SERVICE DESIGN

OBSAH

ÚVOD

Návrh služby je chronologicky druhou fázou životného cyklu služby v rámci ITILu.

Cieľom Service Design je – ako už názov napovedá – navrhnúť nové IT služby. Dizajn služieb sa však neobmedzuje len na navrhovanie nových služieb; navrhuje tiež zmeny a vylepšenia existujúcich služieb. Inými slovami, vždy, keď je potrebné vytvoriť alebo zmeniť službu, vstupuje do fázy návrhu služby a práve tu sa vytvára návrh.

Ak si spomínate späť na fázu stratégie služieb, tá sa týkala finančných aspektov služby, potrieb a dopytu zákazníkov a vôbec sa nezaoberala skutočnou technológiou. Service Design je v tomto smere úplne opačný – tu sa veľmi podrobne rozoberá technológia.

PRIMARY BREAKDOWN – ZÁKLADNÉ ROZDELENIE

Návrh služby sa realizuje prostredníctvom jedenástich hlavných procesov. Najprv si rýchlo vysvetlime, čo tieto procesy robia, skôr než prejdeme k podrobnostiam.
V určitom bode fázy Service Design musí byť vytvorený jasný a podrobný popis všetkých technológií a ich vzájomného pôsobenia, na čo slúži proces **Architecture Management**. Aby bolo možné navrhnúť túto architektúru, množstvo odborníkov bude musieť zvážiť niekoľko oblastí. Aby sa zabezpečilo, že budú správne komunikovať a poskytovať to, čo je potrebné, je zavedený proces **Design Coordination** na koordináciu všetkých týchto činností.
Ak dovolíte prirovnanie: **Design Coordination** je podobný manažérovi, ktorý prideľuje úlohy a termíny ku komplexnej úlohe, a **Architecture Management** je podobný tomu, ako administratívny personál zhromažďuje všetky dokončené úlohy do pekne usporiadaného priečinka alebo balíka.
Legislatívne a priemyselné normy kladú požiadavky, ako je ochrana súkromia alebo odolnosť voči útokom. **Compliance Management** (riadenie súladu) je proces, ktorý zabezpečuje, že naša architektúra spĺňa tieto požiadavky. Podobne, **Information Security Management** (správa informačnej bezpečnosti) zaisťuje, že informácie a údaje spoločnosti nemôžu uniknúť, poškodiť sa alebo zničiť.
Keďže hovoríme o technológiách, existujú *riziká*, ktoré by mohli ohroziť službu, a tie je potrebné riadiť cez **Risk Management**. Technológie majú tiež obmedzenú kapacitu, či už z hľadiska toho, koľko toho môžu pojať, ako rýchlo môžu prenášať, alebo koľko žiadostí dokážu spracovať v danom časovom limite, a to treba brať do úvahy. Na tento účel máme **Capacity Management**.
Niektoré riziká pramenia z katastrof – ako je zničenie majetku alebo strata konektivity v dôsledku výpadku elektriny. Ak by k takýmto udalostiam došlo, mohlo by byť ohrozené samotné poskytovanie služby, v tomto bode sa zaoberáme kontinuitou služby (**Service Continuity**). Tieto typy situácií si zvyčajne vyžadujú iné riešenia ako bežné riziká, a preto je **Service Continuity Management** samostatný proces navrhnutý špeciálne na ich zvládnutie.

Existujú aj dva procesy, ktoré odzrkadľujú skutočnosť, že k rôznym zákazníkom môžeme pristupovať odlišne na základe ich potrieb. Môžeme definovať rôzne **Service Levels – úrovne služieb** (rovnako ako existujú štandardné sedadlá a sedadlá V-I-P na štadióne), a potom sa musíme uistiť, že zákazníci dostanú naše služby na úrovni, ktorú si objednali – inými slovami, že naša služba je pre nich skutočne **dostupná** podľa našej dohody.
Naša služba bude zvyčajne aspoň čiastočne postavená z komponentov alebo bude využívať služby, ktoré poskytujú dodávatelia. Inými slovami, budeme zákazníkmi týchto dodávateľov a iba ak dodajú to, čo sme požadovali, budeme schopní dodať to, čo **naši zákazníci požadovali**. Na zabezpečenie správneho fungovania tohto reťazca je zavedený proces **Supplier Management** (Správa dodávateľov).
Nakoniec, každá služba musí byť zdokumentovaná v našom katalógu služieb (Service **Catalogue**), ktorý je tiež potrebné riadiť.
Toto je teda stručný pohľad na jedenásť procesov patriacich do Service Design. Všetky sú prepojené a ak niektorý z nich nefunguje správne, má to vplyv na funkčnosť všetkých ostatných procesov.
Teraz sa na to môžeme pozrieť bližšie.

