# Cloud audit og assurance initiativer

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Publikationen kan hentes
på IT- & Telestyrelsens
Hjemmeside: http://www.itst.dk
eller på digitaliser.dk/resource/703330

ISBN (internet): 978-87-92572-37-0

>

# Cloud audit og assurance initiativer

IT- & Telestyrelsen
januar 2011

## Indhold >


Indledning 5

Excecutive summery 6

Hvilke typer audit og assurance information har man adgang til i cloud computing 7
- Forskellige typer clouds giver forskellige muligheder 7
- Nogle typer audit og assurance information er man selv ansvarlig for at etablere eller konfigurere 10

Cloud audit og assurance initiativer 12
- SCAP - Security Content Automation Protocol 13
- CloudAudit og Cloud Security Alliance 14
- Cloud Trust 17
- ENISA Assurance Framework (EAF) 18
- ISACA Cloud Computing Management Audit/Assurance program 18
- FedRAMP 18
- CAMM 19
- ACEML (Automatic Compliance Expert Markup Language) 20
- Store cloud-leverandører 20
- Opsummering 21

Eksempler på tilgængelig audit information fra fire forskellige cloud-leverandører 22
- Amazon Web Services 22
- Google 24
- Salesforce 26
- Microsoft 28

# Indledning

>

Cloud-løsninger skal kunne revideres, så det løbende kan vurderes, om en cloud-leverandørs specifikke løsning er tilstrækkelig sikker til at kunne benyttes til et givent system eller løsning. En cloud-leverandør skal samtidig kunne give tilstrækkelig audit og assurance information til at opfylde både kundernes risikovurdering og eventuelle lovkrav.

Denne rapport præsenterer de generelle muligheder for adgang til sikkerhedsdokumentation i Infrastruktur-, Platform- og Software-as-a-Service løsninger. Informationen er primært relevant for *Public Clouds*, hvor infrastruktur og software er placeret hos en cloud tjenesteudbyder. *Private Clouds* er under kundens fulde kontrol, og giver derfor kunden de samme muligheder for audit og assurance information som de traditionelle ”ikke-cloud” baserede løsninger.

Det kan være vanskeligt for en kunde at vurdere, hvor meget audit information en given leverandør kan stille til rådighed. Det kan også være vanskeligt at vurdere, hvem der har ansvaret for at forskellige typer audit information er tilgængelig. Rapporten introducerer og vurderer derfor en række af de nuværende cloud audit-og assurance initiativer, der vil gøre det lettere at sammenligne mulighederne for adgang til sikkerhedsdokumentation hos forskellige cloud-leverandører.

For at kunne vurdere, hvilke muligheder en kunde har på nuværende tidspunkt, introduceres en oversigt over hvilken audit- og assuranceinformation fire specifikke cloud-leverandører, med forskellige typer cloud-løsninger, stiller til rådighed i dag.

Da audit og assurance initiativerne ved rapportens udgivelse er i de tidlige faser, er vurderingen af potentialet et øjebliksbillede som hurtigt vil forandres i takt med udviklingen på området. Rapporten vil derfor blive opdateret løbende efter behov.

# Executive summery >

Denne rapport belyser mulighederne for adgang til sikkerhedsdokumentation i forskellige typer cloud-løsninger og introducerer en række af de nuværende generelle cloud audit og assurance initiativer. Rapporten kan gøre det nemmere, at foretage en vurdering af, hvorvidt en leverandør tilbyder tilstrækkelig audit og assurance information til at opfylde kundernes risikovurdering og eventuelle lovkrav.

Det er i dag muligt at opnå tilstrækkelig information fra en række kvalificerede cloud-leverandører til at imødekomme danske behov for audit og assurance. På nuværende tidspunkt kan det dog kræve en række manuelle opgaver fra både kunden og cloud-leverandøren.

**Tilgængelig audit og assurance information**
En cloud leverandør kan grundlæggende stille tre forskellige typer audit og assurance information til rådighed for deres kunder:
1. Skriftlig dokumentation for procedure, standarder, politikker osv.
Tilgængelig leverandørdokumentation, leverandørcertificeringer som ISO 27001, PCI, COBIT, NIST 800-53, BS 25999 og revisionserklæringer kan ofte give tilstrækkelig information til at vurdere de meget standardiserede og automatiserede cloud-løsninger ud fra.
2. Konfigurationsinfo, dvs oplysninger om standardkonfigurationer og dokumentation for den aktuelle konfiguration af kundens systemer.
3. Løbende log- og monitoreringsinformation.

