Çalıştığımız kuruluşlar için verinin güvenliği ve yasalara uyumluluk sadece yaptığımız Teknik , güvenlik anlamındaki konfigürasyonlar yada çalışmalar değil , bunun yanında iş sürekliliği ve kurumumuzun müşterilere bizlere güvenmesi adına çalışmalar yapmak gerekmektir. Özellikle Regülasyonun ağır olduğu senaryoların çok çok ağır olduğu sektörlerde uyumluluk çok çok önemlidir ve aranan zorunlu maddelerden biridir. Banka , Finans , Sağlık , Kamu sektörlerinde bulut tarafında hizmetlerini konumlandırmak isteyen kişiler için uyumluluk bir değerlendirme kriteridir.

Cloud ortamında uyumlulukların iyi ilerletilebilmesi amacıyla bence Cloud Hizmetlerini büyük Global Bulut Servis Sağlayıcılarından seçim yapmak , tüm süreçlerin ve yapmış olduğunuz işin sektörünü tutacak verinin uyumluluğunu sağlamasını rahatlıkla kolay bulunabilir hale getirmektedir. Bugün bahsedeceğimiz konulardan biri de Microsoft Azure tarafındaki veri merkezinde yada endüstrilere sunmuş olduğu uyumluluk ve sertifikalardan bahsedeceğiz. Microsoft Azure , Globaldeki Uyumluluk ve Güvenlik yatırımlarına çok önemli veren bir Bulut Servis Sağlayıcı diyebiliriz. Bu yatırımlarla birlikte kuruluşların farklı bölgesel ve sektörel regülasyonlara uyum sağlayabilmesine büyük seviyede destek vermektedir ve önem vermektedir. ISO 270001'den GPDR'a , HIPAA'den KVKK'ya yüzlerce sertifikasyon ve standartlarla desteklenen Azure Cloud , kuruluşların uyumluluklarda ilerleme süreçlerine büyük ivme kazandırmaktadır.

İşte bu makalede bahsedeceğimiz konular; Bu Sertifikasyonlar ve Uyumluluklar Nelerdir ? Hangi endüstri üzerinde ne gibi veriler barındırılır ? Yüzlerce uyumluluklar var bunların kullanımlarından ve Use Cases'lerden yani Kulllanımlardan bahsedeceğiz.

Ama tabiki de ilk önce Compliance yani Uyumluluk nedir'den bahsedelim 😊

Bir organizasyonun yasal düzenlemelere , endüstri standartlarına ve iç politikalara uyum sağlamasını destekleyen sertifika veya kural diyebiliriz. Uyumluluğu ayrıca hizmet vermiş olduğunuz müşterilerin güvenini kazanma ve sürekliliğini sürdürme şeklinde de tanımlayabiliriz. Peki sektöre göre biraz somutlaştıralım bu kavramı ; Finansal Organizasyonlar için PCI DSS , Sağlık Sektörü için HIPAA , Avrupada GPDR , Türkiyede KVKK gibi düzenlemeler , cloud üzerinde çalışan veya çalışacak uygulamaların uyması gereken temel standartlardır.

Microsoft, Kendinden hizmet alan Organizasyonlara Sertifikasyonlara ve Regülasyonlara uygun altyapı sağlamaktadır.

Uyumlulukla alakalı bir çok bilgi öğrendik şimdi ne yapıyoruz Microsoft'un sunduğu Uluslararası ve bölgesel uyumluluk sertfikalarını inceleyelim 😊

İlk öncelik olarak bunları bir categorize edilim değil mi 😊

- Global
- US Government
- Financial Services
- Healtcare and life sciences
- Automative , education , energy , media and telecommunication , Regional Americas , Regional Asia Pacific , Regional EMEA ,

Global

- CIS Bencmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3
- ISO 20000 – 1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

CIS Bencmark ; Center of Internet Security bir sistemi güvenli bir şekilde konfigüre etmek için kullanılan yöntemdir. Bunu kullanma amacımız ; Herhangi bir sistemde konfigüre edilen sistemlerin minimum kesinti , hiç kesinti yaşanmaması için önerilerde bulunur. Organizasyonlarda Daha fazla güvenlik gerektiren durumlarda konfigürasyonlar konusunda önerilerde bulunarak , yönlendirme gerçekleştirmektedir. Bu uyumluluk konusunda başvuracağınız Microsoft Servisi ; Microsoft Purview ; Bu servis ile Compliance Manager'I kullanarak uyumluluk ve riskleri daha iyi analiz edebilirsiniz.

CSA Star Attestation ;

CSA STAR Certification

CSA STAR self-assessment ;

Cloud Security Alliance (CSA) ; Gönüllü kuruluşlar tarafından yönetilen kar amacı gütmeyen bir kuruluştur. Organizasyonların Daha güvenli Cloud ortamını kullanmasına yardımcı olmak , Buluta geçiş aşamasında organizasyonların daha çok bilinçli taşıma gerçekleştirmesini sağlamak amaçlıdır.

