CSA cloud security alliance®

Fremme av god praksis for å sikre skytjenester, og gi opplæring i bruk av skytjenester for å sikre alle andre former for databehandling.

www.cloudsecurityalliance.no

BDO

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE (CCSK)

NORMKONFERANSEN 25. NOVEMBER 2019

CCSK™

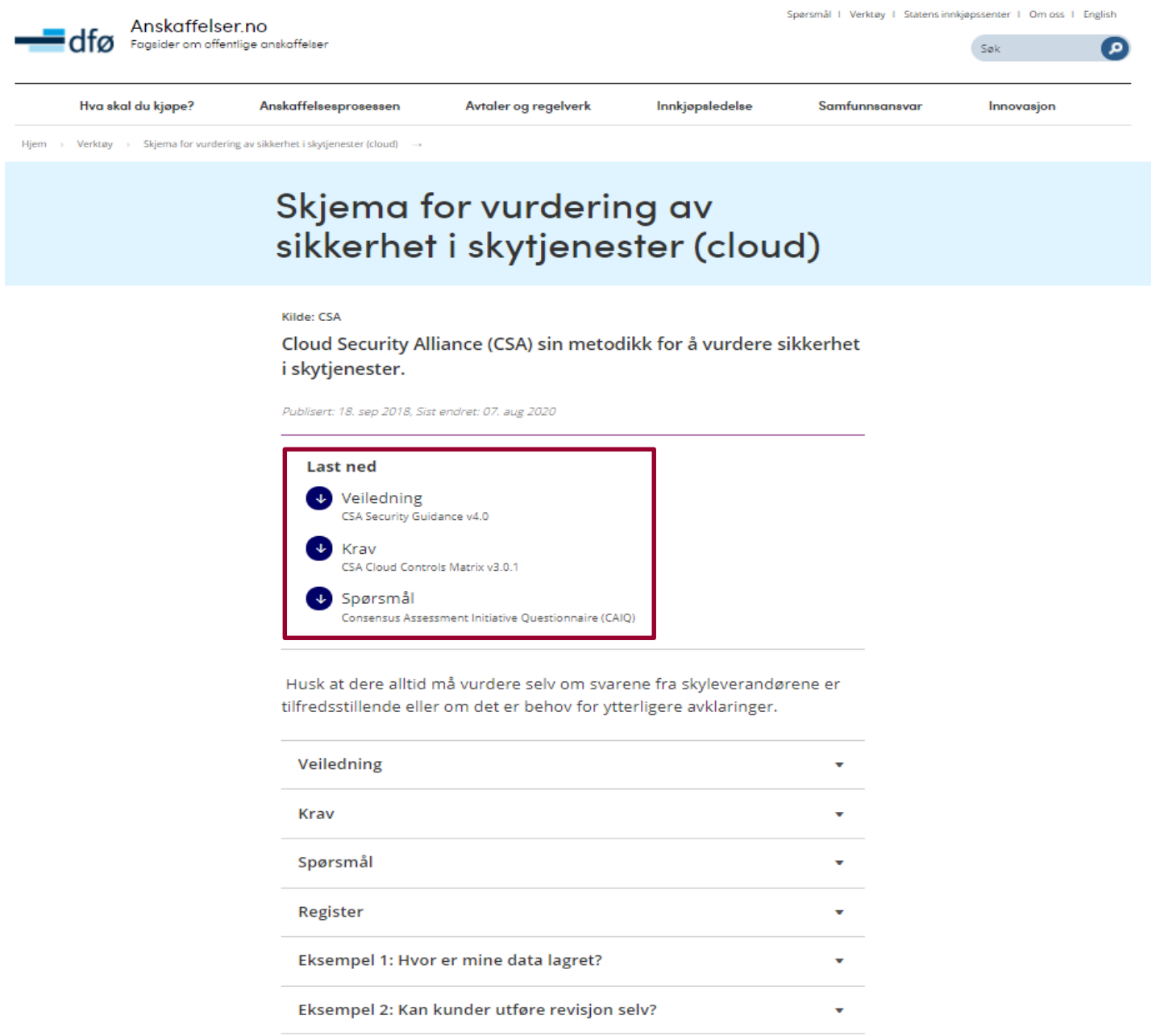
Certificate of

Cloud Security Knowledge

www.cloudsecurityalliance.no/ccsk

BDO

https://www.anskaffelser.no/verktoy/veiledere/skjema-vurdering-av-sikkerhet-i-skytjenester-cloud



