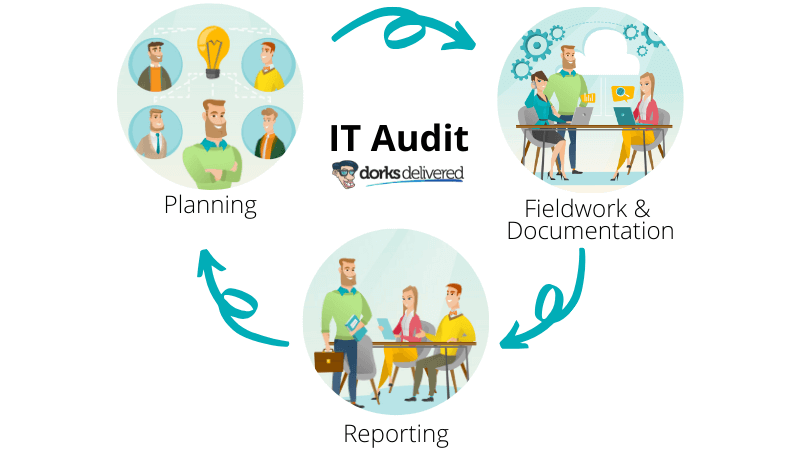
**İT və Biznes (İT Audit)**

**I Hissə**

****

GİRİŞ

* 1. İnformasiya Texnologiyalarının yaranması bizim iş tərzimizi bir çox cəhətdən dəyişdi və audit də istisna deyil. İndi demək olar ki, hər yerdə yayılmış Kompüter, şübhəsiz ki, ən effektiv biznes alətlərindən biri olsa da, avtomatlaşdırılmış biznes mühitinin zəifliklərini də özü ilə gətirdi. Manual əməliyyatların qələm və kağızı kompüterləşdirilmiş proqramların onlayn məlumat daxil edilməsinə yol açdı; fayl kabinetlərinin qıfılları və açarları elektron sənədlərə girişi məhdudlaşdıran parollar və identifikasiya kodları ilə əvəz edilmişdir. Hər bir yeni zəifliyə nəzarət edilməlidir; hər bir nəzarətin adekvatlığının qiymətləndirilməsi auditin yeni üsullarını tələb edir.
  2. 1.2 Son onillikdə əksər Hökumət Departamentləri, Dövlət Sektoru Müəssisələri və özəl orqanlar öz əməliyyatlarını böyük şəkildə kompüterləşdirməyə başlamışlar. Başlanğıcda kompüterlər yüksək alış və istismar xərclərinə görə yalnız böyük təşkilatlarda mövcud idi. Daha sonra fərdi kompüterlərin meydana gəlməsi və xərclərin sürətlə azalması orta ölçülü təşkilatlara da məlumatların emalı üçün İnformasiya Texnologiyalarından yararlanmağa imkan verdi. Hal-hazırda, güclü mikrokompüterlərin və onlarla əlaqəli paketlənmiş proqram təminatının geniş yayılması kompüterlərin hətta kiçik təşkilatlar tərəfindən geniş yayılması ilə nəticələndi. Müvafiq olaraq, məlumat itkisi imkanları və əlaqəli təşkilati xərclər yeni risk faktorları ilə birlikdə çox artmışdır. Şəbəkənin zəifliyi ilə əlaqədar olaraq, İS sistemlərində insayderlər və kənar şəxslər tərəfindən məlumatların dəyişdirilməsi təhlükəsi daha yüksəkdir.
  3. Kompüterlərin özləri sadəcə məlumatların elektron emalı (electronic data processing - EDP) sistemlərindən İnformasiya Texnologiyaları (İT) Sistemləri sahəsinə keçdilər, çünki onlar yalnız məlumatları emal etmir, həm də təşkilati müxtəlif səviyyələrdə qərar qəbul etməyə təsir edən geniş çeşidli məlumatları saxlayır, istifadə edir və ötürürlər. Əslində, kompüter şəbəkə sistemlərinin yaranması və böyüməsi ilə kompüter sistemləri indi İnformasiya Sistemləridir (İS) termini ilə əvəzləndi və bu təkamülün əksi olaraq, “EDP auditi” termini əsasən “İnformasiya Texnologiyaları Auditi” və “İnformasiya Sistemlərinin Auditi” kimi terminlərlə əvəz edilmişdir.
  4. İnvestisiya və kompüterdən asılılığın artması ilə Məlumatların bütövlüyü, sui-istifadə, məxfilik və s. Manual sistemlər ilə müqayisədə xüsusilə çatışmazlıqlı nəzarət mühitində həyata keçirilən İT sistemində müxtəlif risklərə məruz qalmağı minimuma endirmək üçün adekvat tədbirlərin işlənib hazırlanmasına və idarə olunmasına əminlik təmin etmək üçün müstəqil audit tələb olunur.

**İT Auditinin tərifi**

* 1. ***Professor Ron Veber(Monaş Universitetinin fəxri professoru; Kvinslend Universitetinin fəxri professoru) İT Auditi “kompüter sisteminin aktivləri qoruyub qorumadığını, məlumatların bütövlüyünü saxlayıb saxlamadığını, təşkilati məqsədlərə səmərəli şəkildə nail olmağa imkan verib, vermədiyini və resurslardan səmərəli şəkildə istifadə edilib edilmədiyini müəyyən etmək üçün sübutların toplanması və qiymətləndirilməsi prosesi” kimi müəyyən edir.***

İT Auditi Maliyyə Auditlərini (təşkilatın maliyyə hesabatlarının düzgünlüyünü qiymətləndirmək üçün), Əməliyyat Auditlərini (daxili nəzarət strukturunun qiymətləndirilməsi), İnformasiya Sistemlərinin Auditini (fəaliyyət auditi daxil olmaqla), İxtisaslaşdırılmış Auditləri (təşkilatın təqdim etdiyi xidmətlərin qiymətləndirilməsi) əhatə edən geniş termindir. üçüncü tərəf, məsələn, autsorsinq və s.) və Məhkəmə Auditləri.

Bununla belə, ümumi amil, yoxlanılan təşkilatda İT sistemlərinə etibar etmə dərəcəsi ilə bağlı rəyin formalaşmasıdır. Hazırlanmaqda olan İnformasiya Texnologiyaları Sistemlərinin auditləri və İT ilə bağlı də bu geniş Qruplaşmaya aiddir.

**İT Auditinin Məqsədləri**

İT auditinin məqsədlərinə (a) aşağıdakı beş aktiv növü daxil olan aktivlərin qorunmasını təmin edən proseslərin dəyərləndirilməsi və qiymətləndirilməsi daxildir:

• **Məlumat**

Geniş mənada verilənlər obyektləri, yəni xarici və daxili, strukturlaşdırılmış və strukturlaşdırılmamış, qrafika, səs, sistem sənədləri və s.