SOC 1 ;

Microsoft'un Azure, Dynamics 365, Power Platform ve bazı Microsoft 365 servisler için düzenli olarak bağımsız third party audit yani denetim süreçlerinden geçen SOC 1 Type 2 (Sistem ve Organizasyon Kontrolleri) raporu, finansal raporlama üzerindeki iç kontrol süreçlerinin etkinliğini değerlendiren önemli bir denetim belgesidir. Ayrıca, Finansal hizmetler sektöründe faaliyet gösteren kuruluşların aşağıdaki düzenlemelere uyum sağlamasına destek vermektedir :

- Sarbanes-Oxley Yasası (SOX)
- Federal Finansal Kurumlar Denetim Konseyi (FFIEC)
- Gramm-Leach-Bliley Yasası (GLBA)

SOC 2 and SOC 3 ;

Microsoft'un Azure, Dynamics 365, Microsoft 365 ve Power Platform servisleri için yayımlanan **SOC 2 Type 2** raporları, hizmet sağlayıcılarının güvenlik, erişilebilirlik, işlem bütünlüğü, gizlilik ve mahremiyet gibi güven hizmetleri kriterlerine uyumunu değerlendiren bağımsız denetim raporları diyebiliriz.

SOC 2 Type 2 raporları, aşağıdaki düzenlemelere uyum destek vermektedir :

- ISO/IEC 27001
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4
- Almanya C5:2020

ISO 20000 – 1

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için Bilgi Teknoloji servis yönetimi süreçlerinin etkinliğini ve güvenilirliğini doğrulamak için uluslararası bir standart diyebiliriz. Organizasyonların servis yönetim süreçlerinde standarta uyguluğunu belgelemek için , kendi uyumluluk ve sertifikasyon süreçlerinde kullanacakları standart diyebiliriz. Bu belgeyi referans olarak kullanabilirler.

ISO 22301

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için Business Continuity Management System yani İş sürekliliği yönetim sistemi gereksinimlerine uyumluluğu doğrulayan uluslararası standart diyebiliriz. Organizasyonların iş sürekliliği ve operasyonel kesintilere hazırlığını göstermektedir. **ISO 20000 – 1 gibi** servis yönetim süreçlerinde standarta uyguluğunu belgelemek için , kendi uyumluluk ve sertifikasyon süreçlerinde kullanacakları standart diyebiliriz. Bu belgeyi referans olarak kullanabilirler.

ISO 27001

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için Information Security Management System yani Bilgi Güvenliği Yönetim Sistemi ihtiyaçlarını karşılamak için kullanılan uluslararası standart diyebiliriz. Organizasyonların Bilgi Güvenliği yönetim süreçlerinin etkinliğini ve güvenilirliğini göstermektedir. Önceki bahsetmiş olduğumuz gibi organizasyonlar bu belgeyi referans olarak kullanabilirler.

ISO 27017

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için Cloud Service Provider yani Bulut Servis Sağlayıcıları ve organizasyonlar için Bilgi güvenliği kontrolleri ve uygulama konusunda rehberlik sunan uluslararası standart diyebiliriz. Organizasyonların Cloud ortamlarında shared responsible yani paylaşılan sorumluluklarını netleştirmeye yardımcı olur. Organizasyonların cloud service providerlar'dan ne gibi hizmetleri ve aksiyonları beklemeleri konusunda destek verir. Cloud ortamında barındırılan Virtual Machine'lerin ve Virtual Network'lerin güvenliğinin sağlanması gibi ek kontroller sağlamaktadır.

ISO 27018

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için Cloud Service Provider yani Bulut Servis Sağlayıcılarının kişisel verilerinin korunmasına yönelik uygulamalı rehberlik veren uluslarası standarttır.

ISO 27701

Microsoft'un Azure, Azure Government, Azure China, Dynamics 365, Microsoft 365, Power Platform servisleri için ISO / IEC 27001 ve ISO/IEC 27002 standartlarının uzantısı olarak , kişisel veri yönetimi için bir Privacy Information Management System yani Gizlilik Yönetim Sistemi ihtiyaçlarını ve rehberliği sunmaktadır. Organizasyonlara Kişisel veri yönetimi için kapsam sunmaktadır. GPDR gibi düzenlemelere uyum sağlamaktadır. Farklı düzenlemelere yönelik denetim maliyetlerini minimize etmektedir. Ticari anlaşmalar Kişisel verilerin korunmasına yönelik güvence sağlamaktadır.

ISO 9001

Microsoft'un Azure, Azure Government, Dynamics 365, Microsoft 365, Power Platform servisleri için tutarlı , yüksek kaliteli ürün ve servis sunmayı hedefleyen Quality Management System yani Kalite Yönetim Sistemi standardıdır. ISO 13485 , ISO/IEC/IEEE 90003 gibi sektöre özel kalite standartlarıyla uyum konusunda referans olarak kullanılabilir. Kendi sertifikasyon süreçlerini yürütmek isteyen organizasyonlar için idealdir.

WCAG

Microsoft'un Azure, Dynamics 365, Microsoft 365, Power BI, Office Ürünleri, Intune , Windows Server gibi ürün ve hizmetlerine yönelik erişilebilirlik değerlendirmelerini içermektedir. Web içeriğini , Engelli kullanıcılar için daha erişilebilir hale getirmeyi amaçlayan uluslarası standart diyebiliriz.