dfø Anskaffelser.no
Fagsider om offentlige anskaffelser

Spørsmål | Verktøy | Statens innkjøpssenter | Om oss | English

Søk

Hva skal du kjøpe? | Anskaffelsesprosessen | Avtaler og regelverk | Innkjøpsledelse | Samfunnsansvar | Innovasjon

Hjem › Verktøy › Skjema for vurdering av sikkerhet i skytjenester (cloud) →

Skjema for vurdering av sikkerhet i skytjenester (cloud)

Kilde: CSA

Cloud Security Alliance (CSA) sin metodikk for å vurdere sikkerhet i skytjenester.

Publisert: 18. sep 2018, Sist endret: 07. aug 2020

Last ned

- Veiledning
  CSA Security Guidance v4.0
- Krav
  CSA Cloud Controls Matrix v3.0.1
- Spørsmål
  Consensus Assessment Initiative Questionnaire (CAIQ)

Husk at dere alltid må vurdere selv om svarene fra skyleverandørene er tilfredsstillende eller om det er behov for ytterligere avklaringer.

- Veiledning
- Krav
- Spørsmål
- Register
- Eksempel 1: Hvor er mine data lagret?
- Eksempel 2: Kan kunder utføre revisjon selv?

CCM™
Cloud Controls Matrix

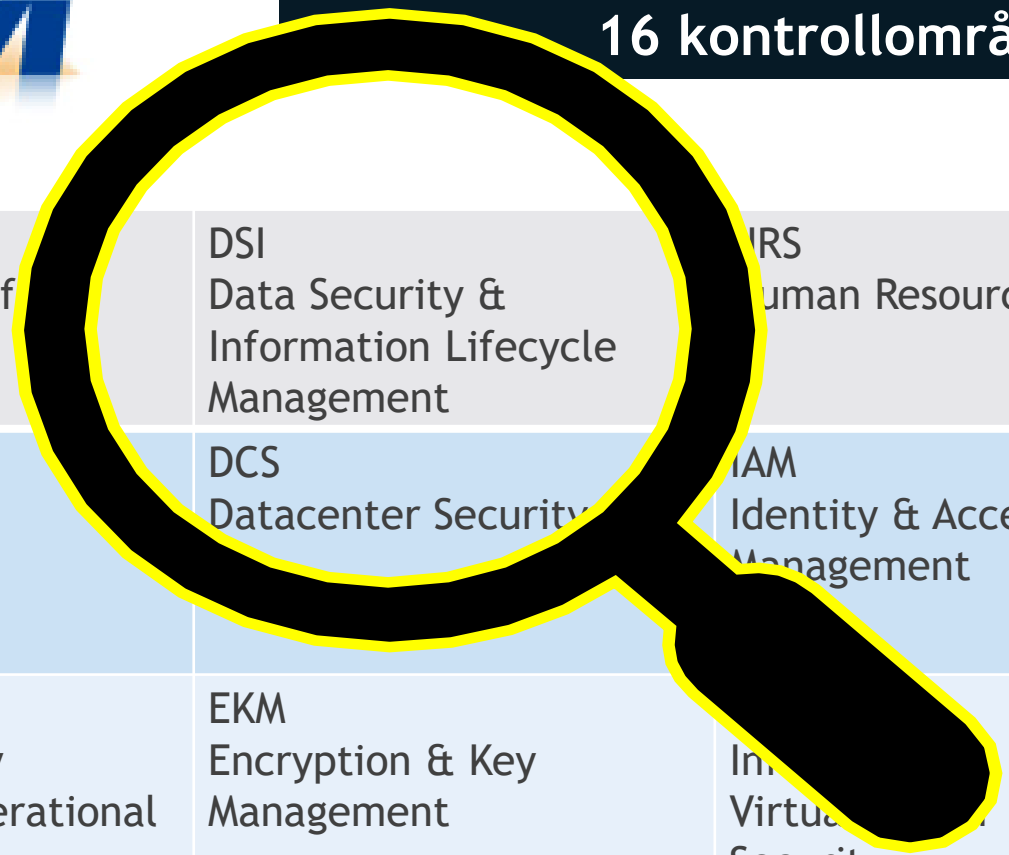
133 kontrollkrav (16 kontrollområder)