SERVICE LEVEL MANAGEMENT

Začneme riadením úrovne služieb – procesom, ktorý sa zaoberá rôznymi úrovňami, na ktorých poskytujeme naše služby. Najjednoduchší spôsob, ako pochopiť, čo sa rozumie pod úrovňami, je predstaviť si rozdiel medzi typickým pasažierom leteckej spoločnosti, verným cestujúcim a členom diamantového klubu alebo medzi štandardným športovým fanúšikom a členom VIP klubu: Pre zákazníkov, ktorí patria k elitnejšej úrovni, poskytovateľ zabezpečuje nadštandardné služby, ako sú klimatizované priestory, garantované miesta na sedenie či nápoje zdarma.
Ak ste už niekedy skúšali mať vlastnú webstránku, možno pre svoju záujmovú činnosť alebo komunitnú skupinu, možno ste si všimli, že webhostingy sú poskytované za výrazne odlišné ceny, ale aj rôzne garantované úrovne dostupnosti. Môžete mať napríklad svoj web zadarmo, ale potom neexistuje žiadna záruka, že bude v prevádzke kedykoľvek, a ak spoločnosť, ktorá poskytla bezplatný hosting, zanikne, nemáte žiadne zákonné páky na to, aby ste dostali svoje dáta späť. Ak ste ochotní zaplatiť pár dolárov ročne, môžete získať čiastočne zaručenú službu, pri ktorej výpadky nepresiahnu desať hodín za mesiac, ale ak sa na stránku pokúsi dostať dvadsať alebo viac návštevníkov naraz, často môžu dostať *time-out* správu, jednoducho preto, že servery robia hosting tisícom iných takýchto webových stránok súčasne.
Keď sa zákazník zaregistruje do služby, súhlasí s konkrétnou úrovňou podpísaním **Service Level Agreement** (zmluvy o úrovni služieb) alebo **S-L-A**. Na tento dokument sa často odkazuje vždy, keď zákazník nie je spokojný so službou, ktorú dostal.
Služba je typicky interne realizovaná spoluprácou viacerých úsekov organizácie spoločnosti, pričom každý z týchto úsekov musí dodať svoju časť v požadovanej kvalite a čase, ak chce spoločnosť ako celok obslúžiť zákazníka k jeho spokojnosti. Napríklad, ak kuchár spáli jedlo, potom bez ohľadu na to, čo čašníci urobia, zákazník sa bude sťažovať, a ak čašník hodí uvarené jedlo na zákazníkov a povie: „Chytaj!“ zákazník sa bude opäť sťažovať. Preto, aby sa zabezpečilo, že každá časť organizácie

poskytuje kvalitnú prácu a načas, uzatvárajú sa medzi týmito časťami dodatočné dohody. Tieto sa nazývajú **Operational Level Agreement**, alebo **O-L-A**.
Existencia rôznych S-L-A a O-L-A znamená, že ľudia v rámci organizácie musia pristupovať k rôznym požiadavkám s rôznym zmyslom pre naliehavosť alebo dôležitosť. VIP klient si vyžaduje viac pozornosti ako štandardný klient. Z tohto a ďalších dôvodov musia byť všetky zmluvy o poskytovaní služieb uložené v **Customer Agreement Portfolio** (portfóliu zmlúv so zákazníkmi). To sa potom používa na objasnenie akejkoľvek neistoty týkajúcej sa spôsobu poskytovania služby.
Toto sú niektoré z pojmov, ktoré definuje Service Level Management a ktoré potrebujeme, aby sme pochopili, ako proces v skutočnosti funguje. Skladá sa zo 4 podprocesov.
Po prvé, ide o **Identification of service requirements** (identifikáciu požiadaviek na službu), proces, ktorý dokumentuje, aké požiadavky zákazníka služba (alebo konkrétna úroveň služby – **Service Level**) splní. Aby sa predišlo nereálnym požiadavkám – to znamená: aby sa neponúklo niečo, čo sa nedá splniť – tieto požiadavky sú po zdokumentovaní podrobené dôkladnému vyhodnoteniu zástupcami všetkých zúčastnených strán. Ak je požiadavka technicky alebo ekonomicky nesplniteľná, títo zástupcovia potom navrhnú alternatívy, ktoré by mohli byť rovnako ústretové, ale reálnejšie.