• **Tətbiq sistemləri**

Tətbiq sistemi əl ilə və proqramlaşdırılmış prosedurların cəmi kimi başa düşülür.

• **Texnologiya**

Texnologiya hardware, əməliyyat sistemləri, verilənlər bazası idarəetmə sistemləri, şəbəkə, multimedia və s.

• **Obyektlər**

Məlumat sistemləri, təchizat və s. yerləşdirmək və dəstəkləmək üçün resurslar.

• **İnsanlar**

İnformasiya sistemləri və xidmətlərini planlaşdırmaq, təşkil etmək, əldə etmək, çatdırmaq, dəstəkləmək və nəzarət etmək üçün personalın bacarıqları, məlumatlılığı və məhsuldarlığı.

(b) Aşağıdakı yeddi atribut isə məlumat və ya məlumat xüsusiyyətlərinin saxlanmasını təmin edir.

• **Effektivlik** - məlumatın biznes prosesinə uyğun olması ilə bərarbər həmçinin vaxtında, düzgün, ardıcıl və istifadəyə yararlı şəkildə çatdırılması ilə məşğul olur. Sistemin effektivliyi ilə məşğul olur – İT sisteminin yuxarı rəhbərliyin və istifadəçilərin ümumi məqsədlərinə cavab verib-vermədiyini qiymətləndirir.

• **Səmərəlilik** - resurslardan optimal (ən məhsuldar və qənaətcil) istifadə etməklə informasiyanın təmin edilməsinə aiddir. Sistemin səmərəliliyi ilə məşğul olur - səmərəli sistemlər tələb olunan məqsədlərə çatmaq üçün optimal resurslardan istifadə edir

• **Məxfilik** - məxfi məlumatın icazəsiz açıqlamadan qorunmasına aiddir.

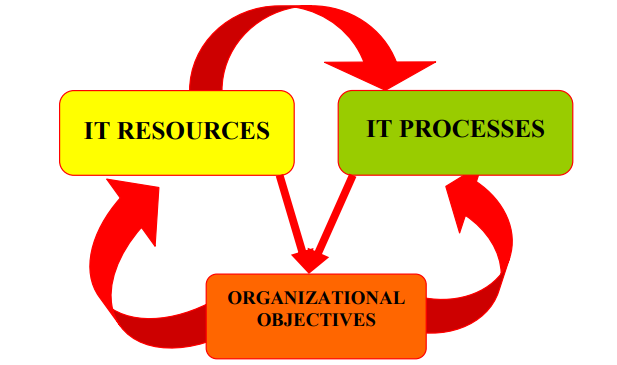
• **Bütövlük** - məlumatın düzgünlüyünə və tamlığına, eləcə də biznesin dəyərlərinə və gözləntilərinə uyğun olaraq etibarlılığına aiddir.

• **Əlyetənlilik** - biznes prosesi tələb etdikdə məlumatın mövcud olması ilə əlaqədardır və bu səbəbdən də resursların qorunmasına aiddir.

• **Uyğunluq** - biznes prosesinin tabe olduğu qanunlara, qaydalara və müqavilə razılaşmalarına riayət edilməsi ilə məşğul olur; yəni xaricdən qoyulan biznes meyarları. Bu o deməkdir ki, sistemlər təşkilatın qaydaları, qaydaları və/yaxud şərtləri çərçivəsində fəaliyyət göstərməlidir. Məsələn, təqdim ediləcək FIR(Flight information region - UÇUŞ MƏLUMATI BÖLGƏSİ) adətən qaydalara uyğun olaraq şikayətçinin imzasını tələb edir və veb əsaslı şikayətlərə icazə vermək üçün qaydaları dəyişdirərək yenidən dizayn edilməlidir. Eynilə, bank əməliyyatları bank qaydalarına və qanunvericiliyə uyğun olmalıdır.

• **İnformasiyanın etibarlılığı** - müəssisənin fəaliyyətində, maliyyə məlumatlarının istifadəçilərinə maliyyə hesabatlarının təqdim edilməsində və qanunlara və qaydalara əməl olunması ilə bağlı tənzimləyici orqanlara hesabat vermək üçün məlumatların verilməsində istifadə edilməsi üçün rəhbərliyi müvafiq məlumatlarla təmin edən sistemlərə aiddir.

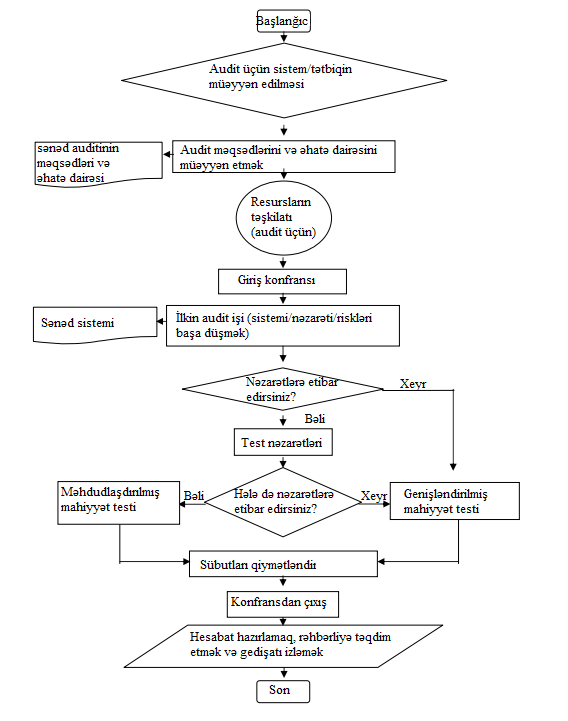
Beləliklə, İT Auditi, mövcud qaydalara riayət etməklə, əməliyyatların Effektivliyi, Səmərəliliyi və İqtisadiyyatı təmin etmək üçün təşkilatın nəzərdə tutulan məqsədlərinə çatmaq üçün İT prosesləri və İT Resurslarının bir araya gəlib-gəlmədiyini yoxlamaqdan ibarətdir. Bunu diaqrammatik olaraq aşağıdakı kimi təsvir etmək olar(Şəkil1):



Şəkil1.

**İT AUDİTİNİN ADDIMLARI**

**İT Audit Proseslərinin Diaqramı**

****

**İT audit prosesi mütləq aşağıdakı addımları əhatə etməlidir**

*• Planlaşdırma*

*• Auditin məqsədləri və əhatə dairəsinin müəyyən edilməsi*

*• Nəzarət vasitələrinin qiymətləndirilməsi*

*• Sübutların toplanması*

*• Sübutların qiymətləndirilməsi*

*• Hesabat vermək və təqib etmək*

**Planlaşdırma**

• Auditor auditi yüksək keyfiyyətli auditin iqtisadi, səmərəli və məhsuldar şəkildə və vaxtında aparılmasını təmin edən şəkildə planlaşdırmalıdır.