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		AICPA 2009 TSC Map	AICPA Trust Service Criteria (SOC 2SM Report)
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer		
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.		X	X	X	X	X	X	X	X	X	X		S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.

Scope Applicability														
CIS-AWS-Foundation v1.1	COBIT 4.1	COBIT 5.0	ENISA IAF	95/46/EC – European Union Data Protection Directive	HITRUST CSF v8.1	ISO/IEC 27001:2013	ISO/IEC 27002:2013	ISO/IEC 27017:2015	ISO/IEC 27018:2015	NERC CIP	NIST SP800-53 R3	NIST SP800-53 R4 App J	PCI DSS v2.0	PCI DS
	AI2.4	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	6.03.01.(c)	Article: 27 (3)	10.b;10.c;10.e	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	9.4.2 9.4.1 12.6.1 14.2.1 14.2.3 14.2.7 18.2.2	9.4.1 12.6.1 14.2.1		CIP-007-3 - R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11	AR-7 The organization designs information systems to support privacy by automating privacy controls.	6,5	6, 6.5

16 kontrollområder



AIS Application & Interf Security	DSI Data Security & Information Lifecycle Management	IRS uman Resources	MOS Mobile Security
AAC Audit Assurance & Compliance	DCS Datacenter Security	IAM Identity & Access anagement	SEF Security Incident Management, E-Discovery, & Cloud Forensics
BCR Business Continuity Management & Operational Resilience	EKM Encryption & Key Management	In & Virtu Security	STA Supply Chain Management, Transparency, and Accountability
CCC Change Control & Configuration Management	GRM Governance and Risk Management	IPY Interoperability & Portability	TVM Threat and Vulnerability Management

DSI
Data Security & Information Lifecycle Management

7 spørsmål

Control specification	
DSI-01	Classification
DSI-02	Data Inventory / Flows
DSI-03	E-commerce Transactions
DSI-04	Handling / Labeling / Security Policy
DSI-05	Nonproduction Data
DSI-06	Ownership / Stewardship
DSI-07	Secure Disposal

DSI-01
Classification

Kontrollspørsmål (CAIQ)	
DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?
DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?

Microsoft Azure

https://cloudsecurityalliance.org/star

Cloud Services by Microsoft

Microsoft Azure

STAR Self-Assessment — **Submitted:** March 30th, 2012

Consensus Assessments Initiative Questionnaire v3.0.1	Download
	Supporting Asset #1