Agreement sign-off and Service Activation (podpísanie zmluvy a aktivácia služby) je proces, ktorý sa spustí po Service Transition (čo vám len pripomínam, že je ďalšou fázou životného cyklu). Tento proces skontroluje, či je služba správne implementovaná a pripravená na prevádzku. Práve tento podproces kontroluje, či sú všetky O-L-A podpísané ich vlastníkmi a či je S-L-A podpísané zákazníkom. Ak je toto všetko splnené, môže služba vstúpiť do fázy **Service Operation**.

Dohoda so zákazníkom zvyčajne vyžaduje, aby poskytovateľ pravidelne zverejňoval štatistiky o prevádzke služby, čo je miesto, kde prichádza na rad **Service Level Monitoring and Reporting** (monitorovanie a vykazovanie úrovne služieb). Tento podproces zhromažďuje potrebné informácie o dosiahnutých úrovniach služieb, porovnáva ich s dohodnutými úrovňami služieb a potom poskytuje tieto informácie zákazníkom a tiež ďalším relevantným stranám.

Upozorňujeme, že v rámci Availability Management (správy dostupnosti) existuje podobný podproces s tým rozdielom, že **Availability Monitoring and Reporting** (monitorovanie a podávanie správ o dostupnosti) je zvyčajne podrobnejšie a informácie sa nezverejňujú ani zákazníkom, ani iným stranám.

Ako podporný proces **Maintenance of the SLM Framework** (údržba rámca SLM) navrhuje a udržiava základnú štruktúru portfólia zákazníckych zmlúv a poskytuje šablóny pre rôzne dokumenty potrebné pre Service Level Management.

AVAILABILITY MANAGEMENT

Žiadna stratégia sa nedá realizovať bez finančných zdrojov, preto ITIL definuje aj proces finančného riadenia.

Cieľom **Availability Managementu** je definovať, merať, analyzovať a zlepšovať dostupnosť IT služby a všetkých jej aspektov. Zabezpečuje, že IT služby sú spoľahlivé a k dispozícii, keď ich používatelia potrebujú. Hlavným cieľom je zabezpečiť dostupnosť služieb tak, aby zodpovedali obchodným potrebám a zmluvám o úrovni služieb (SLA).

Všeobecný priebeh tohto procesu je nasledujúci:

Service Level Management (správa úrovne služieb) – o ktorej sme hovorili predtým – poskytuje popis úrovní služieb, ktoré zákazníci požadujú. To sa potom berie ako vstup pre proces **Design Services for Availability**, ktorý premieňa tieto úrovne na postupy a technické vlastnosti, ktoré ich splnia. Po implementácii týchto postupov a technických aspektov zabezpečuje **Availability Testing** (testovanie dostupnosti) pravidelné testovanie normálneho aj mimoriadneho zaťaženia infraštruktúry. Okrem toho je cieľom **Availability Monitoring and Reporting** (monitorovania a podávania správ o dostupnosti) zhromažďovať informácie o dostupnosti služieb a komponentov, ktoré sa potom poskytujú manažmentu IT. Akékoľvek nezrovnalosti a varovné signály o súčasnej alebo budúcej nedostupnosti môžu byť následne riešené, aby sa zaistila lepšia dostupnosť.

Availability Management môže poskytnúť usmernenia pre špecifické funkcie v rámci organizácie, ktoré zmierňujú problémy s dostupnosťou. Napríklad dobre fungujúci availability management môže nariadiť operátorom, aby sa zamerali aj na menšie poruchy, ktoré, ak by sa nekontrolovali, by mohli prerásť do veľkých incidentov.

