Microsoft

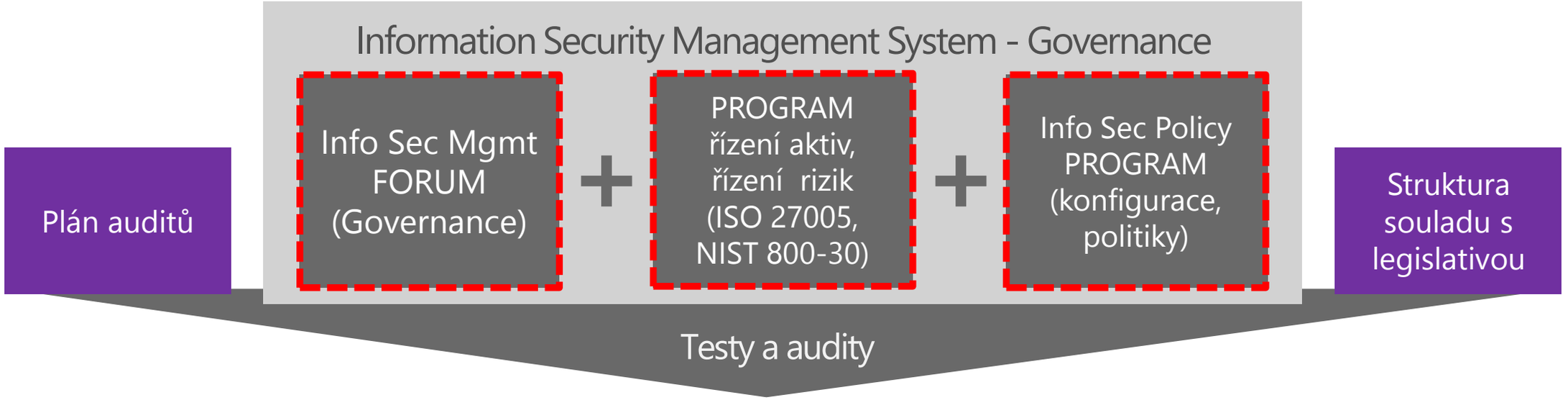
Efektivní přístup ke splnění požadavků ZKB