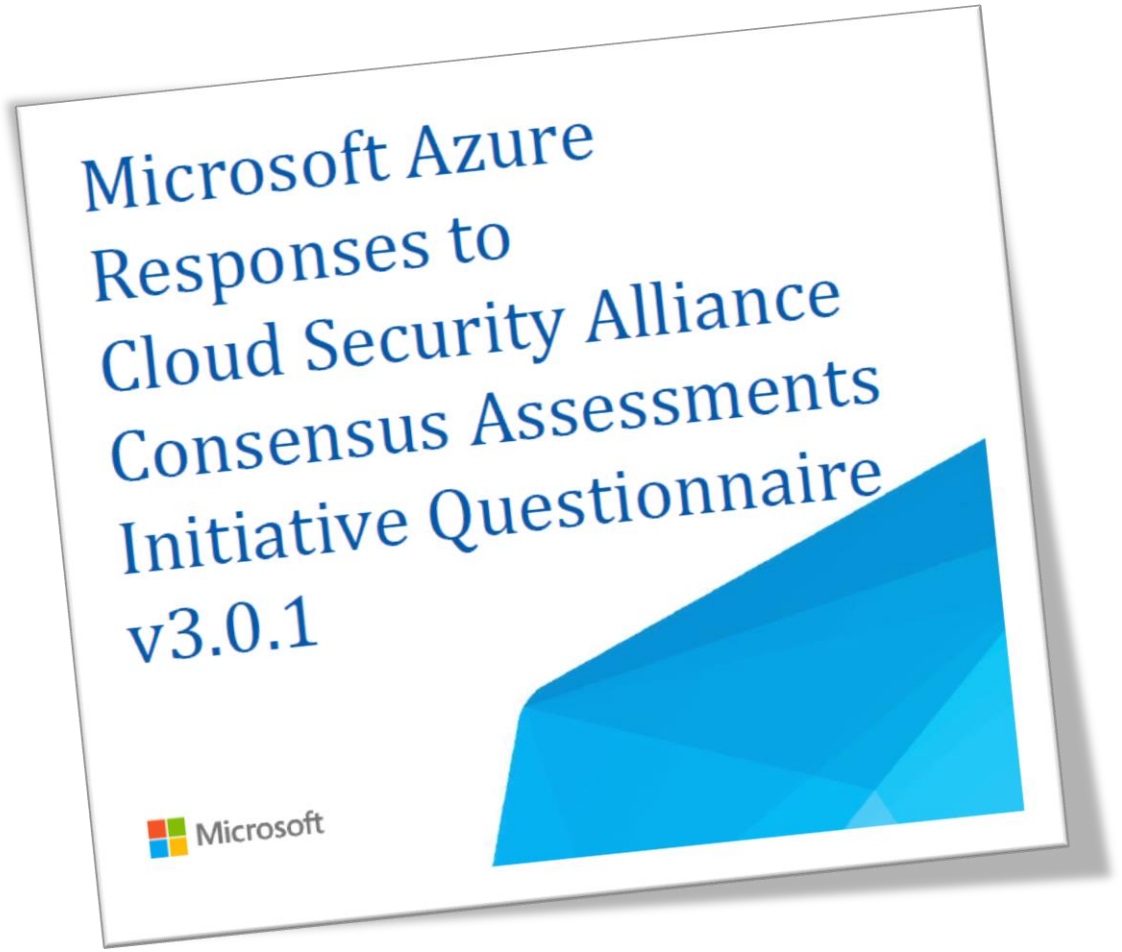
Deprecated

STAR Attestation — **Submitted:** October 1st, 2016

STAR Attestation v1	Download

STAR Certification — **Submitted:** March 30th, 2012

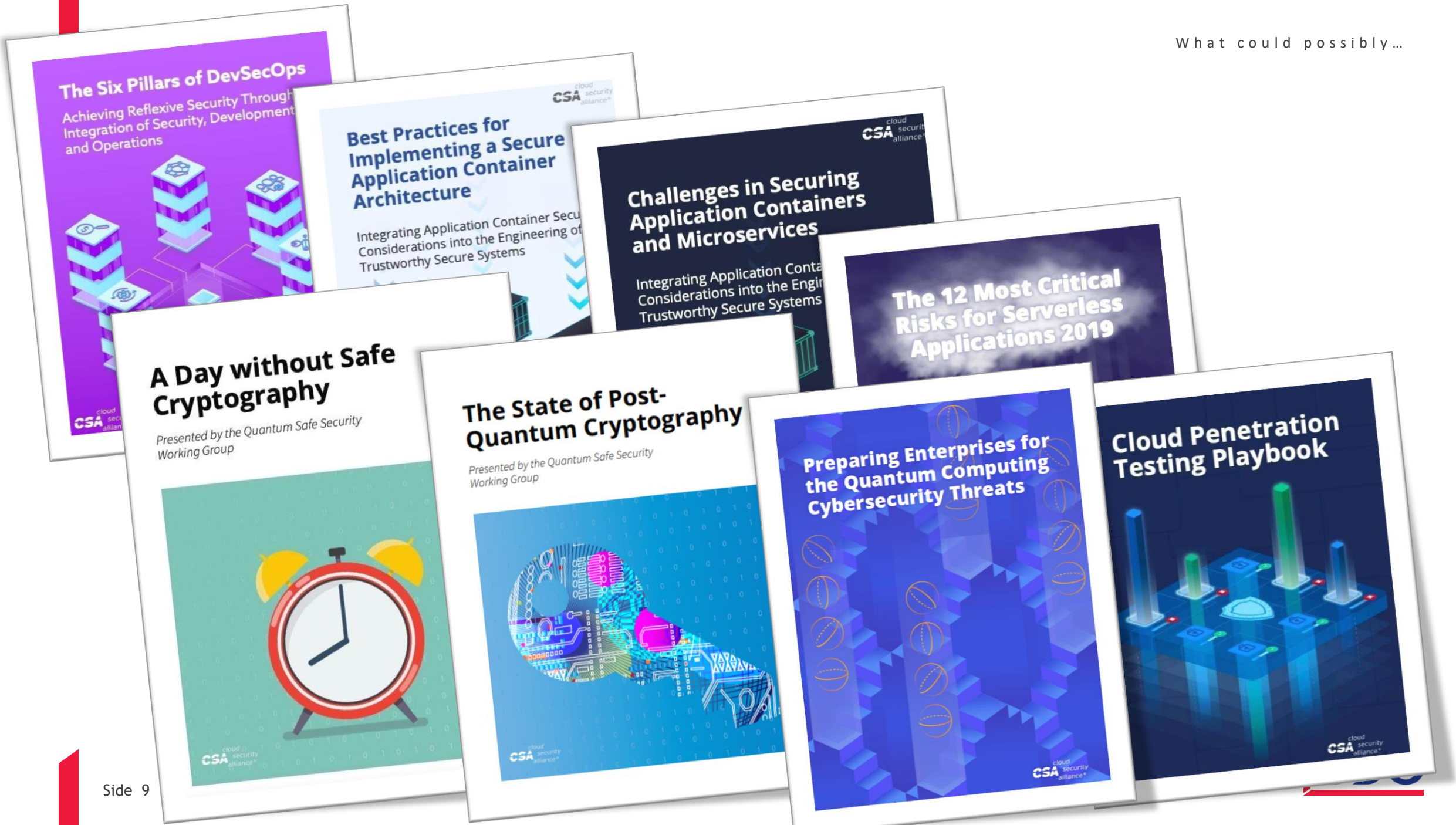
STAR Certification v1	Download



cloud security alliance®

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

BDO


The Six Pillars of DevSecOps
Achieving Reflexive Security Through Integration of Security, Development and Operations
Best Practices for Implementing a Secure Application Container Architecture
Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems
Challenges in Securing Application Containers and Microservices
Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems
The 12 Most Critical Risks for Serverless Applications 2019
A Day without Safe Cryptography
Presented by the Quantum Safe Security Working Group
The State of Post-Quantum Cryptography
Presented by the Quantum Safe Security Working Group
Preparing Enterprises for the Quantum Computing Cybersecurity Threats
Cloud Penetration Testing Playbook

NORMEN

normen.no

https://ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen

CSA har mappet CCM opp mot Normens krav (PDF)

BDO

Tabellen under gir en kryssreferanse mellom Normen 6.0 og de 16 kontrolldomenene i Cloud Controls Matrix.