Rozdiel medzi interným a externým pohľadom na dostupnosť:
Interné zameranie (Reliability, Recoverability, Maintainability):
Tieto tri prvky sa týkajú vnútornej schopnosti IT tímu/firmy spravovať a zabezpečiť nepretržitú prevádzku služieb. Sú orientované na to, čo IT oddelenie/firma môže kontrolovať a optimalizovať v rámci svojich zdrojov:

1. **Reliability (Spoľahlivosť):** IT tím/firma sleduje a optimalizuje, aby systémy nepadali a fungovali dlhodobo bez chýb.
2. **Recoverability (Obnoviteľnosť):** Interný pohľad na schopnosť obnoviť službu po výpadku – ako rýchlo a efektívne dokáže IT tím/firma vrátiť systém do pôvodného stavu.
3. **Maintainability (Udržiavateľnosť):** Vzťahuje sa na schopnosť IT tímu/firmy vykonávať aktualizácie, opravy alebo údržbu bez dlhodobého ovplyvnenia užívateľov.

Externý pohľad (Serviceability):
Na rozdiel od predošlých prvkov, **Serviceability** sa týka služieb, ktoré IT oddelenie/firma získava od externých dodávateľov alebo poskytovateľov. Zameriava sa na ich schopnosť poskytnúť podporu v prípade problémov, riešiť incidenty a dodržiavať SLA.

4. **Serviceability (Servisovateľnosť):** Zabezpečuje externá firma alebo poskytovateľ, ktorí sa zaväzujú, že v prípade problémov zasiahnu a dodržia dohodnuté časy na riešenie problémov podľa SLA.

Z pohľadu zákazníka sú zaujímavé najmä výsledky, teda to, či je služba funkčná a dostupná podľa dohody. Zákazníka obyčajne nezaujímajú interné technické detaily, ako sú spoľahlivosť, obnoviteľnosť a udržiavateľnosť. Tie sú pre neho „neviditeľné“ a očakáva, že IT tím sa o ne postará bez toho, aby to ovplyvnilo jeho skúsenosť.
Pre zákazníka je kľúčová najmä **serviceability** – teda rýchlosť a spoľahlivosť reakcie poskytovateľa služieb v prípade problému. Inými slovami, zákazník chce vedieť, že ak sa niečo pokazí, poskytovateľ rýchlo zasiahne a situáciu vyrieši, ako to bolo sľúbené v SLA.

CAPACITY MANAGEMENT

Dostupnosť našej služby priamo súvisí s témou kapacity, na ktorú sa teraz pozrieme.

Cieľom Capacity Management je zabezpečiť, aby mala organizácia dostatočnú kapacitu poskytovaných služieb a IT infraštruktúry potrebnej na to, aby bola schopná poskytovať dohodnuté ciele úrovne služieb. Toto sa musí uskutočniť nákladovo efektívnym spôsobom a načas. Capacity Management plánuje aj do budúcnosti, krátkodobo aj dlhodobo.

Zaujímavým reálnym príkladom správy kapacity v praxi je to, čo sa deje počas veľkých sviatkov, ako je Silvester, mobilným komunikačným sieťam. O polnoci 1. januára zvyčajne dochádza k masívnemu nárastu pokusov o telefonovanie. Infraštruktúra mobilných sietí zvyčajne nie je navrhnutá tak, aby zvládla *všetkých* telefonujúcich súčasne, a preto sa mnohým zákazníkom môže vyskytnúť chyba siete. Ak by sa sieťoví operátori snažili mať dostatočnú kapacitu, potom by zvyčajne museli znášať náklady na takúto kapacitu po zvyšok roka, keď je prevádzka oveľa nižšia.

Aby bolo možné správne plánovať a riadiť kapacitu služby a infraštruktúry, má Capacity Management tri hlavné podprocesy a, ako je bežné v mnohých ITIL procesoch, ďalší podproces na reporting.

Capacity Management sa delí na **Business Capacity Management, Service Capacity Management a Component Capacity Management.**

- **Business Capacity Management** sa zameriava na dlhodobé plánovanie a strategické ciele firmy.
- **Service Capacity Management** rieši aktuálnu výkonnosť služieb.
- **Component Capacity Management** rieši technické detaily jednotlivých prvkov.

Business Capacity Management (riadenie obchodnej kapacity) Je to časť riadenia kapacity, ktorá sa zameriava na súlad medzi **požiadavkami biznisu** (čo firma alebo organizácia potrebuje) a **IT kapacitami**. Cieľom je zabezpečiť, aby IT dokázalo podporovať budúce potreby firmy.
Kľúčom je plánovanie na základe:

- Očakávaného rastu organizácie,
- Nových projektov alebo služieb,
- Zmeny v počte používateľov alebo transakcií.

