Dedikio A/S
Your Security is our Passion

IT Asset Management barometer (ITAM)

Bemærkninger

>>> Angiv dine valg i kolonne E "Svar": 0=nej, 1=delvist og 2=Ja. Er spørgsmålet ikke relevant skrives 0 i kolonne D "relevans". Begynd eventuelt med at rulle ned til sektionerne "Center for Internet Security" eller "Pragmatisk.."

Kategori	Relevans	Svar	Spørgsmål	Dine bemærkninger
ITIL (15)	✗	✗	ITIL: Alle aktiver skal være unikt identificerbare og ligge i samme system	
	✗	✓	ITIL: Et samlet ITAM system som kan håndtere alle ITAM processer	
	✗	✓	ITIL: Opdag alle aktiver via enautomatiseret undersøgelse af hele netværket	
	✗		ITIL: Tilføjelse og fjernelse af aktiver skal ske i en struktureret proces	
	✗		ITIL: Der skal gennemføres regelmæssige kontroller for validiteten af aktiver i ITAM systemet	
	✗		ITIL: ITAM IT-Sikkerhed - Adgang til ITAM skal ske sikkert hvad angår protokol og brugere	
	✗		ITIL: ITAM IT-Sikkerhed - Administration af ITAM systemet skal ske efter klare retningslinjer	
	✗		ITIL: ITAM IT-Sikkerhed - Rollebaseret adgang til ITAM efter organisatorisk behov	
	✗		ITIL: ITAM IT-Sikkerhed - Klare og tydelige it-sikkerhedspolitikker	
	✗		ITIL: Tilføjer og ændring i mærkater for aktiver skal ske efter en struktureret ændringsproces	
	✗		ITIL: Compliance - Proces for at isolere eller fjerne aktiver som er End of Life (EOL)	
	✗		ITIL: Compliance - Proces for at sammenligne tilladte software licenser med installeret software	
	✗		ITIL: Compliance - Proces for at indkøbe software så licensreglerne er overholdt	
	✗		ITIL: Hold styr på værdien af aktiver inklusive afskrivninger	
	✗		ITIL: Hav en godkendt procedure og proces for bortskaffelse af aktiver	
NIST Cyber Security Framework (10)	✗		NIST CSF: ID.AM-1: Physical devices and systems within the organization are inventoried (CIS 1.4,2.5)	
	✗		NIST CSF: ID.AM-2: Software platforms and applications within the organization are inventoried (CIS 2.1-2,2.4-5)	
	✗		NIST CSF: ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	
	✗		NIST CSF: ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
	✗		NIST CSF: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes (CIS 1.7)	
	✗		NIST CSF: PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions (CIS 1.8)	
	✗		NIST CSF: PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition (CIS 1.4-6)	
	✗		NIST CSF: PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity (CIS 2.8-9)	
	✗		NIST CSF: PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	
	✗		NIST CSF: DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed (CIS 1.1-3+2.3+2.6-9)	
Center for Internet Security (18)	✓		CIS 1.01: Utilize an Active Discovery Tool (IG-2)	
	✗		CIS 1.02: Use a Passive Asset Discovery Tool (IG-3)	
	✓		CIS 1.03: Use DHCP Logging to Update Asset Inventory (IG-2)	
	✓		CIS 1.04: Maintain Detailed Asset Inventory (IG-1)	
	✓		CIS 1.05: Maintain Asset Inventory Information (IG-2)	
	✓		CIS 1.06: Address Unauthorized Assets (IG-1)	
	✓		CIS 1.07: Deploy Port Level Access Control (IG-2)	
	✗		CIS 1.08: Utilize Client Certificates to Authenticate Hardware Assets (IG-3)	
	✓		CIS 2.01: Maintain Inventory of Authorized Software (IG-1)	
	✓		CIS 2.02: Ensure Software is Supported by Vendor (IG-1)	
	✓		CIS 2.03: Utilize Software Inventory Tools (IG-2)	
	✓		CIS 2.04: Track Software Inventory Information (IG-2)	
	✗		CIS 2.05: Integrate Software and Hardware Asset Inventories (IG-3)	
	✓		CIS 2.06: Address unapproved software (IG-1)	
	✗		CIS 2.07: Utilize Application Whitelisting (IG-3)	
	✗		CIS 2.08: Implement Application Whitelisting of Libraries (IG-3)	
	✗		CIS 2.09: Implement Application Whitelisting of Scripts (IG-3)	
	✗		CIS 2.10: Physically or Logically Segregate High Risk Applications (IG-3)	
Pragmatisk tilgang (16)	✓		**Pragmatisk: Alle ITAM aktiver samles i ét system (Fokus på hardware og software)**	
	✓		**Pragmatisk: Automatiseret rettighedsbaseret kontinuerlig/regelmæssig opdagelse af netværket med og uden agenter**	
	✓		**Pragmatisk: Inddeling af hardware og software i relevante dynamiske grupper**	
	✓		**Pragmatisk: Alle relevante systemer dokumenteres med ejer, formål, afhængigheder, kritikalitet og (person)datafølsomhed**	
	✓		**Pragmatisk: Sikker adgang til ITAM baseret på roller**	
	✓		**Pragmatisk: Mapning af afhængigheder på hardware, software og systemer hvor det er muligt og relevant**	
	✓		**Pragmatisk: Rapporter, dashboards og alarmer baseret på ønsker fra organisationen**	
	✓		**Pragmatisk: Fokus på dashboard der understøtter KPI fra CIS kontrollerne**	
	✓		**Pragmatisk: Fokus på sikkerhed ved brug af scanningsrettigheder**	
	✓		**Pragmatisk: Interface til andre systemer hvor det er muligt - ITSM, Endpoint Management, PAM og sårbarhedsscanning**	
	✓		**Pragmatisk: Proces for at justere installerede licenser med ejede licenser**	
	✓		**Pragmatisk: Proces for undersøgelse for og rettelse af scannings fejl - regelmæssigt**	
	✓		**Pragmatisk: Proces for at fjerne uautoriseret software - regelmæssigt**	
	✓		**Pragmatisk: Proces for at fjerne uautoriseret hardware - regelmæssigt**	
	✓		**Pragmatisk: Proces for at vedligeholde ITAM systemet - regelmæssigt**	
	✓		**Pragmatisk: Proces for at fjerne/isolere devices og software som er EOL - regelmæssigt**	