Man skal her være opmærksom på, at forskellige cloud-løsningern giver forskellige muligheder for adgang til konfigurations- og log/monitorieringsinformation. Typen af information som leverandøren kan stille til rådighed vil være afhængig af den type cloud der overvejes (IaaS, PaaS, SaaS). Adgang til audit og assurance information er primært leverandørens ansvar i SaaS-løsninger og et delt ansvar mellem leverandør og kunder i IaaS og PaaS-løsninger.

**Cloud-specifikke projekter**
En række projekter arbejder på at mappe cloud-specifikke sikkerhedsspørgsmål til de ovenfor nævnte standardrammeværk. Der arbejdes også på, at identificere cloud-specifikke spørgsmål, så kunder opnår tilstrækkelig viden og dokumentation for de specifikke løsninger uden at skulle opfinde spørgsmålene hver gang. Cloud-leverandørerne kan ligeledes besvare og dokumentere de mest almindelige og relevante spørgsmål på forhånd, hvorved deres belastning lettes.

For at begrænse de mange manuelle opgaver og processer arbejder flere projekter på at standardisere, og på sigt automatisere, indsamlingen af audit og assurance information. Endelig kan projekter etablere en ”forhåndsgodkendelse” eller forhåndsvurdering af specifikke cloud-løsninger.

Målet er, at opnå en løbende overvågning og vurdering af cloud-leverandørens infrastruktur, for at vise at leverandøren overholder egne sikkerhedspolitikker.

Området er i hastig udvikling. Dette dokument giver derfor en status på de mest relevante initiativer og et overblik over de nuværende audit og assurancemuligheder hos en række cloud-leverandører.

# Hvilke typer audit og assurance information har man adgang til i cloud computing >

En cloud leverandør skal kunne give tilstrækkelig audit og assurance information til at opfylde både kundernes risikovurdering og eventuelle lovkrav.
Audit information kan inddeles i information man selv har kontrol over (f.eks. opsætning af applikationslogning på en virtuel maskine), og information som man er afhængig af, at cloud-leverandøren kan - eller vil - stille til rådighed (f.eks. dokumentation for fysiske sikkerhed og underliggende procedurer og system konfigurationer).

## Forskellige typer clouds giver forskellige muligheder

Det er vigtigt at være opmærksom på de forskellige muligheder for adgang til audit og assurance information der naturligt eksisterer indenfor de forskellige typer af cloud-tjenester.

### De tre forskellige typer cloud tjenester

Cloud tjenester kan opdeles i tre grundlæggende modeller, opdelingen kaldes også ”SPI-modellen”, hvor SPI refererer til henholdsvis Software, Platform og Infrastruktur som en tjeneste.


***Software as a Service (SaaS)***

I SaaS-løsninger får man som kunde adgang til en software løsning, hvor man kan administrere egne brugere og egen data. Man har ikke administratoradgang til operativsystemet eller applikationen som sådan, men kan frit ændre visse funktionaliteter i de applikationer man benytter.

***Platform as a Service (PaaS)***

I PaaS-løsninger får man som kunde adgang til et operativ- og databasesystem, hvor man kan installere og administrere egne programmer. Man har ikke administratoradgang til operativsystemet, men kan frit udvikle funktionaliteter (eller tilkøbe) egne applikationer.

***Infrastructure as a Service (IaaS)***

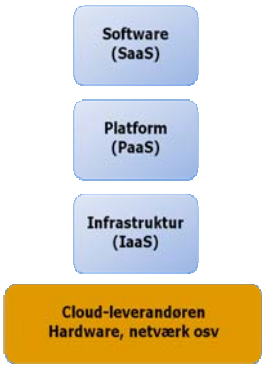
I IaaS-løsninger får man som kunde adgang til et virtualiseret miljø, hvor man kan installere og administrere virtuelle maskiner. Man har administratoradgang til egne virtuelle maskiner og kan frit udtrække information fra egne virtuelle maskiner, som om de stod i eget datacenter.

***Cloud-leverandøren***

Cloud-leverandøren har som minimum altid ansvaret for hosten (den underliggende fysiske server), hardwaren, netværksenheder og naturligvis de fysiske bygninger. Alle procedurer omkring driften af hardwaren er altid cloud-leverandørens ansvar.
Jo mere man bevæger sig fra Infrastruktur over Platform til Software as a Service til Software as a Service, jo flere ting har cloud-leverandøren ansvaret for at både administrere og stille funktionalitet til rådighed for kunderne.