Príklad z reštaurácie

Predstav si, že reštaurácia plánuje rozšíriť svoj podnik o nové priestory alebo spustiť donáškovú službu. **Business Capacity Management** preverí, či:

1. Kuchyňa zvládne viac objednávok,
2. Personál bude dostatočný,
3. IT systém (napr. objednávkový softvér) zvládne väčší počet zákazníkov.

Zohľadňuje teda **strategické plány** reštaurácie, aby sa kapacita prispôsobila budúcim potrebám. Ako si viete predstaviť, ak sa prepočet, výpočet alebo odhady urobia nesprávne, potom spoločnosť buď nemusí mať dostatočnú kapacitu, alebo môže prísť o peniaze tým, že zaplatí za príliš veľkú kapacitu.

Service Capacity Management (Riadenie kapacity služieb):

Sleduje výkon a kapacitu celej IT služby z pohľadu používateľov. Cieľom je zabezpečiť, aby služba fungovala podľa požiadaviek (napríklad rýchlosť odozvy aplikácie).

- **Príklad**: Ak používatelia sledujú filmy cez streamovaciu službu, **Service Capacity Management** sa stará o to, aby servery zvládli veľký počet používateľov počas špičky (napríklad večer).

Component Capacity Management (Riadenie kapacity komponentov):

Zameriava sa na jednotlivé technické prvky infraštruktúry (servery, procesory, pamäť, sieť). Kontroluje, či majú dostatočný výkon na podporu IT služieb.

- **Príklad**: Ak je problém s databázovým serverom, ktorý nestíha spracovávať požiadavky, rieši to **Component Capacity Management**.

Rozdiel:

- **Service** sa pozerá na IT službu ako celok.
- **Component** sa zameriava na konkrétne technické časti, ktoré službu podporujú.

Ak by sme to prirovnali k reštaurácii:

- **Service Capacity Management** rieši, či má reštaurácia dosť miest a dokáže obslúžiť všetkých zákazníkov.
- **Component Capacity Management** kontroluje, či kuchyňa má dosť ingrediencií a či sporák funguje správne.

RISK MANAGEMENT

Capacity Management sa vo väčšine prípadov bude zaoberať prípadmi, keď dopyt po našej službe stúpa a my musíme byť pripravení tento dopyt uspokojiť.

Sú však veci, ktoré sa môžu pokaziť a negatívne ovplyvniť naše podnikanie. V rámci prípravy na takéto udalosti poskytuje proces **Risk Management** (riadenie rizík) jasný pracovný tok a podporu.

Risk Management nie je jedinečný pre ITIL. Je to opakujúca sa téma vo všetkých metodológiách podnikania a projektového riadenia.

Risk Management vo všeobecnosti pozostáva z posúdenia, aká je pravdepodobnosť výskytu určitej negatívnej udalosti a aký by bol dopad na podnikanie, ak by k nej došlo.

Na podporu Risk Managementu ITIL definuje niekoľko pojmov. Prvým z nich je **Process and Asset Valuation** (Procesné a majetkové oceňovanie), čo je odhad hodnoty konkrétneho procesu alebo aktíva pre naše podnikanie. Toto je potom jeden zo vstupov pre **Business Impact and Risk Analysis** (Analýza dopadov na podnikanie a rizík), ktorá hodnotí pravdepodobnosť výskytu rizikovej udalosti a jej dopad na naše podnikanie. Výsledkom tejto analýzy je **Risk Register** (register rizík), zoznam všetkých rizík podľa priorít, s ktorými je potrebné sa následne vysporiadať.

Pri rozhodovaní o opatreniach na zmiernenie rizika sa používa proces Assessment of Required Risk Mitigation (posúdenie požadovaného zmiernenia rizika). Tento proces potom priradí každé riziko vlastníkovi rizika – **Risk Owner**, ktorý je zodpovedný za implementáciu týchto zmierňujúcich opatrení a za priebežnú údržbu.

Všetky tieto čiastkové procesy sú podporované podporou riadenia rizík – **Risk Management Support**, ktorá definuje celkový rámec alebo politiku riadenia rizík.