• Hər bir səviyyədə və audit mərhələsində audit heyətinin işinə audit zamanı lazımi qaydada nəzarət edilməli və audit heyətinin yüksək vəzifəli üzvü sənədləşdirilmiş işi nəzərdən keçirməlidir.

• Auditor auditin həcmini və əhatə dairəsini müəyyən edərkən daxili nəzarətin etibarlılığını öyrənməli və qiymətləndirməlidir.

Hər hansı bir auditin bəlkə də ən vacib fəaliyyəti planlaşdırmadır. Planlaşdırmaya nə qədər diqqət yetirilsə, audit bir o qədər dəqiq və effektiv olacaqdır. Planlaşdırma üç səviyyədə həyata keçirilir:

* Strateji planlaşdırma
* Makro planlaşdırma
* Mikro planlaşdırma

*Strateji Planlaşdırma* - Bu, bütün yoxlanılan şəxslərin İT sistemlərinin auditinin məqsəd və vəzifələrinin baş Auditor tərəfindən təxminən 3-5 il müddətinə müəyyən edildiyi uzunmüddətli planlaşdırmadır. Bu plan bütün yoxlanılan təşkilatları əhatə etməli və aşağıdakı kimi məsələləri həll etməlidir:

• auditin məqsədləri və uzunmüddətli məqsədləri;

• Dəyişikliyə cavab vermək üçün audit üsulları və üsullarının yenidən istiqamətləndirilməsinə qoyulan tələblər;

• insan və infrastruktur tələbləri

• təlim ehtiyacları

*Makro Planlaşdırma* - Bu, orta müddətli plandır və uzunmüddətli planı növbəti il üçün iş proqramına çevirir (“illik audit planımıza” ekvivalenti). Burada planlaşdırma sahə ofislərində mövcud olan resursları nəzərə alaraq il ərzində həyata keçiriləcək əsas auditlərin hər birinin məqsəd və vəzifələrini müəyyən edir.

*Mikro Planlaşdırma* - Bu, hər bir fərdi audit üçün əməliyyat planıdır və vaxt cədvəli ilə birlikdə hər bir audit üçün yerinə yetiriləcək tapşırıqların təfərrüatlarını təsvir edir. Bu mərhələdə texniki və logistika detalları həll edilməlidir.

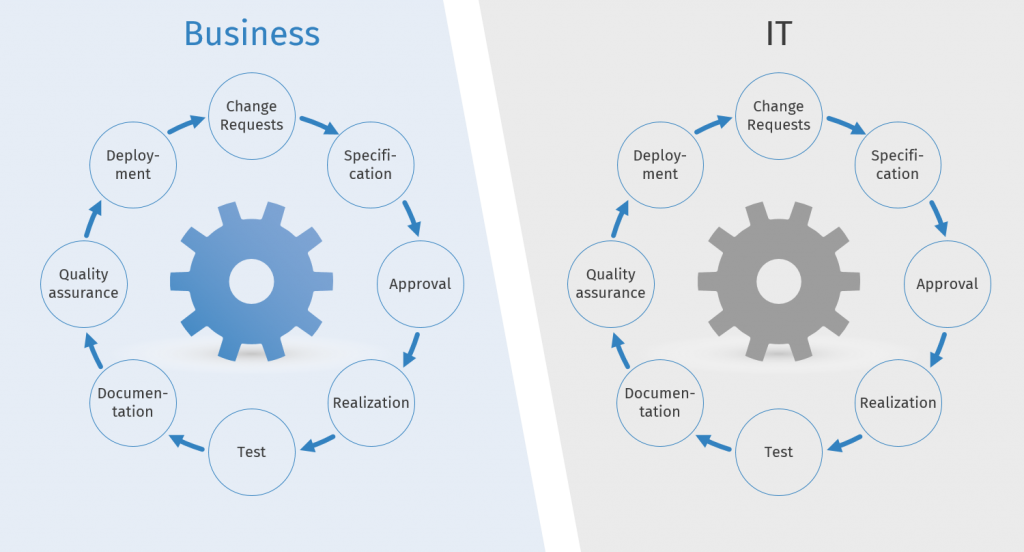
Makro və mikro planlar statik və ya sabit ola bilməz. Audit obyektinin fəaliyyət göstərdiyi mühitdəki dəyişikliklərə, eləcə də risk qavrayışındakı dəyişikliklərə uyğun düzəlişlər etmək üçün onlara vaxtaşırı yenidən baxılmalıdır.

**İT Auditinin planlaşdırılmasının təstiq edilmiş prosedurları**

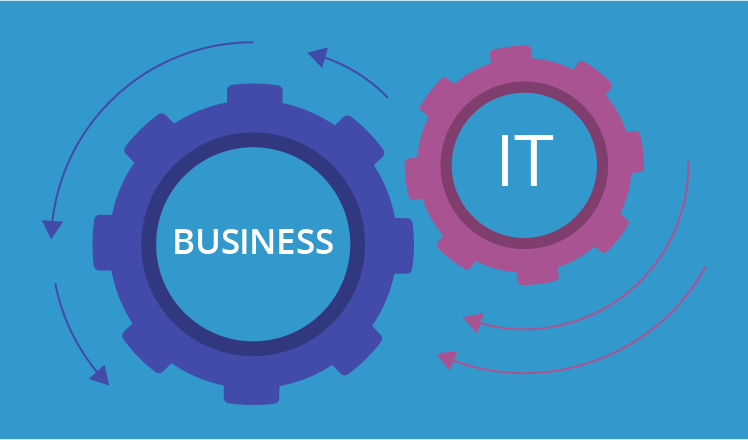
Nəzarətçi və Baş Auditor İT Auditlərinin planlaşdırılması, monitorinqi, işlənməsi və təsdiqi üçün aşağıdakı proseduru təsdiq etmişdir:

1. İT Auditlərinin Planlaşdırılması - İT Auditləri üçün mövzuların seçimi lokal ofislər və Funksional qollarla məsləhətləşmələr əsasında İT Auditi tərəfindən həyata keçiriləcək.

2. Monitorinq - Pilot tədqiqatların qiymətləndirilməsi, təlimatların yekunlaşdırılması, seminarların keçirilməsi, ortamüddətli qiymətləndirmələr və s. İT Auditi tərəfindən həyata keçiriləcək. Müvafiq funksional qollar inkişaflardan xəbərdar olacaqlar.