US Government

- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

CJIS (Criminal Justice Information Services)

FBI tarafından işletilen bir sistemdir. Polis veya diğer adli kurumlara suç geçmişi , parmak izi gibi hassas bilgileri onların hizmetine sağlamaktadır. Bu politika ile bahsetmiş olduğumuz verilerin bulut ortamlarında muhafaza edilmesi , iletilmesi , işlenmesi gibi işlemler sırasında uyulması gereken ihtiyaçları içermektedir. Azure ve Azure Government sistemlerinde kullanılmaktadır.

CMMC (Cybersecurity Maturity Model Certification)

ABD Savunma Bakanlığı (DoD) tarafından geliştirilmiş güvenlik çerçevesi diyebiliriz. CMMC , doğrudan Azure gibi bulut hizmetlerine yönelik bir sertifikasyon değildir. Bir savunma sanayi vb. Tedarikçi organizasyonlar tarafından kullanılan süreçlerin ve uygulamaları değerlendirmektedir.

CNSSI 1253

CNSSI yani Committee on National Security Systems Instruction No.1253) olarak geçmektedir. ABD Ulusal Güvenlik Sistemlerinin güvenliğini categorize edip control seçimi yapılmasını sağlayan bir standarttır. CNSSI 1253 , Sadece Azure Government ortamları için geçerlidir.

DFARS

DFARS yani Defense Federal Acquisition Regulation Supplement olarak geçmektedir. ABD Savunma Bakanlığı (DoD) ile iş yapan organizasyonlar için bir güvenlik kuralıdır. Bu kural özellikle hassas ama gizli olmayan bilgilerle çalışırken dataları korumayı , belli güvenlik standartlarını uygulamayı , meydana gelecek siber saldırılara karşı DoD bildirim yapmak kural gereği zorunludur. Microsoft Azure ve Azure Government servislerinde kullanılmaktadır. Yani kısacası ; DFARS , DoD ile çalışan şirketlere özel bir güvenlik koşulu diyebiliriz. Azure ve Azure Government zaten bu kurala uyuyor. Siz müşteri olarak kendi tarafınızdaki ayarları ve uygulamaları doğru yaparsanız , DFARS uyumlu olmuş oluyorsunuz.

DoD IL2

DoD IL2 , Amerika Birleşik Devletleri Savunma Bakanlığı'nın belirlediği güvenlik seviyesidir. Bu güvenlik seviyesinde kontrolü yapılmamış gizliliği olmayan veriler için geçerlidir. Halkla paylaşılabilecek ya da düşük önemdeki datalar için uygun bir güvenlik seviyesi olarak geçmektedir. Microsoft Azure ve Azure Government servislerinde kullanılmaktadır. Bu ortamları kullanan bir DoD tedarikçisi altyapı tarafında IL2 uyumluluğunu sağlamış olur.

DoD IL4

DoD IL4 , Savunma Bakanlığına ait olan ve kontrollü , gizli olmayan bilgileri içeren veriler için geçerli güvenlik seviyesidir. Ne gibi veriler ; İhracat kontrolü verileri , sağlık bilgileri , hukuk güvenliği bilgileri hassas fakat tam olarak sınıflandırılmamamış verileri kapsamaktadır. Bu veriler sınıflandırılmamış olarak geçer diyoruz ama korunması gereken bilgiler olarak öne çıkmaktadır. Azure Government , bu seviyede çalışmak isteyen organizasyonlara DISA (Defense Information System Agency) onaylı güvenli bir ortam sunmaktadır. Örnek vermek gerekirse ; Hassas Sağlık Verilerini bu ortamda güvenle barındırabilirsiniz.

DoD IL5

DoD IL5 , ABD Savunma Bakanlığı'nın bulut servis sağlayıcıları için getirdiği çok yüksek güvenlik seviyesidir. DISA , bu güvenlik seviyesini tanımlama ve düzenleme görevlerini gerçekleştirmektedir. Ne gibi veriler ; Hassas yada kritik verilen işlendiği ortamların en yüksek düzeyde izolasyon , şifreleme ve yetki kontrolleri işlemleri ile korunmaktadır. Bunu kullanacak ortamlarda gereklilik olarak Compute servisler için Dedicated Host veya Isolated VM şeklinde sunucu yapılandırması ve veriler için ise Customer Managed Key (CMK) ile şifreleme gerekmektedir. Anlattığımız üzere sadece US Government bölgelerinde kullanılmaktadır.