Zdeněk Jiříček
National Technology Officer

Microsoft

Information Security Management System

Ochrana obchodních zájmů + Standardy a regulatorní požadavky

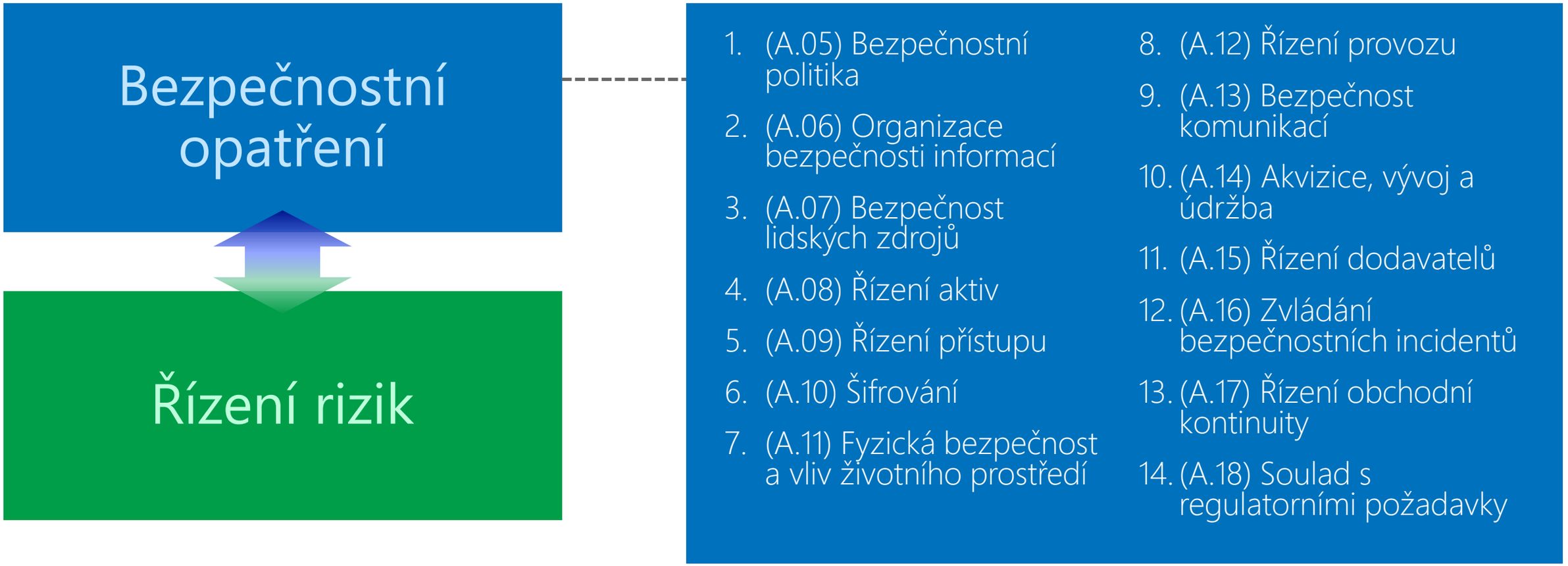


Certifikace a atesty

- ISO / IEC 27001:2005
- SSAE 16/ISAE 3402 - SOC 1
- AT101 - SOC 2 and 3
- PCI DSS (Payment Card Industry)
- FedRAMP P-ATO, FISMA akreditace
- A další...

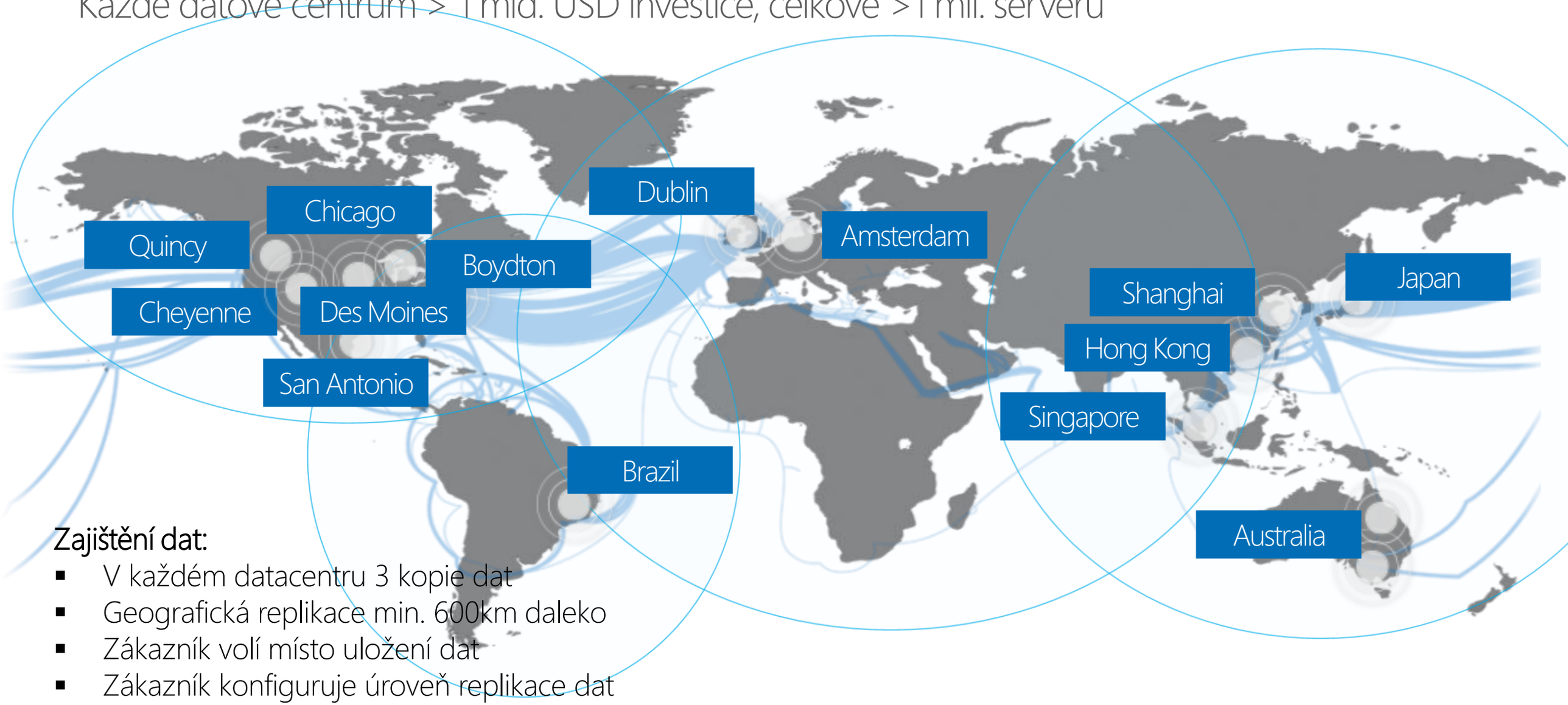
Microsoft cloud: domény pro ISO 27001:2005