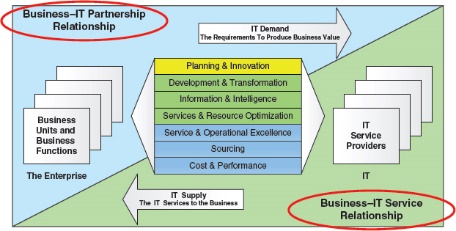
**II Hissə**

****

İnformasiya texnologiyaları (İT) müasir müəssisələrdə səmərəli fəaliyyət göstərməyə, əsaslandırılmış qərarlar qəbul etməyə və rəqabətə davamlı olmağa imkan verməklə həlledici rol oynayır. İT və biznes arasında kəsişmənin bəzi əsas aspektləri bunlardır:

1. Rəqəmsal Transformasiya (Digital Transformation): Bir çox müəssisələr əməliyyatları sadələşdirmək, müştəri təcrübələrini artırmaq və innovasiyaları təşviq etmək üçün müasir İT alətləri və texnologiyalarının qəbulunu nəzərdə tutan rəqəmsal transformasiyadan keçir.
2. Məlumatların idarə edilməsi (Data Management): İT sistemləri böyük həcmdə məlumatların toplanması, saxlanması və təhlili üçün istifadə olunur. Bu məlumatlar bizneslərə dataya əsaslanan qərarlar qəbul etmək və strategiyalarını təkmilləşdirmək üçün dəyərli fikirlər verə bilər.
3. Kibertəhlükəsizlik (Cybersecurity): Rəqəmsal texnologiyadan asılılığın artması ilə kibertəhlükəsizlik əsas narahatlıq doğurur. Müəssisələr öz məlumatlarını və sistemlərini ciddi maliyyə və reputasiya nəticələrinə səbəb ola biləcək kiber təhlükələrdən qorumalıdırlar.
4. Bulud Hesablama (Cloud Computing): Bulud xidmətləri biznesləri genişləndirilə bilən və sərfəli İT infrastrukturu və proqram təminatı həlləri ilə təmin edir. Bulud hesablamaları şirkətlərə kapital xərclərini azaltmağa və dəyişən biznes ehtiyaclarına daha asan uyğunlaşmağa imkan verir.
5. Müəssisə Resurslarının Planlaşdırılması (Enterprise Resource Planning - ERP): ERP sistemləri müxtəlif biznes prosesləri və funksiyaları vahid sistemə inteqrasiya edərək resursları, maliyyə və əməliyyatları idarə etməyi asanlaşdırır.
6. Elektron ticarət (E-Commerce): İT müəssisələrin onlayn əməliyyatlar aparma və müştərilərlə qarşılıqlı əlaqədə inqilab etdi. Elektron ticarət platformaları şirkətlərə qlobal müştəri bazasına çatmağa və 24/7 fəaliyyət göstərməyə imkan verir.
7. Business Intelligence (BI): BI alətləri və texnologiyaları bizneslərə məlumatlı qərarlar qəbul etmək üçün məlumatları təhlil etməyə kömək edir. Onlar hesabatlar yarada, idarə panelləri yarada və proqnozlaşdırıcı analitika həyata keçirə bilərlər.
8. Süni İntellekt (AI) və Maşın Öyrənmə (ML): Bu texnologiyalar biznesdə müştəri xidməti chatbotları, proqnozlaşdırıcı texniki xidmət və fərdiləşdirilmiş marketinq kimi vəzifələr üçün getdikcə daha çox istifadə olunur.
9. İT İdarəçiliyi (IT Governance): İT investisiyalarının biznes məqsədlərinə uyğun olmasını, riskləri idarə etməsini və qaydalara uyğunluğunu təmin etmək üçün bizneslərin effektiv İT idarəetmə strategiyalarına ehtiyacı var.
10. İT Strategiyası (IT Strategy): Ümumi biznes məqsədlərinə uyğun gələn İT strategiyasının hazırlanması çox vacibdir. Bu strategiya texnologiyanın qəbulu, resursların bölüşdürülməsi və davamlı texniki xidmət planlarını əhatə etməlidir.
11. İT Dəstəyi (IT Support): İT departamentləri və ya İT xidmət təminatçıları texnoloji infrastrukturun saxlanmasında və nasazlıqların aradan qaldırılmasında mühüm rol oynayır, onun operativ və səmərəli qalmasını təmin edirlər.
12. Biznes Davamlılığı və Fəlakətin Bərpası (Business Continuity and Disaster Recovery - BCDR): Müəssisələrin İT nasazlıqları və ya fəlakətlər halında fəaliyyətlərini davam etdirmələrini təmin etmək üçün planları olmalıdır.

Bunlar İT və biznesin bir-birinə qarışdığı yollardan yalnız bəziləridir. Biznes daxilində İT-nin uğurlu inteqrasiyası və idarə olunması onun rəqabət qabiliyyətinə, səmərəliliyinə və ümumi uğuruna əhəmiyyətli dərəcədə təsir göstərə bilər. Xüsusi suallarınız varsa və ya bu mövzulardan hər hansı birinə dair daha ətraflı məlumat lazımdırsa, lütfən soruşmaqdan çekinmeyin.



1. **Rəqəmsal Transformasiya (Digital Transformation)**

Rəqəmsal transformasiya bizneslərin rəqəmsal dövrün inkişaf edən ehtiyaclarını qarşılamaq üçün əməliyyatlarında, mədəniyyətində və müştəri təcrübələrində əsaslı dəyişikliklər etmək üçün rəqəmsal texnologiyalardan istifadə etdiyi strateji prosesdir. Söhbət təkcə yeni texnologiyaların tətbiqi ilə bağlı deyil, həm də sürətlə dəyişən rəqəmsal mənzərədə biznesin necə aparıldığını yenidən düşünməkdən gedir. Rəqəmsal transformasiyanın bəzi əsas aspektləri bunlardır:

Texnoloji Qəbul (Technological Adoption): Bulud hesablamaları, böyük verilənlərin analitikası, süni intellekt (AI), Əşyaların İnterneti (IoT) və avtomatlaşdırma kimi inkişaf etməkdə olan texnologiyaların tətbiqi rəqəmsal transformasiyanın əsasını təşkil edir. Bu texnologiyalar biznesə prosesləri təkmilləşdirməyə, anlayışlar əldə etməyə və innovativ məhsul və xidmətlər yaratmağa imkan verir.

Müştəri mərkəzli yanaşma (Customer-Centric Approach): Rəqəmsal transformasiya çox vaxt müştəri təcrübələrinin yaxşılaşdırılmasına diqqət yetirməklə başlayır. Müəssisələr müştərilərlə əlaqə saxlamaq, fərdiləşdirilmiş xidmətlər təklif etmək və qüsursuz onlayn qarşılıqlı əlaqə yaratmaq üçün rəqəmsal kanallardan istifadə edirlər.

Məlumata əsaslanan qərarların qəbulu (Data-Driven Decision-Making): Məlumat rəqəmsal dövrdə qiymətli varlıqdır. Təşkilatlar məlumat toplamaq, əsaslandırılmış qərarlar qəbul etmək və rəqabət üstünlüyü əldə etmək üçün məlumat analitikası və biznes kəşfiyyatı alətlərindən istifadə edirlər.