DoD IL6

DoD IL6 , ABD Savunma Bakanlığına ait secret yani sır seviyesindeki en gizli verilerin işlenmesi ve muhafaza edilmesi için tanımlanmış en yüksek güvenlik standartıdır. Bu seviye çalışan yada çalışacak bulut ortamındaki sunucular , sadece özel onaylı altyapılarda çalışabilir ve sadece uygun güvenlik koşullarını sağlayan Cloud Service Provider'lara verilir. Azure Government Secret , IL6 Provisional Authorization (PA) yetkisine sahip olan , Microsoft'un Classified Cloud Service Offering (CSO) ortamıdır. DISA tarafından onaylanan , High Confidentiality yani yüksek gizlilik , High Integrity yani yüksek bütünlük olarak H-H-x sınflandırılmıştır. Ayrıca bu ortam SIPRNet (Secret Internet Protocol Router Network) özel olan kapalı bir ağ altyapısında bulunmaktadır. Yani internetten değil , sadece bu güvenli ağ üzerinden erişim sağlanabilir. Azure Government yapısında çalışır. Azure Government Secret ayrıca IaaS , PaaS , SaaS bulut tiplerinde çalışmaktadır. Veriye bağlı olarak bir çok Azure servisleri IL6'ya dahil edilebilir. Örnek olarak ; Virtual Desktop Infrastructure , SQL , Cosmos DB , Identity Management , Azure OpenAI Service (en gizli sınıflandırma seviyesindeki görevler için hazır durumdadır)

DoE 10 CFR Part 810

ABD Enerji Bakanlığı (DoE) ait bir ihracat control düzenlemesi olarak geçmektedir. Atom Enerjisi Kanunu ve Nükleer Yayılmayı Önleme Kanunları kapsamında sınıflandırması yapılmamış nükleer teknolojilerinin veya yardımın dış ülkelere aktarımının control edilmesini sağlamaktadur. Bu tür bilgilerin veya hizmetlerin paylaşılabilmesi için DoE'den özel izin alınması gerekmektedir. Azure Government tarafından hizmet sunulmaktadır.

EAR

Export Administration Regulations olarak anılmaktadır. ABD Ticaret Bakanlığının uyguladığı düzenlemelerdir. Ticari ve Askeri amaçlı ürünler , yazılım ihracatı ve yeniden ihracatı üzerinde control sağlamaktadır. Bu düzenlemeye göre bulut ortamına yüklenen verilerde , müşteri veri sahibi olarak geçmektedir ve EAR'e göre sorumlu olan ihracatçı olarak değerlendirilir. Microsoft değildir. Microsoft Azure , Azure Government ve Azure Government Secret ortamlarında kullanılabilir.

FedRAMP

Federal Risk and Authorization Management Program olarak geçmektedir. ABD federal kurumları için bulut servislerinin güvenli şekilde değerlendirilmesi , yetkilendirilmesi ve sürekli izlenmesi amacıyla oluşturulan bir programdır. Azure ve Azure Government üzerinde kullanılabilir. Hizmet bazında bakmak gerekirse Cosmos DB , Azure Kubernetes Service , Azure Open AI , PowerBI , SQL Database gibi bir çok Azure hizmetlerini desteklemektedir.

FIPS 140

Federal Information Processing Standart olarak geçmektedir. ABD Hükümeti tarafından belirlenen bir standarttır. Kriptografik modüllerin minimum güvenlik seviyelerini tanımlamaktadır. Azure Key Vault ve Key Vault'un HSM (Hardware Security Module) altyapısında kullanılan cihazlar , Managed HSM'lerde kullanılmaktadır.

US Government

- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

ICD 503

Intelligence Community Directive 503 olarak geçmektedir. Amerika Birleşik Devletleri istihbarat topluluğu için bilgi sistemlerinde risk yönetimi ve yetkilendirme süreçlerini düzenleyen resmi bir politikadır. Bu politikanın içeriğinde risk yönetimi , yetkilendirmenin yanında karşılıklı Kabul , değerlendirme ve sistemler arası bağlantı gibi öğeleri içermektedir. Azure Government Top Secret yani en gizli ortamlarda kullanılmaktadır. Bu ortamda ABD hükümeti verileri güvenli şekilde işlenmektedir. Azure Government Top Secret ortamında bir çok Azure servisi kullanılmaktadır. Bunlara örnek ; Azure OpenAI Service , Azure Machine Learning , Power BI, Microsoft Graph , Microsoft Entra Domain Services vb bir çok servisleri kullanabiliriz.

IRS 1075

Internal Revenue Service 1075 olarak geçmektedir. Amerika Birleşik Devletlerinde FYI (Federal Tax Information) yani Federal Vergi Bilgilerini alan , işleyen veya depolayan federal , eyalet ve yerel kamu kurumlar için hazırlanmış bir güvenlik ve gizlilik kurallarını tanımlayan rehber olarak tanımlanmaktadır.

Azure , IRS 1075 uyumluluğunu FedRAMP High güvenliği , FIPS 140 şifreleme , Azure Policy ile denetim ve Microsoft'un sözleşmesel taahhütleri ile sağlamaktadır.

ITAR

International Traffic in Arms Regulations olarak anılmaktadır. Amerika Birleşik Devletleri Dışişleri Bakanlığı tarafından yönetilen ve savunmaya dair ürün , hizmet ve teknoloji bilgilerinin ihracatını , yeniden ihracatını ve transferini control eden düzenlemelerdir. Bu düzenleme ile veri aktarımları ve depolama işlemleri sırasında güçlü şifreleme teknolojilerini kullanmaktadır. Kullanıcıların , kendi anahtarlarını yönetebilecekleri seçenekler de sunulur. ITAR düzenlemesinde verilerin işlenmesi için Azure Government ve Azure Government Secret ortamları kullanılmaktadır.Ayrıca servis bağlamında bakacak olursak ; Azure Red Hat Openshift 'te ITAR uyumluluğunu desteklemektedir.