Plus další požadavky dle NIST 800-53 a PCI-DSS (Payment Card Industry...)



Škálovatelnost a redundance zdrojů

Každé datové centrum > 1 mld. USD investice, celkově >1 mil. serverů



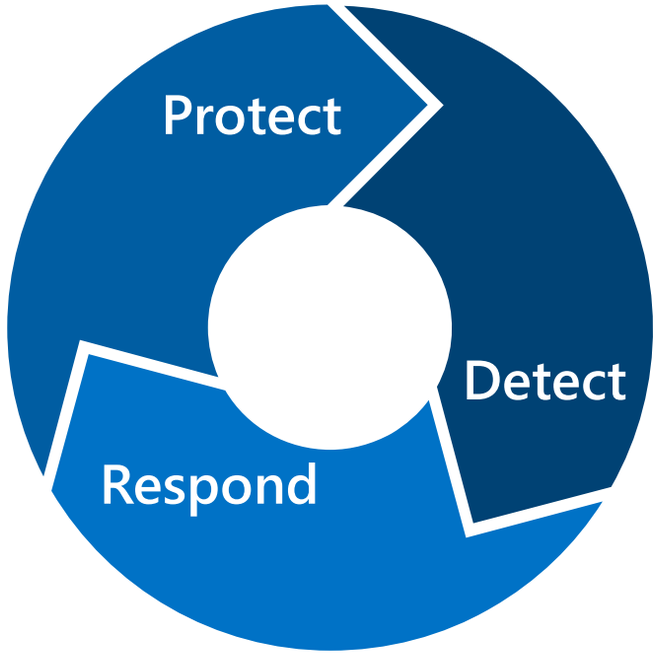
Zajištění dat:

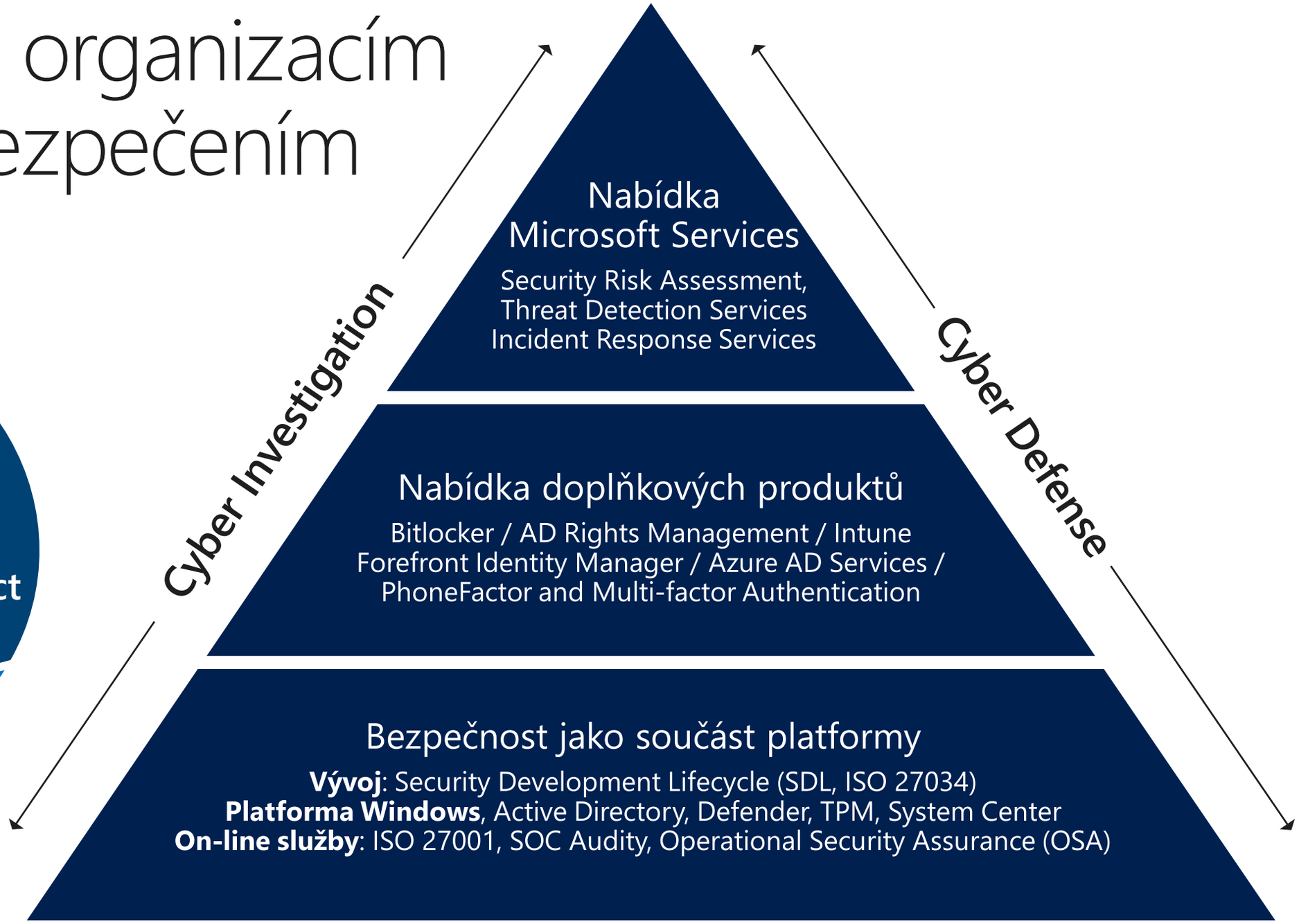
- V každém datacentru 3 kopie dat
- Geografická replikace min. 600km daleko
- Zákazník volí místo uložení dat
- Zákazník konfiguruje úroveň replikace dat

Certifikace MS online služeb – stav 10/2014

Standard - certifikace	Office 365	Microsoft Dynamics CRM	Microsoft Azure	Windows Intune	GFS (Global Foundation Services – infrastruktura datových center)
ISO 27001:2005	Ano	Ano	Ano	Ano	Ano
EU Model Clauses (Standardní smluvní doložky Evropské unie, ověřen „soulad“)	Ano	Ano	Ano	Ano	Ano
EU Safe Harbor	Ano	Ano	Ano	Ano	Ano
PCI DSS (Payment Card Industry Data Security Standard)	N/A	N/A	Ano	N/A	Ano
SOC 1 Type 2 (Service Organization Controls - SSAE 16/ISAE 3402)	Ano	Ano	Ano	Ne, jen Type 1	Ano
SOC 2 Type 2 (AT Section 101)	Ano	Ne	Ano	Ne, jen Type 1	Ano
UK G-Cloud	Ano	Ano	Ano	Ne	N/A
FedRAMP (US) (Moderate)	Ano	Ne	Ano	Ne	Ano
FERPA (US – Education)	Ano	N/A	Ano	N/A	N/A
HIPPA/BAA (US - Healthcare)	Ano	Ano	Ano	Ano	Ano
IPv6	Ano	Ne	Ne	Ne	N/A
CJIS (US - Criminal Justice)	Ano	Ne	Ne	Ne	N/A