Çevik və Əməkdaşlıq Mədəniyyəti (Agile and Collaborative Culture): Rəqəmsal transformasiya təşkilat mədəniyyətində dəyişiklik tələb edir. Şirkətlər tez-tez çevik metodologiyalara doğru irəliləyir və daha sürətli qərar qəbul etməyi və dəyişikliklərə uyğunlaşmağı asanlaşdırmaq üçün komandalar arasında əməkdaşlığı təşviq edirlər.

Proseslərin optimallaşdırılması (Process Optimization): Rəqəmsal transformasiya səmərəliliyi artırmaq və xərcləri azaltmaq üçün daxili proseslərin yenidən qiymətləndirilməsini və optimallaşdırılmasını nəzərdə tutur. Avtomatlaşdırma və iş axınının idarə edilməsi vasitələri bu aspektdə mühüm rol oynayır.

İnnovasiya (Innovation): Rəqəmsal transformasiyanın tətbiqi innovasiya mədəniyyətini inkişaf etdirir. Şirkətlər davamlı olaraq yeni məhsullar, xidmətlər və ya biznes modelləri vasitəsilə müştərilərə dəyər təqdim etməyin yeni yollarını araşdırırlar.

Təhlükəsizlik və Uyğunluq (Security and Compliance): Rəqəmsal əməliyyatlar genişləndikcə təhlükəsizlik ən vacib məsələyə çevrilir. Müəssisələr güclü kibertəhlükəsizlik tədbirlərinə sərmayə qoymalı və məlumatların qorunması qaydalarına uyğunluğu təmin etməlidirlər.

Ekosistem Tərəfdaşlıqları (Ecosystem Partnerships): Rəqəmsal ekosistemdə texnologiya tərəfdaşları, startaplar və digər təşkilatlarla əməkdaşlıq rəqəmsal transformasiya səylərini sürətləndirə bilər. Bu əməkdaşlıqlar təcrübə və resurslara çıxışı təmin edə bilər.

Dəyişikliklərin İdarə Edilməsi (Change Management): İşçilər yeni texnologiyalara və proseslərə uyğunlaşdıqca dəyişikliyin idarə edilməsi vacibdir. Effektiv dəyişikliklərin idarə edilməsi strategiyaları hamar bir keçid təmin etməyə kömək edir.

Müvəffəqiyyətin ölçülməsi (Measuring Success): Əsas performans göstəricilərinin (KPI) müəyyən edilməsi və mütəmadi olaraq tərəqqinin ölçülməsi rəqəmsal transformasiya təşəbbüslərinin uğurunu izləmək üçün çox vacibdir.

Rəqəmsal transformasiya birdəfəlik layihə deyil, davamlı bir səyahətdir. Bu, yüksək rəhbərlikdən öhdəlik, aydın baxış və inkişaf edən rəqəmsal mənzərəyə uyğunlaşmaq istəyi tələb edir. Uğurlu rəqəmsal transformasiya rəqabət qabiliyyətinin artması, müştəri məmnuniyyətinin artması, əməliyyat səmərəliliyi və rəqəmsal iqtisadiyyatda yaranan imkanlardan istifadə etmək bacarığı ilə nəticələnə bilər.

1. **Məlumatların idarə edilməsi (Data Management)**

Məlumatların idarə edilməsi təşkilatlara onlardan səmərəli istifadə etməyə və ondan dəyər əldə etməyə imkan verən şəkildə məlumatların toplanması, saxlanması, təşkili və saxlanması təcrübəsidir. Bugünkü dataya əsaslanan dünyada məlumatların effektiv idarə edilməsi bizneslərin əsaslandırılmış qərarlar qəbul etməsi, əməliyyatları təkmilləşdirməsi və rəqabətədavamlı qalması üçün çox vacibdir. Məlumatların idarə edilməsinin əsas aspektləri bunlardır:

Məlumatların toplanması (Data Collection): Bu, həm daxili (məsələn, əməliyyat məlumat bazaları, sensorlar, işçilər tərəfindən yaradılan məlumatlar) və həm də xarici (məsələn, müştəri rəyi, bazar araşdırması, sosial media) müxtəlif mənbələrdən məlumatların toplanması prosesini əhatə edir. Məlumat strukturlaşdırılmış (verilənlər bazasında) və ya strukturlaşdırılmamış (mətn sənədləri və şəkillər kimi) ola bilər.

Məlumatların saxlanması (Data Storage): Toplandıqdan sonra məlumat təhlükəsiz və səmərəli şəkildə saxlanmalıdır. Bu, ənənəvi əlaqəli verilənlər bazalarını, NoSQL verilənlər bazalarını, məlumat anbarlarını, məlumat göllərini və ya bulud əsaslı saxlama həllərini əhatə edə bilər. Seçim məlumatların növündən və təşkilatın ehtiyaclarından asılıdır.

Data Keyfiyyəti (Data Quality): Məlumatların dəqiqliyini, ardıcıllığını və etibarlılığını təmin etmək çox vacibdir. Məlumatların keyfiyyətinin idarə edilməsi səhvləri və uyğunsuzluqları aradan qaldırmaq üçün məlumatların təmizlənməsi, təsdiqlənməsi və zənginləşdirilməsi proseslərini əhatə edir.

Məlumatların idarə edilməsi (Data Governance): Məlumatların idarə edilməsi təşkilat daxilində məlumatların idarə edilməsi üçün siyasətlər, standartlar və prosedurlar müəyyən edir. O, məlumatların bütövlüyünü və qaydalara uyğunluğunu qorumaq üçün rol və məsuliyyətləri, giriş nəzarətlərini və məlumat sahibliyini müəyyən edir.

Məlumatların inteqrasiyası (Data Integration): Bir çox təşkilatlarda müxtəlif siloslarda və formatlarda saxlanılan məlumatlar var. Məlumatların inteqrasiyası ayrı-ayrı mənbələrdən alınan məlumatların təhlil və hesabat üçün vahid və ardıcıl formata birləşdirilməsini və çevrilməsini nəzərdə tutur.

Məlumat Təhlükəsizliyi (Data Security): Həssas məlumatların qorunması çox vacibdir. Şifrələmə, giriş nəzarəti və audit daxil olmaqla möhkəm təhlükəsizlik tədbirləri məlumatların pozulmasının və icazəsiz girişin qarşısını almaq üçün vacibdir.

Məlumatların Yedəklənməsi və Bərpası (Data Backup and Recovery): Məlumatların itirilməsi ciddi nəticələrə səbəb ola bilər. Daimi məlumatların ehtiyat nüsxəsi və bərpa planları məlumatların təsadüfən silinməsi, avadanlıqların nasazlığı və ya digər fəlakətlər halında bərpa edilməsini təmin edir.

Master Data Management (MDM): MDM təşkilat daxilində əsas biznes məlumatlarının (məsələn, müştəri məlumatları, məhsul məlumatları) vahid, ardıcıl və dəqiq versiyasını yaratmağa və idarə etməyə diqqət yetirir.