JSIG

Joint Special Access Program (SAP) Implementation Guide (JSIG) olarak anılmaktadır. ABD Savunma Bakanlığının en hassas verilerini korumak için hazırlanmış bir güvenlik kılavuzudur. Bu kılavuzda Bilgi Sistemlerinin güvenliğini artırmak amacıyla kurallar ve prosedürler içermektedir. Azure Government Secret VE Azure Government Top Secret ortamları JSIG standartlarına uygundur. Buradaki verileri sadece hükümet ve savunma projeleri gibi yüksek güvenlik gerektiren durumlarda geçerli olmaktadır.

NDAA

National Defense Authorization ACT olarak anılmaktadır. ABD Hükümentinin güvenliğini artırmayı amaçlayan kanun maddesidir. Bu madde ise belirli telekomünikasyon ekipmanlarının ve hizmetlerinin kullanımını yasaklamaktadır. Özellikle Huawei , ZTE , Hytera , Hikvision ve Dahua gibi şirketlerin ürün ve hizmetleri bu yasakta yer almaktadır. Microsoft'un Azure , Office365 , Dynamics 365 ve Surface gibi hizmetleri , ABD'deki sunucularındabu yasaklı şirketlerin ürünlerini kullanmaz. Yalnızca onaylı ve güvenli tedarikçilerle çalışılabilir.

NIST 800-161

The National Institute of Standarts and Technology (NIST) SP-800-161 olarak anılmaktadır. ABD'nin federal ajansları için hazırlanan kılavuzdur. Tedarik zincirindeki riskleri örnek olarak sahte donanım , kötü yazılım , hırsızlık belirlemek ve bu gibi durumların azaltılmasını sağlamak.

NIST 800-171

Controlled Unclassified Information (CUI) yani control altında tutulması gereken sınıflandırılmamış bilgileri korumaya yönelik standart diyebiliriz. Bu standart , federal olmayan kuruluşların CUI'yi koruması için belirli kriterler sunmaktadır. FedRAMP High sertifikası sayesinde uyumlu Kabul edilebilmektedir.

NIST 800-53

The National Institute of Standarts and Technology (NIST) 800-53 , Amerika Birleşik Devlet kurumları için hazırlanmış güvenlik kuralları listesi olarak geçmektedir. Sistemleri siber saldırılara , veri sızıntılarına ve kötü kullanıma karşı korumak amaçlanmaktadır. Birçok firma (özellikle devletle çalışanlar) bu kurallara uymak zorundadır. Microsoft Azure , bu kurallara uygun ortam sunmaktadır.

NIST 800-63

The National Institute of Standarts and Technology (NIST) 800-63 , Digital Identity Guidelines yani dijital kimlik doğrulama ve kimlik oluşturma süreçleri için Teknik ihtiyaçlarını tanımlamaktadır. Özellikle devlet kurumları tarafından kimlik hizmetleri üzerinde çalışmaktadır. Sağlık, Finans ve benzeri sektörler de bu standartları benimseyebilirler.

Bir nevi dijital kimlik havuzu diyebiliriz.

Üç ana bölümden oluşmaktadır:

Kimlik Kanıtlama (63A) ; " Bu kişi gerçekten kim ? "

Kimlik Doğrulama (63B) ; " Doğru kişi giriş yapıyor mu ? "

Federation (63C) ; " Aynı kimlikle farklı sistemlere güvenle giriş yapabilir mi ? "

Azure Entra ID , bu standartlara göre kimlik doğrulama işlemlerini gerçekleştirmene destek olmaktadır.

NIST CSF

The National Institute of Standarts and Technology (NIST) Cyber Security Framework yani Siber Güvenlik Çerçevesi olarak anılmaktadır. Amacı kritik sistemleri korumak için hazırlanmış siber güvenlik rehberi diyebiliriz. Burada amaç , riskleri anlamak , önlemler almak , olaylara hızlı tepki vermek ve normale dönmek için bir Framework sunmaktır. Bu rehberde 5 fonksiyon bulunmaktadır. Bunlar ;

Identify yani Tanımla ; Hangi varlıkların korunması gerektiğini belirlemek

Protect yani Koruma ; Güvenlik önlemleri almak

Detect yani Tespit ; Tehditleri ve olayları farketmek

Respond yani Yanıtla ; Olaylara müdahale etmek

Recovery yani Kurtar ; Sistemleri ve servisleri eski haline getirmek

Azure ve Azure Government ortamlarında çalışabilir. Azure'un bu çerçeveye uygunluğu denetlenmiş ve onaylanmıştır.