Príklady Risk Mitigation

1. Zálohovanie dát
    - **Riziko:** Strata dôležitých dát kvôli zlyhaniu hardvéru alebo kybernetickému útoku.
    - **Mitigácia:** Implementácia pravidelného zálohovania dát (napr. každý deň alebo týždeň) na bezpečné úložisko mimo hlavnej infraštruktúry, napríklad do cloudu alebo na iný fyzický server.

Príklad: Reštaurácia zálohuje všetky objednávky a údaje o zákazníkoch z ich objednávkového systému, aby ich v prípade výpadku IT mohla rýchlo obnoviť.

2. Redundantné servery
    - **Riziko:** Ak server zlyhá, všetky služby sa stanú nedostupnými.
    - **Mitigácia:** Zavedenie redundancie serverov (napr. využitie clusterov alebo failover riešení), aby sa druhý server automaticky zapol, ak prvý zlyhá.

Príklad: E-shop má dva servery, takže aj keď jeden padne, web stále funguje, a zákazníci môžu nakupovať.

3. Pravidelné bezpečnostné aktualizácie
    - **Riziko:** Zraniteľnosti v softvéri môžu byť zneužité hackermi.
    - **Mitigácia:** Pravidelné aktualizácie operačných systémov, softvérov a firewallov, aby boli odstránené známe chyby a zvýšila sa bezpečnosť.

Príklad: IT tím reštaurácie pravidelne aktualizuje svoj objednávkový systém, aby chránil údaje zákazníkov pred hackermi.

4. Testovanie záložných plánov (Disaster Recovery Tests)
    - **Riziko:** Počas krízovej situácie (výpadok IT, prírodná katastrofa) nebudú zamestnanci vedieť, ako správne reagovať.
    - **Mitigácia:** Pravidelné testovanie plánu obnovy, aby každý vedel, čo má robiť, a plán bol pripravený na ostré použitie.

Príklad: Spoločnosť simuluje výpadok IT a testuje, ako rýchlo dokáže obnoviť služby.

5. Kontrola prístupov a oprávnení
    - **Riziko:** Neoprávnené osoby môžu mať prístup k citlivým údajom.

- **Mitigácia:** Zavedenie striktnej kontroly prístupových práv (napr. iba admin môže meniť nastavenia servera, bežní používatelia majú obmedzený prístup).

Príklad: Iba manažér reštaurácie má prístup k finančným reportom, aby sa minimalizovalo riziko úniku údajov.

6. Školenia zamestnancov o kybernetickej bezpečnosti
   - **Riziko:** Zamestnanci môžu nevedomky otvoriť phishingové e-maily alebo zdieľať citlivé údaje.
   - **Mitigácia:** Pravidelné školenia o bezpečnom používaní IT a rozpoznávaní podvodných aktivít.

Príklad: Zamestnanci reštaurácie sa učia, ako rozpoznať podvodné e-maily a nepoužívať jednoduché heslá.

7. Pravidelný monitoring systému
   - **Riziko:** Zlyhania alebo útoky môžu zostať nepovšimnuté, čo môže spôsobiť veľké škody.
   - **Mitigácia:** Zavedenie monitorovacieho nástroja, ktorý upozorní na podozrivé aktivity alebo klesajúci výkon.

Príklad: Monitoring systému reštaurácie upozorní IT tím, ak databázový server prekročí povolené zaťaženie.

SUPPLIER MANAGEMENT

Ďalším procesom, na ktorý sa pozrieme podrobnejšie, je Supplier Management (riadenie dodávateľov).

Proces Supplier Management zabezpečuje, že zmluvy s dodávateľmi sú nastavené (a udržiavané) tak, aby podporovali potreby nášho podnikania, a dodávatelia dodávajú všetky dohodnuté dodávky podľa zmlúv.

Supplier Management sa vo všeobecnosti vykonáva podľa dodávateľskej stratégie – **Supplier Strategy**, čo je usmernenie, ktoré definuje, ako budeme obstarávať tovary a služby. Táto smernica zvyčajne definuje kritériá pre výber najlepších dodávateľov – v niektorých prípadoch môžu byť primárnym kritériom náklady, ale zaručená kvalita sa vo všeobecnosti považuje za dôležitejšiu.

Na základe tejto stratégie potom naša organizácia zvyčajne podpíše **Underpinning Contract** (Podkladovú zmluvu) s vybranými dodávateľmi, ktorá definuje pravidlá a podmienky pre Purchase Orders (nákupné objednávky) v budúcnosti. Tento Underpinning Contract by preto mohol definovať ceny, za ktoré budeme nakupovať napríklad komponenty infraštruktúry alebo služby.