Məlumat Məxfiliyi və Uyğunluq (Data Privacy and Compliance): Təşkilatlar GDPR (Ümumi Məlumatların Qorunması Qaydası) və ya HIPAA (Sağlamlıq Sığortasının Daşınması və Hesabatlılığı Aktı) kimi məlumatların mühafizəsi qaydalarına əməl etməlidirlər. Uyğunluğa razılığın alınması, məlumatların anonimləşdirilməsi və pozuntuların bildirilməsi daxildir.

Data Analitika (Data Analytics): Məlumatların idarə edilməsi məlumat analitikası səylərini dəstəkləyir. Məlumat alimləri və analitikləri anlayışlar əldə etmək, proqnozlaşdırıcı modellər qurmaq və məlumatlara əsaslanan qərarlar qəbul etmək üçün təmiz və yaxşı təşkil edilmiş məlumatlardan istifadə edirlər.

Məlumat həyat dövrünün idarəedilmədi (Data Lifecycle Management): Bu, verilənlərin yaradılmasından son təqaüdə çıxmasına qədər idarə edilməsini əhatə edir. Bura arxivləşdirmə, saxlama siyasətləri və uyğun şəkildə məlumatların utilizasiyası daxildir.

Ölçeklenebilirlik və Performans (Scalability and Performance): Məlumatların idarə edilməsi həlləri artan məlumat həcmlərinə uyğunlaşmaq üçün miqyaslana bilən olmalıdır və analitik və əməliyyat ehtiyacları üçün məlumatlara yüksək performanslı girişi təmin etməlidir.

Effektiv məlumatların idarə edilməsi müxtəlif şöbələr arasında əməkdaşlığı və ən yaxşı təcrübələrə riayət etməyi tələb edən davamlı bir prosesdir. O, təşkilatlara öz məlumatlarını qiymətli aktiv kimi istifadə etməyə, fikirlər əldə etməyə, qərar qəbul etməyi təkmilləşdirməyə və sürətlə dəyişən biznes mühitində çevik qalmağa imkan verir.

1. **Kibertəhlükəsizlik (Cybersecurity)**

Kibertəhlükəsizlik kompüter sistemlərinin, şəbəkələrinin, cihazların və məlumatların oğurluqdan, zədələnmədən, icazəsiz girişdən və digər kiber təhdid və hücumlardan qorunması təcrübəsinə aiddir. Bizneslər və fərdlər getdikcə rəqəmsal texnologiyalara və internetə etibar etdikcə, kibertəhlükəsizlik həssas məlumatların qorunması və rəqəmsal əməliyyatların bütövlüyünün qorunması üçün vacib hala gəldi. Kibertəhlükəsizliyin bəzi əsas aspektləri bunlardır:

Kibertəhlükələrin növləri: Kibertəhlükəsizlik müxtəlif növ təhdidlərə, o cümlədən:

Zərərli proqram (Malware): Viruslar, ransomware və casus proqramlar kimi zərərli proqram.

Fişinq (Phishing): Giriş etimadnamələri və ya maliyyə detalları kimi həssas məlumatları üzə çıxarmaq üçün şəxsləri aldatmaq cəhdləri.

Xidmətdən imtina (Denial of Service - DoS) və Paylanmış Xidmətdən imtina (Distributed Denial of Service - DDoS) Hücumları: Hədəf sistemi və ya şəbəkəni onun normal fəaliyyətini pozmaq üçün sıxışdırmaq.

Məlumatların pozulması (Data Breaches): Həssas məlumatlara icazəsiz giriş və oğurluq.

Sosial Mühəndislik (Social Engineering): Məxfi məlumatları aşkar etmək və ya təhlükəsizliyi pozan hərəkətlər etmək üçün fərdləri manipulyasiya etmək.

Daxili Təhdidlər (Insider Threats): Təşkilat daxilində həssas məlumatlara çıxışı olan işçilər və ya şəxslər tərəfindən yaranan təhlükəsizlik riskləri.

Sıfır Gün Zəiflikləri (Zero-Day Vulnerabilities): Proqram təminatı zəifliklərinin tərtibatçılar tərəfindən düzəldilməzdən əvvəl istismar edilməsi.

Kibertəhlükəsizlik tədbirləri (Cybersecurity Measures): Kibertəhlükələrdən qorunmaq üçün təşkilatlar və şəxslər bir sıra təhlükəsizlik tədbirləri tətbiq edirlər, o cümlədən:

Firewalllar: İcazəsiz girişin qarşısını almaq üçün daxil olan və gedən trafiki filtrləyən şəbəkə təhlükəsizlik cihazları.

Antivirus və Zərərli Proqram Təminatı: Zərərli proqram təminatını aşkarlayan və aradan qaldıran proqramlar.

Şifrələmə (Encryption): Verilənləri yalnız müvafiq açarla deşifrə edilə bilən koda çevirməklə təhlükəsizliyin təmin edilməsi.

Çox faktorlu Doğrulama (Multi-factor Authentication - MFA): Hesaba və ya sistemə daxil olmaq üçün bir çox autentifikasiya üsulları (məsələn, parol və barmaq izi) tələb olunur.

Müntəzəm Proqram Yeniləmələri (Regular Software Updates): Məlum zəiflikləri düzəltmək üçün təhlükəsizlik yamaqlarının və yeniləmələrinin tətbiqi.

İşçilərin Təlimi (Employee Training): İşçilərə kibertəhlükəsizlik üzrə ən yaxşı təcrübələr və təhdidləri necə tanımaq və onlara cavab vermək barədə məlumatlandırmaq.

Təhlükəsizlik Siyasətləri və Uyğunluq (Security Policies and Compliance): Təşkilatlar təhlükəsizlik tədbirlərinin ardıcıl şəkildə tətbiq olunmasını təmin etmək üçün tez-tez kibertəhlükəsizlik siyasətləri və təcrübələri yaradırlar. Sənayeyə məxsus qaydalara və məlumatların qorunması qanunlarına (məsələn, GDPR və ya HIPAA) uyğunluq vacibdir.

Hadisəyə Cavab (Incident Response): Təhlükəsizlik insidentlərinin təsirini aşkar etmək, saxlamaq və azaltmaq üçün planın olması çox vacibdir. Bu, pozuntunun mənbəyinin müəyyən edilməsi, təsirə məruz qalan tərəflərin məlumatlandırılması və gələcək hadisələrin qarşısının alınması daxildir.

Təhlükəsizlik məlumatlılığı (Security Awareness): Kibertəhlükəsizlik şüurunun və təşkilat daxilində təhlükəsizlik mədəniyyətinin təşviqi həyati əhəmiyyət kəsb edir. İşçilər riskləri və təhlükəsizliyin qorunmasında onların rolunu başa düşməlidirlər.

Təhlükəsizlik Texnologiyaları (Security Technologies): Kibertəhlükəsizlik həlləri, müdaxilənin aşkarlanması sistemləri (intrusion detection systems - IDS), müdaxilənin qarşısının alınması sistemləri (intrusion prevention systems - IPS), Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi (Security Information and Event Management - SIEM) alətləri və s. daxil olmaqla, geniş texnologiyaları əhatə edir.