Section 508 VPATs

U.S. Section 508 , Amerika Birleşik Devletleri'nde federal kurumların elektronik ve bilgi teknolojisi (yazılım, doküman , donanım vb.) ürünlerinin , engelli kişiler tarafından erişilebilir ve kullanılabilir olmasını zorunlu kılan bir kanundur. Microsoft, bu erişilebilirlik yükümlülüğünü desteklemek amaçlı , ürün ve hizmetleri section 508 kriterlerine ne oranda uyduğunu gösteren Accessbility Conformance Reports yani Erişilebilirik Uyumluluk Raporları " yayımlamaktadır. Bu raporlar genelde Voluntary Product Accessibility Template (VPAT) formatında hazırlanmaktadır. VPAT , Microsoft ürünlerinin erişilebilirlik ihtiyaçlarını nasıl karşıladığını detaylı şekilde gösteren bir şablondur. Hangi ürünleri kapsar peki ? Azure ve Azure Government , Dynamics 365 , Intune, Office365

StateRAMP

State RAMP yani DevletRAMP , 2021 yılında Amerika Birleşik Devletlerindeki State and Local Goverments yani eyalet ve yerel yönetimlerin ihtiyaçlarına yönelik geliştirilen bir siber güvenlik programıdır. StateRAMP amacı eyalet ve yerel yönetim kurumlarının bulut servisi sağlayan firmaların güvenlik seviyelerini standart ve sade bir şekilde değerlendirmek , doğrulamaktır. Hangi servisleri ve ortamları destekliyor? Azure , Azure Government , Dynamics 365 , Dynamics 365 US Government ortamlarını desteklemektedir.

Financial Services

- 23 NYCRR Part 500 (US)
- AFM and DNB (Netherlands)
- AMF ve ACPR (France)
- APRA (Australia)
- CFTC 1.31 (US)
- EBA (EU)
- FCA and PRA (UK)
- FFIEC (US)
- FINMA (Switzerland)

23 NYCRR Part 500 (US)

New York Eyaleti'nin finansal kurumlar için siber güvenlik yönetmeliğidir. Yönetmeliğin amacı ; Müşteri verilerini ve bilgi sistemlerini korumaktır. Bu yönetmeliğe kimler uymalıdır ? Bankalar , Sigorta şirketleri, kredi ve yatırım firmaları gibi New York'ta faaliyet gösteren finansal kuruluşlardır. Microsoft Azure ve Microsoft 365 hizmetleri için uyum rehberi ve araçlar sunmaktadır.

AFM and DNB (Netherlands)

Dutch Authority for the Financial Markets and the Central Bank of the Netherlands

AFM and DNB yani Hollanda Finansal Piyasalar Otoritesi ve Hollanda Merkez Bankası olarak anılmaktadır. Hemen bunları tanımlayalım mı ?

AFM ; Hollandadaki tasarruf, kredi , yatırım ve sigorta piyasalarını denetleyen bağımsız bir kuruluştur.

DNB ; Avrupa Merkez Bankası Sistemi içinde yer alır ; Hollanda'daki finansal kuruluşları denetler ve para politikasını uygular.

Her iki kurum da AB Bankacılık Otoritesi (EBA) ile birlikte çalışarak cloud computing alanındaki düzenlemeleri belirler.

Buradaki amaç ; Microsoft bulut hizmetlerini kullanarak düzenleyici gereksinimlere uyum sağlamak. Ne gibi hizmetler mevcut : Microsoft Azure, Dynamics 365 , Microsoft 365

AMF ve ACPR (France)

Financial Authority (AMF) and Prudential Authority (ACPR) France

AMF ; Fransa'daki finansal piyasaları ve yatırım firmalarını denetleyen otorite olarak tanımlanmaktadır.

ACPR ; Fransa Merkez bankası'na bağlı, bankacılık ve sigorta sektörlerini denetleyen bağımsız bir otoritedir.

Fransadaki finansal kurumlar Microsoft Bulut Hizmetlerini kullanarak AMF ve ACPR düzenlemelerini uyum sağlamak amaçlıdır. Bu uyumlar; AMF Genel Düzenlemesi ile bulut servis sağlayıcılarıyla yapılacak sözleşmelerde bulunması gereken şartları , ACPR yönergeleri ise cloud computing riskleri ve bu servis sağlayıcılarıyla yapılacak sözleşmelerde bulumması gereken zorunlu şartları , AB Bankacılık Otoritesi Yönergeleri, Finansal kurumların bulut servis sağlayıcılarıyla işbirliği yaparken dikkate alması gereken genel yönergeleri içermektedir. Hangi Hizmetlerde kullanılır ? Microsoft Azure , Dynamics 365 , Microsoft 365

APRA (Australia)

Australian Prudential Regulation Authority olarak anılmaktadır. Avustralyada'ki bankalar, sigorta şirketleri ve diğer finansal hizmet sağlayıcılarını denetleyen bağımsız bir düzenleyici otoritedir. Cloud Computing'e geçişin artan önemini göz önünde bulundurarak , finansal kurumların bulut servis sağlayıcılarını değerlendirirken dikkatli bir risk değerlendirmesi yapmaları ve düzenli denetimler gerçekleştirmelerine destek vermektedir. Hangi hizmetlerde kullanılır ? Microsoft Azure , Dynamics 365 , Microsoft 365

CFTC 1.31 (US)

Securities and Exchange Commission (SEC) Rule;

SEC Rule 17a-4 ; Amerika Birleşik Devletleri Menkul Kıymetler ve Borsa Komisyonu (SEC) ,menkul kıymetler aracılık firmaların ve broker-dead'ların kayıtlarını dijital ortamda saklamalarını şart koşar.