Pomáháme organizacím s jejich zabezpečením





Reakce na incident

- Úplný proces v 9 krocích
- Zaměřeno na rychlou identifikaci a obnovení
- Upozornění je součástí smluvních závazků

Vyhláška - §4 Hodnocení hrozeb/zranitelností

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§4 Řízení rizik, odst. 4 – povinná osoba „**zvažuje hrozby**“	Písm. c) zneužití identity jiné fyzické osoby	DIF – Dynamic Identity Framework Assessment
	d) užívání SW v rozporu s licenčními podmínkami	SAM – Software Asset Management
	f) škodlivý kód	SERA – Security Error Reporting & Analysis
	k) trvale působící hrozby (APT)	PADS – Persistent Adversary Detection Services
§4 Řízení rizik, odst. 5 – povinná osoba „**zvažuje zranitelnosti**“	b) uživatelé a administrátoři c) nedostatečná údržba systému d) nevhodné nastavení přístupových oprávnění f) nedostatečné monitorování činnosti uživatelů a administrátorů	MSRA – Microsoft Security Risk Assessment SUM – Software Update Management

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§8 Řízení aktiv

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§8 Řízení aktiv	Odst. 1. c) hodnotí důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti (4 úrovně dle Vyhlášky)	Metodika pro označení primárních aktiv do 4 úrovní (HBI / MBI / LBI / Public)
	Odst. 2. a) identifikuje a eviduje podpůrná aktiva c) vazby mezi primárními a podpůrnými aktivy, důsledky závislostí	CCM – Change & Configuration Management (dle ITIL, volitelně s využitím System Center) SMAP – Service Mapping
	Odst 3. a) 2. - pravidla pro manipulaci s aktivy podle jejich úrovně (sdílení a přenášení...) 3. - přípustné způsoby používání aktiv b) Pravidla ochrany odpovídající úrovni aktiv	Pravidla zabezpečovacích mechanismů: ....Zabezpečené přenosy dat ....RMS pro Outlook / MS Office ....Bitlocker - šifrování (média) ....Elektronický podpis

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

Aktiva - řešení důvěrnosti & integrity

	Integrita: vysoká	Integrita: kritická
Důvěrnost: vysoká	Požadavek **řízení a zaznamenávání přístupu (logy):** Standardní nástroje (Exchange, SharePoint, Office 365). **Přenosy vnější** sítí - **kryptografická** ochrana: SSL/TLS (https); Jednotlivá aktiva externě: RMS nebo S/MIME šifrování (řeší důvěrnost + integritu)	
Důvěrnost: kritická	Požadavek **evidence osob**, které k aktivům přistoupily, vč. ochrany proti **administrátorům**: Auditní logy (Exchange, SharePoint) – záznam činností (čtení, zápis, výmaz, atp.) vč. identity provádějící osoby. Přístup administrátora je možné omezit pomocí RMS na úrovni aktiva. **Všechny přenosy** – **kryptografická** ochrana: Lze SSL/TLS i na vntiřní síti; Jednotlivá aktiva: RMS nebo S/MIME šifrování	
Integrita:	Speciální prostředky sledování **historie změn + identita osoby:** Verzování v SharePointu s uvedením identity uživatele; Editační revize v MS Office (?)	**Průkaznost identity**: Elektronický podpis dokumentu, emailu, časové razítko nebo důvěryhodný archiv Ukládání do úložiště: nastavit kontrolu/vynucení jednoznačné identifikace zpracovatele (proces na SharePointu)

Aktiva – řešení dostupnosti

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
Příloha č. 1 **Dostupnost: vysoká**	Využití **záložních systémů;** obnova může být podmíněna **zásahy obsluhy** či **výměnou technických aktiv**.	Serverové systémy Microsoft „on-premise“ – konfigurace pro vysokou dostupnost a Disaster Recovery. Zálohování / obnova na různé úrovni granularity podle použitého zálohovacího systému. Cloudové služby Microsoft: SLA dostupnost 99,9% nebo vyšší.
Příloha č. 1; **Dostupnost: kritická**	**Záložní systémy;** Obnova je **krátkodobá a automatizovaná**.	„On-premise“ – konfigurace pro vysoká dostupnost s volbou automatizovaných scénářů pro „fail-over“. Lze využít geo-redundantních datových center. Cloudové služby Microsoft: v rámci EU zajištění geo-redundance ze dvou nezávislých datových center.