Üçüncü tərəf Risk İdarəetmə (Third-party Risk Management): Bir çox təşkilat üçüncü tərəf satıcılarına və xidmət təminatçılarına etibar edir. Bu əlaqələrlə bağlı kibertəhlükəsizlik risklərini qiymətləndirmək və idarə etmək vacibdir.

IoT və Cloud-da kibertəhlükəsizlik: Əşyaların İnterneti (IoT) cihazlarından və bulud hesablamalarından istifadə artdıqca, onların təhlükəsizliyinin təmin edilməsi kritik məsələyə çevrilir. IoT cihazlarında və ya bulud xidmətlərindəki zəifliklər təcavüzkarlar tərəfindən istifadə edilə bilər.

Kibertəhlükəsizlik davam edən və inkişaf edən bir sahədir, çünki kibertəhlükələr daim uyğunlaşır və daha təkmilləşir. Effektiv kibertəhlükəsizlik proaktiv yanaşma, müntəzəm qiymətləndirmələr və yaranan təhdidlər və təhlükəsizlik texnologiyaları ilə yenilənmək öhdəliyi tələb edir.

1. **Bulud Hesablama (Cloud Computing)**

Bulud hesablama daha sürətli innovasiya, çevik resurslar və miqyasda qənaət təklif etmək üçün serverlər, yaddaş, verilənlər bazası, şəbəkə, proqram təminatı, analitika və s. kimi hesablama xidmətlərinin internet (“bulud”) üzərindən çatdırılmasını əhatə edən texnologiya paradiqmasıdır. Fiziki məlumat mərkəzləri və serverlərə sahib olmaq və onlara qulluq etmək əvəzinə, təşkilatlar bulud resurslarına daxil ola və istifadə edə bilər, lazım olduqda onları böyüdə və ya azalda bilər. Bulud hesablamasının bəzi əsas aspektləri bunlardır:

Xidmət Modelləri - Service Models:

Xidmət olaraq İnfrastruktur (Infrastructure as a Service - IaaS): Virtual maşınlar, yaddaş və şəbəkə daxil olmaqla internet üzərindən virtuallaşdırılmış hesablama resurslarını təmin edir. İstifadəçilər əməliyyat sistemini, proqramları və məlumatları idarə edirlər.

Xidmət olaraq Platforma (Platform as a Service - PaaS): Tərtibatçılara infrastrukturun idarə edilməsindən narahat olmadan proqramlar qurmaq, yerləşdirmək və idarə etmək üçün platforma və mühit təklif edir. PaaS provayderləri əsas infrastrukturu idarə edirlər.

Xidmət kimi proqram (Software as a Service - SaaS): Proqram təminatı proqramlarını internet üzərindən abunə əsasında təqdim edir. İstifadəçilər proqram təminatına veb-brauzerlər vasitəsilə daxil olurlar və provayder proqramın bütün aspektlərini, o cümlədən yeniləmələri və texniki xidməti idarə edir.

Yerləşdirmə Modelləri - Deployment Models:

İctimai Bulud - Public Cloud: Xidmətlər üçüncü tərəf bulud provayderləri tərəfindən təmin edilir və resurslar çoxsaylı müştərilər arasında paylaşılır. O, sərfəli miqyaslılıq təklif edir, lakin təhlükəsizlik və uyğunluq problemlərini artıra bilər.

Şəxsi Bulud - Private Cloud: Resurslar tək bir təşkilata həsr olunub və onlar yerli və ya üçüncü tərəf provayderi tərəfindən yerləşdirilə bilər. Şəxsi buludlar daha çox nəzarət, təhlükəsizlik və fərdiləşdirmə təklif edir, lakin daha yüksək ilkin xərclərə malik ola bilər.

Hibrid Bulud - Hybrid Cloud: İctimai və özəl bulud resurslarını birləşdirir, verilənlərin və tətbiqlərin onlar arasında hərəkət etməsinə imkan verir. Mövcud infrastrukturun çevikliyini və optimallaşdırılmasını təmin edir.

Bulud Hesablamanın Faydaları:

Xərc Effektivliyi (Cost Efficiency): Təşkilatlar yalnız istifadə etdikləri resurslara görə ödəməklə, aparat və texniki xidmət üçün kapital xərclərini azalda bilər.

Ölçeklenebilirlik (Scalability): Optimal performans və xərclərə nəzarəti təmin edərək dəyişən tələbləri ödəmək üçün bulud resursları asanlıqla böyüdülə və ya azaldıla bilər.

Çeviklik (Flexibility): İstifadəçilər uzaqdan işləməyi və işin davamlılığını təşviq edərək internet bağlantısı olan hər yerdən bulud xidmətlərinə daxil ola bilərlər.

Sürət və çeviklik (Speed and Agility): Resursların sürətli təmin edilməsi və avtomatlaşdırılmış idarəetmə proqramların daha sürətli inkişafına və yerləşdirilməsinə imkan verir.

Etibarlılıq və ehtiyat (Reliability and Redundancy): Bulud provayderləri məlumatların həmişə əlçatan olmasını təmin etmək üçün tez-tez yüksək əlçatanlıq və məlumat ehtiyatı təklif edirlər.

Təhlükəsizlik (Security): Bulud provayderləri təhlükəsizlik tədbirlərinə və uyğunluğa böyük sərmayə qoyurlar, çox vaxt ayrı-ayrı təşkilatların təkbaşına əldə edə biləcəyini üstələyir.

Problemlər və Mülahizələr - Challenges and Considerations:

Təhlükəsizlik və Uyğunluq (Security and Compliance): Məlumatların qorunması və qaydalara uyğunluğun təmin edilməsi bulud provayderi ilə müştəri arasında paylaşılan məsuliyyətdir.

Məlumatların ötürülməsi və bant genişliyi xərcləri (Data Transfer and Bandwidth Costs): Böyük həcmli məlumatların buluddan və buluddan köçürülməsi əlavə xərclərə səbəb ola bilər və kifayət qədər bant genişliyi tələb edə bilər.

Satıcı Kilidi (Vendor Lock-In): Tətbiqlərin və məlumatların bir bulud provayderinin mühitindən digərinə köçürülməsi mürəkkəb və bahalı ola bilər.

İş vaxtı və kəsintilər (Downtime and Outages): Bulud provayderləri yüksək əlçatanlığa can atsalar da, xidmətdə fasilələr yarana bilər.

Məlumatların Məxfiliyi (Data Privacy): Buludda məlumatların saxlanması, xüsusən də məlumatlar müxtəlif coğrafi bölgələrdə yerləşdirildikdə məxfiliklə bağlı narahatlıqları artıra bilər.