SEC Rule 18a-6 ; Güvenlik Bazlı Takas işlemcileri ve büyük Güvenlik Bazlı Takas katılımcıları için benzer dijital kayıt saklama gereksinimlerini belirler.

Bu kurallar ile finansal kuruluşların kayıtlarını güvenli ve erişilebilirbir şekilde saklanmalarını sağlamak için tasarlanmıştır.

Microsoft , SEC kurallarına uyum sağlamanız için Immutable Blob Storage , Preservation Lock, Audit Trail hizmetleriyle yardımcı olmaktadır.

EBA (EU)

European Banking Authority yani Avrupa Bankacılık Otoritesi olarak anılmaktadır. Avrupa Birliğin'de bankacılık sektöründe etkin ve tutarlı düzenleme ve denetimi sağlamak amacıyla kurulmuş bağımsız bir otoritedir. Kısaca; Microsoft , EBA uyumlu finans kurumlara denetim, dış kaynak bildirimi,very merkezi seçenekleri, alt yüklenici yönetimi , iş sürekliliği ev risk izleme desteği sunmaktadır. Hangi hizmetlerde kullanılır ? Microsoft Azure, Microsoft 365

FCA and PRA (UK)

Financial Conduct Authority (FCA) ve Prudential Regulation Authority olarak geçmektedir.

FCA ; İngiltere'de finansal piyasaları yani Bankaları ve yatırım firmalarını denetlemektedir.

PRA ; İngiltere'de bankalar ve sigorta şirketlerinin finansal sağlamlığını denetlemektedir.

Microsoft , Finansal kurumlara denetim hakları , dış kaynak bildirimi, alt yüklenici bildirimi, iş sürekliliği ve risk izleme desteği sunmaktadır. Hangi hizmetlerde kullanılır ? Microsoft Azure , Dynamics 365 , Microsoft 365 , Microsoft Intune

FFIEC (US)

ABD Federal Financial Institutions Examination Council (FFIEC) yani ABD Federal Finansal Kurumlar Denetim Konseyi olarak geçmektedir. Amerika Birleşik Devletlerindeki finansal kurumların teknoloji altyapılarını denetleyen federal kuruldur. FFIEC IT Denetim El kitabı ve Outsourcing Technology Services kitapçıkları , bulut servis sağlayıcılarının değerlendirilmesinde kullanılacak kriterleri belirlemektedir. Hangi hizmetlerde kullanılır ? Microsoft Azure, Dynamics 365 , Microsoft 365

FINMA (Switzerland)

Financial Market Supervisory Authority Switzerland yani İsviçre Finansal Piyasalar Denetleme Otoritesi olarak anılmaktadır. İsviçre'deki finansal kurumları denetleyen bağımsız bir oteritedir. Finansal kurumların kritik işlevlerini dış kaynak kullanımıyla buluta taşıması durumunda uyması gereken düzenlemeleri belirlemektedir.

Microsoft, FINMA uyumu için denetim, dış kaynak ve alt yüklenici bildirimi, veri merkezleri, iş sürekliliği ile risk ve güvenlik izleme desteği sağlar. Hangi hizmetlerde kullanılır ? Microsoft Azure, Dynamics 365 , Microsoft 365

Financial Services

- FINRA 4511 (US)
- FISC (Japan)
- FSA (Denmark)
- GLBA (US)
- KNF (Poland)
- MAS and ABS (Singapore)
- NBB and FSMA (Belgium)
- OSFI (Canada)

FINRA 4511 (US)

The Financial Industry Regulatory Authority kapsamındaki düzenlemeye göre SEC Rule 17a-4 ve 18a-6 , broker-dealer'ların ve swap işlemcilerinin kayıtlarını güvenli ve erişilebilir bir biçimde saklamasını zorunlu kılmaktadır. Bu kurallara uyum sağlanabilmesi için ; WORM yani kayıtların değiştirilemez , denetlenebilir ve gerektiğinde erişilebilir olması gerektiğini belirtmektedir. Microsoft Azure ve Microsoft 365 bu kurallara uygun çalışmaktadır. Microsoft , resmi bir uygunluk mektubu hazırlayıp SEC'e sunmanız için sizlere destek vermektedir. Kısacası ; Microsoft , Finans şirketlerinin kayıtlarını güvenli saklamasını ve SEC kurallarına uyum sağlamasını kolaylaştırmaktadır.