CCMv3.0.1 Control Domain	NORMEN Versjon 6.0
Application & Interface Security AIS	4.3 Innebygd personvern 5.4.1 Konfigurasjonskontroll 5.7.6 Systemleverandører
Audit Assurance & Compliance AAC	2.4 Styringssystem 2.5 Ledelsens gjennomgang 5.4.6 Sikkerhetsrevisjon
Business Continuity Management & Operational Resilience BCR	3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet 5.4.3 Sikkerhetskopiering 5.7.5 Vedlikehold, fjernaksess eller fysisk service 5.9 Nødrutiner

Change Control & Configuration Management CCC	5.4.1 Konfigurasjonskontroll 5.4.2 Endringsstyring 5.7.6 Systemleverandører
Data Security & Information Lifecycle DSI	3.3 Oversikt over teknologi og behandling av helse- og personopplysninger 4.2.3 Innsyn 4.2.4 Retting og sletting 4.2.5 Tilgjengeliggjøring og utlevering av opplysninger i behandlingsrettet helseregister 4.2.6 Oppbevaring av helse- og personopplysninger 4.3 Innebygd personvern 5.4.1 Konfigurasjonskontroll
Datacenter Security DCS	3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet 5.3 Fysisk sikkerhet og håndtering av utstyr

Encryption & Key Management EKM	5.3.4 Mobilt utstyr og hjemmekontor 5.3.5 Kryptering 5.5.3 Elektronisk samhandling 5.6 Digital kommunikasjon til den registrerte
Governance and Risk Management GRM	2.1 Roller og ansvar for informasjonssikkerhet og personvern 2.2 Dataansvarliges ansvar 2.3 Databehandlers ansvar 2.4 Styringssystem 2.5 Ledelsens gjennomgang 3 Risikostyring 3.4 Risikovurdering og risikohåndtering 3.5.1 Personvernkonsekvensvurdering 5.7 Leverandørforhold og avtaler 5.7.3 Tjenesteutsetting 5.7.4 Databehandler 5.7.9 Skytjenester

Human Resources HRS	4.2.1 Taushetsplikten 5.1.1 Vilkår og betingelser 5.1.2 Opplæring og kompetanse 5.1.3 Opphør av arbeidsforhold 5.7.1 Krav til leverandørers taushetsplikt
Identity & Access Management IAM	3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet 5.2 Tilgangsstyring 5.2.1 Autorisering 5.2.2 Autentisering 5.2.3 Kontroll av tilgang 5.4.4 Logging 5.5.2 Tilkobling til eksterne nett 5.5.5 Tilkobling til Internett
Infrastructure & Virtualization Security IVS	3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet 5.3.3 Infrastruktur 5.4.1 Konfigurasjonskontroll 5.4.4 Logging 5.4.5 Styring og håndtering av tekniske sårbarheter 5.5.1 Styring av nettverkssikkerhet 5.5.2 Tilkobling til eksterne nett 5.5.5 Tilkobling til Internett

Interoperability & Portability IPY	5.5.3 Elektronisk samhandling
Mobile Security MOS	5.3.4 Mobilt utstyr og hjemmekontor
Security Incident Management, E-Discovery, & Cloud Forensics SEF	5.8.1 Avvikshåndtering 5.8.2 Brudd på personopplysningssikkerhet
Supply Chain Management, Transparency, and Accountability STA	5.7.3 Tjenesteutsetting 5.7.4.1 Databehandlers underleverandører 5.7.8 Overføring av opplysninger til utlandet
Threat and Vulnerability Management TVM	5.4.1 Konfigurasjonskontroll 5.4.5 Styring og håndtering av tekniske sårbarheter 5.7.6 Systemleverandører