Bulud hesablamaları müasir İT infrastrukturunun əsas komponentinə çevrilərək, təşkilatlara sürətlə inkişaf edən texnoloji mənzərədə innovasiyalar, miqyas və rəqabət qabiliyyətini qorumağa imkan verir. Bulud xidməti modelinin və provayderin seçimi təşkilatın xüsusi ehtiyaclarından, məqsədlərindən və məhdudiyyətlərindən asılıdır.

1. **Müəssisə Resurslarının Planlaşdırılması (Enterprise Resource Planning - ERP)**

Müəssisə Resurslarının Planlaşdırılması (Enterprise Resource Planning - ERP) təşkilatların müxtəlif şöbələr arasında müxtəlif əsas biznes proseslərini və funksiyalarını idarə etmək və vahid sistemə inteqrasiya etmək üçün istifadə etdiyi hərtərəfli proqram həllidir. ERP-nin əsas məqsədi təşkilatlara məlumatlara əsaslanan qərarlar qəbul etmək, səmərəliliyi artırmaq və ümumi performansı artırmaq imkanı verən məlumat axınını asanlaşdırmaq və əməliyyatları sadələşdirməkdir. Müəssisə Resurslarının Planlaşdırılmasının əsas aspektləri bunlardır:

Modullar və Funksionallıq: ERP sistemləri adətən biznes əməliyyatlarının müxtəlif aspektlərini həll edən çoxsaylı modullardan ibarətdir. Ümumi modullara aşağıdakılar daxildir:

Maliyyə və Mühasibat Uçotu: Maliyyə əməliyyatlarını, büdcələri və maliyyə hesabatlarını idarə etmək.

İnsan Resursları (Human Resources - HR): İşçi məlumatları, əmək haqqı, müavinətlər və işçi qüvvəsinin idarə edilməsi.

Təchizat Zəncirinin İdarə Edilməsi (Supply Chain Management - SCM): Satınalma, inventar, istehsal və paylamanın idarə edilməsi.

Müştərilərlə Əlaqələrin İdarə Edilməsi (Customer Relationship Management - CRM): Müştərilərlə qarşılıqlı əlaqə, satış, marketinq və xidmətin idarə edilməsi.

İstehsal (Manufacturing): İstehsal proseslərinin optimallaşdırılması, planlaşdırma və keyfiyyətə nəzarət.

İnventar İdarəetmə (Inventory Management): İnventar səviyyələrini və ehtiyatların hərəkətini izləmək və idarə etmək.

Satış və Sifarişin İdarə Edilməsi (Sales and Order Management): Satış sifarişlərini, qiymətləri və sifarişlərin yerinə yetirilməsini idarə etmək.

Hesabat və Biznes Kəşfiyyatı (Reporting and Business Intelligence): Məlumatların təhlili, hesabat vermə və qərar qəbuluna dəstək üçün alətlərin təmin edilməsi.

İnteqrasiya (Integration): ERP sistemləri məlumat silolarını aradan qaldıraraq və kommunikasiyanı təkmilləşdirərək, məlumat və prosesləri şöbələr arasında birləşdirməyi hədəfləyir. İnteqrasiya məlumatın müxtəlif funksiyalar arasında maneəsiz şəkildə axmasını təmin edir, məlumatların əl ilə daxil edilməsini və səhvləri azaldır.

Məlumatların Mərkəzləşdirilməsi (Data Centralization): ERP məlumatları vahid verilənlər bazasında və ya məlumat anbarında mərkəzləşdirir. Bu, məlumatların ardıcıllığını və dəqiqliyini təmin edən təşkilati məlumatlar üçün vahid həqiqət mənbəyini təmin edir.

Avtomatlaşdırma (Automation): ERP sistemləri müxtəlif iş proseslərini avtomatlaşdırır, əl ilə müdaxiləyə ehtiyacı azaldır və iş axınlarını sadələşdirir. Bu, səmərəliliyin artmasına və əməliyyat xərclərinin azalmasına səbəb ola bilər.

Real-vaxt Məlumatı (Real-time Information): ERP sistemləri istifadəçilərə məlumatlı qərarları tez bir zamanda qəbul etməyə imkan verən məlumatlara real vaxt rejimində çıxışı təmin edir. Bu, inventar, satış və maliyyə məlumatlarını izləmək üçün xüsusilə dəyərlidir.

Fərdiləşdirmə (Customization): Bir çox ERP sistemləri proqram təminatını təşkilatın xüsusi ehtiyaclarına və sənaye tələblərinə uyğunlaşdırmaq üçün fərdiləşdirmə variantları təklif edir.

Ölçeklenebilirlik (Scalability): ERP sistemləri, biznes genişləndikcə artan məlumat həcmini və istifadəçi sayını nəzərə alaraq təşkilatla birlikdə böyümək üçün nəzərdə tutulmuşdur.

Təhlükəsizlik və Girişə Nəzarət (Security and Access Control): ERP sistemləri həssas məlumatları qorumaq və istifadəçilərin öz rollarına əsasən müvafiq giriş səviyyələrinə malik olmasını təmin etmək üçün möhkəm təhlükəsizlik xüsusiyyətlərini ehtiva edir.

Mobil və Bulud İmkanları (Mobile and Cloud Capabilities): Müasir ERP sistemləri tez-tez mobil girişi dəstəkləyir və buludda yerləşdirilə bilər ki, bu da istifadəçilərə internet bağlantısı olan istənilən yerdən məlumat əldə etməyə və tapşırıqları yerinə yetirməyə imkan verir.

Təlim və Dəstək (Training and Support): ERP sisteminin tətbiqi adətən işçilərin proqram təminatından səmərəli istifadə etməsi üçün təlim tələb edir. Sistemin düzgün işləməsi üçün davamlı dəstək və texniki xidmət də vacibdir.

Xərclə bağlı mülahizələr (Cost Considerations): ERP tətbiqi proqram təminatının lisenziyalaşdırılması, aparat təminatı, tətbiq xidmətləri və davamlı texniki xidmət xərcləri baxımından əhəmiyyətli investisiya ola bilər.

ROI(Return on Investment - İnvestisiya gəliri) və Biznes Faydaları (ROI and Business Benefits): Effektiv şəkildə tətbiq olunduqda, ERP sistemləri təkmilləşdirilmiş əməliyyat səmərəliliyi, daha yaxşı qərar qəbulu, xərclərin azaldılması və təkmilləşdirilmiş müştəri məmnuniyyəti də daxil olmaqla çoxsaylı faydalar verə bilər.

ERP sisteminin tətbiqi diqqətli planlaşdırma, maraqlı tərəflərin cəlb edilməsi və təşkilatın prosesləri və məqsədləri haqqında hərtərəfli başa düşülməsini tələb edən mürəkkəb bir işdir. Uğurla icra edildikdə, ERP biznes əməliyyatlarını optimallaşdırmaq və böyüməyi sürətləndirmək üçün güclü bir vasitə ola bilər.