§10 Řízení provozu a komunikací

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§10 Řízení provozu a komunikací, odst. 3 – provozní pravidla a postupy	a) práva a povinnosti administrátorů a uživatelů	Operations Consulting – Roles and Knowledge Management
	b) postupy spuštění a ukončení chodu systému, obnovení chodu systému po selhání....	RES – Recovery Execution Services (Windows Server, Cluster AD, Exchange, Sharepoint, SQL)... výstup je Disaster Recovery Plan
	c) sledování kybernetických bezpečnostních událostí, ochrana provozních logů	System Center Operations Manager: Proactive Monitoring
	e) řízení a schvalování provozních změn	CCM - Change and Configuration Management

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§11 Řízení přístupu uživatelů

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 11 Řízení přístupu a bezpečné chování uživatelů, odst. 1 a odst. 3	Odst. 1 – Jednoznačný identifikátor (uživatelů) Odst. 3 – Oprávněná osoba zajistí: a) samostatný identifikátor pro aplikace b) administrátorská oprávnění c) přístupová oprávnění d) Přezkoumává přístupová oprávnění, rozdělení uživatelů do přístupových skupin nebo rolí e) nástroj pro ověřování identity / řízení přístupových oprávnění	ESAE – Enhanced Security Administrative Environment DIF – Dynamic Identity Framework Assessment Identity management (Microsoft Active Directory, AD Federation Services, a Forefront Identity Manager)
	f) Bezpečnostní opatření pro mobilní (a jiná) zařízení....	Enterprise Mobility Suite – Azure AD Premium, služba Intune, RMS (Rights Mgmt Services)

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§12 Akvizice, §13 Zvládání incidentů

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 12 Akvizice, vývoj a údržba, odst. 2	b) bezpečnost vývojového prostředí c) bezpečnostní testování změn IS.... před jejich zavedením do provozu	SDL – Security Development Lifecycle (vyvinut pro vývoj SW Microsoft, nyní metodika pro ISO/IEC 27034-1:2011
§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů	a) oznamování kybernetických bezpečnostních událostí (uživatelé, administrátoři atd.) + vedení záznamů b) ....vyhodnocení bezpečnostních událostí..., identifikace bezpečnostních incidentů c) klasifikace incidentů, odvrácení a zmírnění dopadu, zajistí sběr věrohodných podkladů pro analýzu d) prošetří příčiny incidentu, vyhodnotí účinnost řešení, opatření k zamezení opakování incidentu e) dokumentuje zvládání bezpečnostních incidentů	Procesní podpora: Microsoft System Center (Service Manager, Operations Manager) SERA – Security Error Reporting & Analysis PADS – Persistent Adversary Detection Services IR&R – Incidence Response & Recovery Service

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§14 Řízení kontinuity činností

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 14 Řízení kontinuity činností	Odst. 1, písm. b) řízení kontinuity činností formou určení 1. minimální úrovně poskytovaných služeb 2. doby zotavení služby po incidentu 3. doby do obnovení dat po incidentu	Operations Consulting – Service Level Management ITSCM – IT Service Continuity Management
	Odst. 2, písm. b) stanoví, aktualizuje a testuje plány kontinuity	RES – Recovery Execution Services: Windows Server, Cluster AD, Exchange, Sharepoint, SQL Server

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§15 Kontrola a audit

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 15 Kontrola a audit kybernetické bezpečnosti	Odst. 3 – provádí kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů.... a reaguje na zjištěné zranitelnosti	Risk Assessment Program (RAP) as a Service for Microsoft Security (Security Healthcheck) Active Directory Security Assessment

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§17 Nástroj pro ochranu integrity sítí

