost aplikačního softwaru
- ISO 27035 - Informační technologie - Bezpečnostní techniky - Řízení incidentů informační bezpečnosti (Information security incident management)

ISO 27001

- ISO 27001 je označení standardu pro systém řízení informační bezpečnosti v organizaci. ISO 27001 patří do rodiny ISO 27000 a je součástí mezinárodních standardů vydávaných Mezinárodní organizací pro standardizaci ISO (International Organization for Standardization).
- ISO 27001 nahradila normu BS 7799 a stala se mezinárodním standardem pro systémy řízení informační bezpečnosti.

ISO 27001

- ISO 27001 je hlavní normou celé rodiny ISO 27000 a poskytuje komplexní přístup k informační bezpečnosti v organizaci. Zahrnuje veškerá aktiva od dat, přes papírové dokumenty, informační a komunikační technologie až po znalosti. Zahrnuje též rozvoj kvalifikace zaměstnanců a technickou ochranu proti počítačovým podvodům.


ISO/IEC 27001
Compliance
Laws & regulations
3rd parties
Policies
Audit
Risk management
Risk assessment
Risk analysis
Risk mitigation
Policy
Policies
Standards
Guidelines & procedures
Principles & axioms
Organization
Structure
Reporting
Liaison
Asset management
Inventory
Classification
Ownership
HR security
Joiners/movers
Leavers
Awareness training & education
Physical & environmental
Physical access
Air conditioning
Fire & water
Power
Comms & Ops management
Archives
Backup
Logging
Patching
Configs
Access control
Physical
Network
Systems
Applications
Functions
Data
Software development
Requirements
Design
Develop \ acquire
Test
Implement
Maintain & support
Incident management
Prepare
Identify
React
Manage & contain
Resolve
Learn
Business continuty
Disaster recovery
Resilience

ISO 27001

Principy ochrany informací dle ISO 27001 jsou založeny na třech principech informační bezpečnosti:

1) Důvěrnosti - což znamená, že informace jsou přístupné pouze těm, kteří mají povolený (autorizovaný) přístup
2) Celistvosti - což znamená, že existuje správnost a úplnost informací
3) Dostupnosti - což znamená, že oprávnění uživatelé mají přístup k informacím v okamžiku, kdy je potřebují

ISO 27001

- Norma ISO 27001 je určena jak pro organizace soukromého i veřejného sektoru, bez ohledu na jejich velikost nebo lokalitu. Specifikuje požadavky na systém řízení informační bezpečnosti. Využívá se při certifikaci k nezávislému posouzení schopnosti organizace vytvořit a udržovat komplexní systém informační bezpečnosti.
- Norma ISO 27001 je standardně používaná pro certifikaci.

Business Continuity Management

- Business Continuity Management (BCM) je oblast řízení, která je zaměřena na to, aby byly trvale dostupné všechny kritické funkce organizace vůči zákazníkům, dodavatelům a dalším stranám. Tedy aby v případě jejich přerušení byla zajištěna co nejrychlejší obnova běžného provozu.
- BCM upravuje ISO 27031.
- Business Continuity Management se zaměřuje na vytvoření pravidel a plánů, prevenci a snížení následků závažných incidentů nebo katastrof. Je rovněž součástí provozních procesů, které tyto pravidla realizují (například zálohování).

Business Continuity Management

- Cílem BCM je předejít negativních jevům nebo alespoň zmírnit jejich následky a co nejrychlejší obnova běžného provozu.
- Business Continuity Management řeší fakticky každá organizace, nicméně zcela klíčový je pro organizace, kde je vyžadována vysoká míra dostupnosti - výpadek může znamenat ztráty na životech nebo vysoké finanční škody (např. zdravotnictví, banky, důležitá data o zákaznících, výroba atd.)

Continuity Management Process Relationships