ndarder for Hardware inven	- **CIS CSC** 1	
	- **COBIT 5** BAI09.01, BAI09.02	
(følge NIST CSF 800-53r4)	- **ISA 62443-2-1:2009** 4.2.3.4	
	- **ISA 62443-3-3:2013** SR 7.8	
	- **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2	
	- **NIST SP 800-53 Rev. 4** CM-8, PM-5	

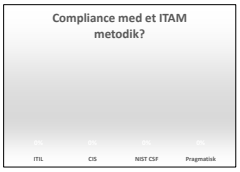
ndarder for Software inven	- **CIS CSC** 2	
	- **COBIT 5** BAI09.01, BAI09.02, BAI09.05	
(følge NIST CSF 800-53r4)	- **ISA 62443-2-1:2009** 4.2.3.4	
	- **ISA 62443-3-3:2013** SR 7.8	
	- **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1	
	- **NIST SP 800-53 Rev. 4** CM-8, PM-5	

Resultat

Ja=1, Nej=1, Delvist=1 Ja=0, Nej=0, Delvist=0 Ja=0, Nej=0, Delvist=0

ITIL (15)	CIS (18)
0%	0%

NIST CSF (10)	Pragmatisk (13)
0%	0%



Udfyldt af:	Navn / e-mail
Dato:	dd.mm.åååå
Virksomhed:	Navn på virksomhed
Ledelsesgodkendt:	Ja / Nej / Delvist / Ukist