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 17 Nástroj pro ochranu integrity komunikačních sítí	Odst. 1 a) bezpečný přístup mezi vnější a vnitřní sítí c) kryptografické prostředky (§ 25) pro vzdálený přístup / WiFi	Direct Access (součást OS Windows) a UAG (Unified Access Gateway) a jeho nástupce WinServer 2012 R2; Federace identit ADFS
	b) segmentace - demilitarizované zóny pro přístup k aplikacím z vnější sítě a k zamezení průniku Odst. 2 využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci	NAP (Network Access Protection) – součást OS Windows

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

§18-22 Technická opatření

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 18 Nástroj pro ověřování identity uživatelů	Splňuje dané požadavky	Microsoft Active Directory jako součást OS Windows
§ 19 Nástroj pro řízení přístupových oprávnění	Splňuje dané požadavky	Forefront Identity Manager a prostředky OS Windows
§ 20 Nástroj pro ochranu před škodlivým kódem	b) serverů... c) pracovních stanic, vč. pravidelné aktualizace nástroje (definice a signatury)	System Center Endpoint Protection – součást Core CAL (EA) Windows Defender jako součást OS Windows
§ 21 Nástroj pro zaznamenávání činností systémů, jejich uživatelů a administrátorů	Splňuje dané požadavky	System Center Audit Collection Services a součásti OS Windows
§ 22 Nástroj pro detekci kybernetických bezpečnostních událostí	Odst. 2, písm. b) serverů....	System Center Endpoint Protection SERA – Security Error Reporting & Analysis

§23-26 Technická opatření

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	Microsoft nenabízí SIEM. Lze pokrýt nastavením a vyhodnocením vlastního reportingu.	System Center, a SQL Reporting Services
§ 24 Aplikační bezpečnost	Odst. 1 – bezpečnostní testy zranitelnosti aplikací (přístupných z vnější sítě) před uvedením do provozu a po zásadních změnách zabezpečení	SDL (Security Development Lifecycle) – Application vulnerability assessment
§ 25 Kryptografické prostředky	Symetrické algoritmy: AES 128 nebo 256 bit Asymetrické algoritmy: DSA, EC-DSA, RSA 2048 bit Hash funkce SHA-2 / SHA-256 a vyšší	Součásti OS Windows jako Bitlocker, EFS, RMS, IPSec, KMS, atd., Windows Phone
§ 26 Nástroj pro zajišťování úrovně dostupnosti	Odst. 2 – a) dostupnost informačního systému... c) zálohování důležitých technických aktiv 1. redundancí v návrhu řešení 2. zajištěním náhradních technických aktiv v určeném čase.	System Center Operations Manager Data Protection Manager, Windows Cluster, Cold Backup Windows Azure, StorSimple

Microsoft Services v oblasti Cyber Security

Globální sdílení know-how mezi bezpečnostními architekty, konzultanty, vývojáři

Protect	Detect	Respond
Microsoft Security Risk Assessment (MSRA) Vyhodnotí bezpečnostní rizika, ověří stávající bezp. opatření proti dobrým praktikám	**Security Error Reporting & Analysis (SERA)** Detekce přítomnosti malwaru ve Vaší organizaci, používá Windows jako senzor	**Incident Response & Recovery Service (IR&R)** Pomůže zvládnout incident a obnovit normální provoz
Dynamic Identity Framework (DIF) Vyhodnocení a návrh dynamického řízení identity a přístupu uživatelů	**Persistent Adversary Detection Service (PADS)** Proaktivní vyhodnocení ohrožení trvale působícími hrozbami	
Enhanced Security Administrative Environment (ESAE) Pokročilé technologie a doporučené praktiky pro zvýšení úrovně zabezpečení		

Security Health Check (Win servery, Active Directory)

Test „hygieny“ a praktik při obraně serverové infrastr. (ADSA, SLAM)

Podrobný popis služeb: http://aka.ms/PremierSecurityCatalogue

Shrnutí

- Bezpečnost v rámci Premier Support Services
- Využití stávajících investic do licencí (Enterprise Agmt)
- Rozšíření na míru dle zvolených opatření
  - Doplňkové produkty pro specifické oblasti zabezpečení
  - Pokročilá řešení – řízení přístupu, správa / federace identit, ochrana dokumentů
  - Pokročilé typizované služby Microsoft Services – „dobré praktiky“
- Zabezpečení cloudových služeb (standardy, audity)


Microsoft