Všetky zmluvy s dodávateľmi sú uložené v **Supplier and Contract Management Information System** (informačnom systéme riadenia dodávateľov a zmlúv) alebo S-C-M-I-S

To sú niektoré z pojmov, ktoré ITIL definuje pre Supplier Management, čo nám umožňuje pozrieť sa na jeho podprocesy.

Podprocesy riadenia dodávateľov sú v podstate presnými kópiami toho, ako by riadenie dodávateľov fungovalo v akomkoľvek inom odvetví:

Horeuvedená Supplier Strategy je výstupom procesu s názvom **Providing Supplier Management Framework** (Poskytovanie rámca pre riadenie dodávateľov) – proces, ktorý riadi a štandardizuje spôsob, akým obstarávame služby a aktíva.

Na základe stratégie potom môžeme použiť **Evaluation of new Supplier and Contracts** (Hodnotenie nových dodávateľov a zmlúv), ktoré vyhodnotí možných dodávateľov a vyberie tých dodávateľov, ktorí najlepšie vyhovujú našim obchodným potrebám.

To potom vedie k zakladaniu nových dodávateľov a zmlúv – **Establishing new Suppliers and Contracts**. Po podpísaní zmlúv sa **Processing of Standard Orders** (Spracovanie štandardných objednávok) používa na objednanie služieb a tovaru pre dodávateľov.

Zmluvy sú zvyčajne dohodnuté na obdobie jedného roka alebo niekoľkých rokov a my používame **Supplier and Contract Review** (preskúmanie dodávateľov a zmlúv) na vyhodnotenie toho, či dodávatelia dodávajú v súlade s dohodou a či sú zmluvy stále zosúladené s našimi potrebami. V prípade zistenia nedostatkov je potrebné definovať opatrenia na zlepšenie - tieto opatrenia sa môžu týkať kvality, ceny alebo časových parametrov zákaziek.

Keď zmluva dosiahne koniec svojej platnosti, **Contract Renewal or Termination** (Obnovenie alebo ukončenie zmluvy) vyhodnotí, či bude zmluva potrebná, a v závislosti od výsledku sa zmluva obnoví alebo ukončí.

INFORMATION SECURITY MANAGEMENT

Kľúčovou témou v IT biznise je bezpečnosť dát. Zákazníci a používatelia zverujú svoje údaje poskytovateľovi služieb a očakávajú, že tieto údaje budú chránené. **Information Security Management** (riadenie bezpečnosti informácií) je proces, ktorý zabezpečuje túto ochranu.

Pre poskytovateľa IT služieb je dôležité brať bezpečnosť údajov vážne, a preto je **Information Security Management** súčasťou Security Management strategy (celkovej stratégie správy bezpečnosti) – táto celková stratégia sa vzťahuje aj na fyzickú bezpečnosť, prístup do budov a kancelárií a ďalšie témy.

Cieľom **Information Security Management** je zabezpečiť dôvernosť, dostupnosť a integritu údajov, informácií a tiež IT služieb ako celku. ITIL Security Management zvyčajne tvorí súčasť

Confidentiality (dôvernosť) znamená, že informácie sú prístupné iba oprávneným používateľom – inými slovami, nikto iný sa k údajom nedostane.

Availability (dostupnosť) znamená, že údaje musia byť prístupné vždy, keď o ne požiadajú oprávnení používatelia, pokiaľ sú takéto požiadavky predložené v súlade so zmluvou o poskytovaní služieb.

Integrity (integrita) údajov znamená, že údaje nemožno poškodiť alebo upraviť bez výslovného povolenia oprávnených používateľov.

V poslednom desaťročí došlo k niekoľkým vážnym narušeniam bezpečnosti IT – viacerým službám boli ukradnuté databázy zákazníkov a v niektorých prípadoch boli zverejnené alebo predané iným. Vždy, keď k takémuto prieniku dôjde, vyšetrovatelia analyzujú, ako boli údaje zabezpečené, kto k nim mal prístup a či sa pravidelne vykonávali bezpečnostné audity.