FISC (Japan)

Center for Financial Information Systems , Japonya Maliye Bakanlığı tarafından kurulmuş ve bankacılık sistemlerinin güvenliğini artırmayı amaçlayan organizasyondur. Finansal kuruluşlar için bilgisayar sistemlerinde güvenlik politikaları , acil durum planları ve 300'den fazla control içeren standartlardır. Bunlar yasal bir zorunluluk olmasa da Japonya'daki finansal kurumlar genellikle bu standartlara uymaktadır. Microsoft'un bu uyumuyla , Japonya'daki finansal kurumların bulut geçişlerinde güven oluşturmasına yardımcı olmaktadır. Hangi hizmetlerde kullanılır ? Microsoft Azure , Dynamics 365, Office 365 , Intune , Power BI

FSA (Denmark)

Financial Supervisory Authority Denmark yani Danimarka Finansal Denetim otoritesi olarak anılmaktadır. Danimarka'nın finansal kurumlarını denetleyen resmi otoritesi olan ülke içindeki bankalar ve finans kuruluşlarına yönelik düzenleyici kurallar hazırlamak ve uyumu denetlemekle sorumludur. Ayrıca Avrupa Bankacılık Otoritesi (EBA) ile birlikte çalışarak, bulut bilişimde dış kaynak kullanımına dair kapsamlı öneriler sunmaktadır. Hangi hizmetlerde kullanılır ? Microsoft Azure , Dynamics 365 , Microsoft 365

GLBA (US)

Gramm–Leach–Bliley Act olarak anılmaktadır. GLBA , Amerika Birleşik Devletlerinde Finansal Kuruluşların müşteri gizliliğini koruma zorunluluğunu getiren yasadır. Hangi hizmetlerde kullanılır ? Microsoft Azure, Office 365, Dynamics 365 , Power BI

KNF (Poland)

The Polish Financial Supervision Authority (KNF) yani Polonya Finansal Denetim Otoritesi olarak anılmaktadır. Polonya'daki bankacılık, sermaye piyasaları, sigorta, emeklilik ve elektronik para kurumlarını denetleyen ana finansal düzenleyici otoritedir. KNF, Avrupa Bankacılık Otoritesi (EBA) ile birlikte finansal kuruluşların bulut hizmet sağlayıcılarını nasıl değerlendirmesi gerektiğine dair rehberler oluşturmaktadır. Microsoft, Polonya'daki finansal kurumlar için bir **bulut uyumluluk kontrol listesi (compliance checklist)** sağlar. Hangi hizmetlerde kullanılır ? Microsoft Azure, Dynamics 365 , Microsoft 365

MAS and ABS (Singapore)

Monetary Authority of Singapore (MAS) yani Singapur Para Otoritesi , Association of Banks in Singapore yani Singapur Bankalar Birliği olarak anılmaktadır.

MAS , Singapur'un merkezi bankası ve finansal kurumları denetleyen otoritesidir. Finansal kurumların bulut hizmetlerinde güvenli ve risk temelli bir yaklaşım benimsemesini önermektedir. Bunlardan biri, **"material outsourcing"** olarak tanımlanan kritik dış kaynak kullanımının yıllık gözden geçirilmesi ve denetim haklarının sözleşmelere dahil edilmesi olarak tanımlanmaktadır. MAS, bulut hizmet kullanımından önce bilgi verilmesini zorunlu kılmaz; ancak risk temelli kendi değerlendirmelerini yapmalarını istemektedir.

ABS , MAS yönergelerine destek olarak bankalara yönelik **Uygulama Rehberi (Cloud Computing Implementation Guide)** yayınlamıştır. Özellikle sözleşme detayları ve teknik güvenlik önlemleri konusunda yol gösterir.

NBB and FSMA (Belgium)

National Bank of Belgium (NBB) yani Belçika Ulusal Bankası Financial Services and Markets Authority (FSMA) yani Finansal Hizmetler ve Piyasalar Otoritesi olarak anılmaktadır.

NBB ; Bankalar, sigorta şirketleri, aracı kurumlar gibi finansal kuruluşların denetiminden sorumlu merkez bankası

FSMA ; Finansal piyasaları, yatırım şirketlerini ve tasarruf-planlarını denetleyen kurumdur.
Her iki kuruluş da, AB düzeyinde Outsourcing yani dış kaynak kullanımı konusunda ortak standartlar belirleyen EBA ile uyumlu şekilde çalışmaktadır. Belçika'daki finans kurumlarına, Microsoft'un bulut hizmetlerini kullanırken NBB ve FSMA düzenlemelerine **uyumlu olabilmeleri** için hazırlanmış bir **uyum kontrol listesi (compliance checklist)** sunmaktadır. Hangi hizmetlerde kullanılır ? Microsoft Azure, Dynamics 365 , Microsoft 365

OSFI (Canada)

Office of the Superintendent of Financial Institutions , Kanada'da finansal kurumları (bankalar, sigorta şirketleri gibi) denetleyen düzenleyici otoritedir. Finansal kuruluşlar, bulut hizmet sağlayıcılarıyla yaptıkları dış kaynak kullanımında OSFI'nin **B-10 yönergelerine** ve Kanada'nın gizlilik kanunlarına (örneğin PIPEDA) uymak zorundadırlar. Hangi hizmetlerde kullanılır? Microsoft Azure, Dynamics 365 , Microsoft 365