Samlet oversikt Normens krav

Nr	Krav (formulert som spørsmål)	Kap. i Normen	Kap. i ISO 27001 og Annex A	CSA CCM Control ID	Systemkrav i behandlings-rettet helse-register	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivaretatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivaretatt av data-behandler
1.	Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv?	1.5	6.1.1 8.1	(GRM-09)			☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21 FLK § 6	
2.	Er valgte tiltak basert på risikovurderinger?	1.5	6.1.3 8.3	GRM-08 STA-04			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐Ja ☐Nei
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	1.5	6.1* 8.1.*	(GRM-09)			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	
4.	Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges?	2	5.1 5.2 5.3	(GRM-03)			☐Ja ☐Nei	PJL § 22 HRL § 21 HTL § 5-10 første punktum PVF artikkel 24 FLK § 7	
5.	Har virksomhetens øverste leder bestemt nivå for akseptabel risiko?	2 3.2	6.1.2	GRM-11			☐Ja ☐Nei	PJL § 22 HRL § 21 PVF artikkel 32 FLK § 5 og 6	☐Ja ☐Nei
6.	Har virksomhetens øverste leder bestemt regler for håndtering av risiko?	2	6.1.3	GRM-04			☐Ja ☐Nei	PJL § 23 HRL § 22 PLF § 6	☐Ja ☐Nei

() = Kravet kan ikke ivaretas av databehandler, men det aktuelle temaet dekkes av CCM Control ID.
* = Kravet i Normen er delvis dekket av CCM Control ID.

37.	Er følgende minimumskrav til konfidensialitet fastsatt?: Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger. • hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten • avgrense tilgang for autorisert personell iht. tjenstlig behov • ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerhet	3.2	(A.9.2*, A.10.1*, A.11.1*, A.11.2*, A.12.4* & A.13.2.4*)	AIS-01 IAM-04 IAM-07 IAM-08 EKM-01 DSI-07 DCS-02 HRS-03 HRS-06 IVS-01 IVS-09

Nr	Krav (formulert som spørsmål)	Kap. i Normen	Kap. i ISO 27001 og Annex A	CSA CCM Control ID	Systemkrav i behandlings-rettet helse-register	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)
79.	Sikrer virksomheten at den som gjør sine rettigheter gjeldende er identifisert?	4.2.3				
80.	Gis pasienten, som utgangspunkt innsyn i alle opplysninger i behandlingsrettet helseregister som omhandler seg selv? Dette gjelder også lydopptak, røntgenbilder, videoopptak etc.	4.2.3.1				
81.	Gir helsepersonell på anmodning forklaring på faguttrykk mv.?	4.2.3.1				
82.	Legges det til rette for at samiskspråklige, fremmedspråklige og personer med funksjonshemninger kan utøve innsynsretten?	4.2.3.1				
83.	Dokumenteres det at samiskspråklige, fremmedspråklige og personer med funksjonshemninger kan utøve innsynsretten?	4.2.3.1				

291.	Kartlegges også hvilke andre systemer og hvilken infrastruktur de klassifiserte systemene er avhengige av? Disse skal ha samme klassifisering og nivå for akseptabel risiko som for de klassifiserte systemene.	5.9	A.17.1*	BCR-09			☐Ja ☐Nei
292.	Har ledelsen fastsatt nivå for akseptabel risiko for tilgjengelighet for hver aktuell klassifisering, med minimum maksimal avbruddstid?	5.9	A.17.1*	(GRM-11)			☐Ja ☐Nei
293.	Har virksomheten etablert nødrutiner med utgangspunkt i klassifiseringen av informasjonssystemene for: • Alternativ drift uten bruk av informasjonssystemene • Alternativ drift med delvis støtte fra informasjonssystemene	5.9	A.17.1*	BCR-04 BCR-07 BCR-08 BCR-11			☐Ja ☐Nei
294.	Øves, testes, revideres og oppdateres nødrutinene minst en gang i året?	5.9	A.17.1*	BCR-02 BCR-11			☐Ja ☐Nei

() = Kravet kan ikke ivaretas av databehandler, men det aktuelle temaet dekkes av CCM Control ID.
* = Kravet i Normen er delvis dekket av CCM Control ID.