Medzinárodná norma ISO 27 001 sa vo všeobecnosti používa ako požadované minimum a akékoľvek nezhody môžu byť interpretované ako porušenie **due diligence** (povinnej starostlivosti), čo umožňuje zákazníkom požadovať náhradu škody. Existencia tohto a podobných štandardov je tiež dôvodom, prečo ITIL neposkytuje podrobné vysvetlenie všetkých bezpečnostných pojmov a namiesto toho len zdôrazňuje najdôležitejšie oblasti, čím pomáha organizáciám správne aplikovať bezpečnostné hľadiská na iné procesy.

Information Security Management sa skladá zo štyroch podprocesov.

Design of Security Controls (Návrh bezpečnostných kontrol) navrhuje pravidlá a postupy, ktoré zabezpečia ochranu údajov a informácií. Jedným z nich sú bezpečnostné testy, ktoré sa potom pravidelne vykonávajú prostredníctvom **Security Testing** (Testovania bezpečnosti). Tieto testy musia preskúmať **všetky** bezpečnostné mechanizmy.

Počas každodennej prevádzky je **Management of Security Incidents** (Správa bezpečnostných incidentov) proces, ktorý zisťuje a rieši incidenty súvisiace s bezpečnosťou, ako sú útoky hackerov, a ak dôjde k narušeniu bezpečnosti, tento proces sa snaží minimalizovať spôsobené škody. Aby to fungovalo, funkcie zahrnuté v tomto procese musia byť splnomocnené na vykonávanie akcií, ako je vypnutie pripojení. To má nešťastný vedľajší účinok, že títo jednotlivci sú atraktívnym cieľom útokov sociálneho inžinierstva.

A nakoniec, **Security Review** je proces, ktorý pravidelne hodnotí všetky bezpečnostné pravidlá, postupy, privilégiá a personál, aby sa skontrolovalo, či sú stále dostatočné na ochranu údajov a informácií, a overí sa, či bolo testovanie bezpečnosti vykonané dôkladne. Zistenia sa používajú ako vstupy pre proces **Design of Security Controls**, čím sa zabezpečujú pravidelné zlepšenia.

ARCHITECTURE MANAGEMENT

Najvyšším cieľom Service Design je – ako už názov napovedá – navrhnúť nové alebo zmenené služby. Tieto návrhy reprezentuje Enterprise Architecture, ktorá je riadená **Architecture Management**om – finálnym procesom, na ktorý sa podrobnejšie pozrieme v tejto kapitole.

Budovanie **Enterprise Architecture** (podnikovej architektúry) je komplexná úloha, ktorá si od účastníkov vyžaduje vysokú odbornosť. Enterprise Architecture je v podstate plánom vnútorného fungovania podniku, čo znamená, že opisuje nielen technológiu a jej prepojenia, ale aj informácie, aplikácie a podnikanie. Ako si viete predstaviť, tieto podrobné plány sú mimoriadne cenné.

Enterprise Architecture sa zmení, keď si Service Design uvedomí, že súčasná architektúra už nemôže plne podporovať službu. Ak chcete vykonať zmenu, musíte najprv odoslať **Change Request for Enterprise Architecture** (požiadavku na zmenu podnikovej architektúry). Tento dokument musí

obsahovať všetky podrobnosti o požadovanej zmene alebo doplnení a potom sa ním ďalej zaoberá **Service Transition**, čo je ďalšia logická fáza životného cyklu služby.

Architecture Management sa tiež snaží definovať **Application Framework** (aplikačný rámec), ktorý je súborom pravidiel, princípov, smerníc a štandardov, ktorých cieľom je uľahčiť používanie a opätovné použitie IT infraštruktúry, viac štandardizovanej a predvídateľnejšej.

Pre lepšie pochopenie si zoberme príklad zo sveta mimo IT. Až do nedávnej doby, vždy, keď chcela automobilka vyrobiť nový model, musela všetko navrhnúť od začiatku – motor, prevodovku, podvozok, riadenie…

V rokoch 2000 až 2010 však niektoré automobilky vyvinuli svoje zjednocujúce „modulárne platformy“, ktoré sú navrhnuté tak univerzálne, že na nich možno postaviť autá s výrazne odlišnými rozmermi, hmotnosťami a typmi motorov. To potom zjednodušuje proces navrhovania, urýchľuje vývoj a znižuje náklady. V tomto príklade by tieto modulárne platformy boli súčasťou **architektúry**, zatiaľ čo ďalšou časťou architektúry by boli montážne linky a továrne.