>

**Forskellige muligheder i de tre forskellige typer tjenester**




I "Infrastructure as a Service" har man flere muligheder for selv at opsætte, konfigurere og installere tredjeparts programmer for egne virtuelle servere, f.eks. ved at installere egne overvågningsprogrammer.
I Platform as a Service kan man stille krav til hvilke logningsfaciliteter ens egne programmer skal opfylde, hvorimod man i en "Software as a Service" løsninger er afhængig af de logs og overvågningsfunktionaliteter, som en specifik leverandør stiller til rådighed.

Adgang til audit og assurance information er derfor primært leverandørens ansvar i SaaS-løsninger og et delt ansvar mellem leverandør og kunder i IaaS og PaaS-løsninger.

**En cloud leverandør kan grundlæggende stille tre forskellige typer audit og assurance information til rådighed for deres kunder:**

1. Dokumentation for procedure, standarder, politikker osv.
2. Konfigurationsinfo, dvs oplysninger om standardkonfigurationer og dokumentation for aktuel konfiguration af kundens systemer.
3. Løbende log- og monitoreringsinformation.

**1. Dokumentation for procedure, standarder, politikker osv.**
Formelle sikkerhedspolitikker og procedurer ændrer sig sjældent. Har man først verificeret, at der er etableret kameraovervågning i et datacenter, eller at der er etableret en formel procedure for at håndtere brud på sikkerheden, behøver man normalt ikke at checke hver dag om det stadig er tilfældet.

Man kan derfor læne sig opad en generel revisionserklæring for cloud-leverandøren, i USA typisk en SAS70 erklæring, og derigennem i det mindste vurdere om erklæringen er tilstrækkelig dækkende. Sammen med en vurdering af eventuelle sikkerhedscertificeringer o.lign. og specifikke uddybende spørgsmål, kan man i mange tilfælde opnå en tilfredsstillende grad af viden om de underliggende procedurer, politikker osv. uden selv at kende dem i detaljer.

*Forstå hvad der har indgået i vurderingen*
For at vurdere en SAS70 erklæring eller en ISO 27001/2 certificering er det nødvendigt at vide præcist, hvad der er vurderet, og hvad man erklærer sig om; principielt kan man få lavet en revisionserklæring der verificerer, at man har valgt ikke at have sikkerhedskontroller.
De fleste leverandører giver adgang til baggrundsmateriale, ofte imod underskrivelse af en fortrolighedserklæring.

I traditionelle hosting- og outsourcingløsninger får mange kunder udført en specifik revisionserklæring for kundens egne systemer hos leverandøren, sammen med den generelle erklæring. It-revisoren verificerer så i den forbindelse om outsourcing-

leverandøren f.eks. lever op til kontraktens krav, og om leverandørens generelle procedurer følges for kundens systemer.

*Cloud computing er en standardiseret og automatiseret ydelse*
I traditionelle hosting- og outsourcingløsninger arbejder navngivne personer direkte på de specifikke kunder-systemer som de er ansvarlige for. Dermed er der en række procedurer og specifikke opgaver der kan revideres. I cloud-løsninger er dette helt anderledes.

Som regel er cloud-løsninger standardiserede og de fleste arbejdsopgaver er fuldt automatiserede, det er således ikke udsædvanligt med én administrator for 10-, 20- eller 30.000 fysiske maskiner. Det giver derfor ikke mening, at revidere alle cloud-kundernes systemer individuelt i cloud datacenterne.

Hvis man kan opnå tilstrækkelig viden igennem en vurdering af revisionserklæringer, sikkerhedscertificeringer, og evt. supplerede spørgsmål til leverandørerne, er der ikke behov for selv at få foretaget en fysisk inspektion af cloud-datacentret.

**2. Konfigurationsinfo (standardkonfigurationer og specifik information for udvalgte systemer)**

Systemopsætninger ændres nogle gange. En kunde kan f.eks. vælge at ændre på kravene til brugernes passwords i en SaaS-løsning, eller firewall regler kan ændres i forbindelse med test eller omkonfigurationer.
Det kan være en god ide jævnligt at foretage et check af, om systemerne er konfigureret som forventet. Og i forbindelse med en gennemgang af sikkerheden kan det være nødvendigt, at dokumentere om de specifikke konfigurationer for et – eller alle – kundens cloud-systemer er stærke nok.

I mange tilfælde er det i dag primært kundens eget ansvar at udtrække dokumentation for opsætningen, men flere initiativer arbejder på at lette arbejdet igennem automatisering af opgaverne.

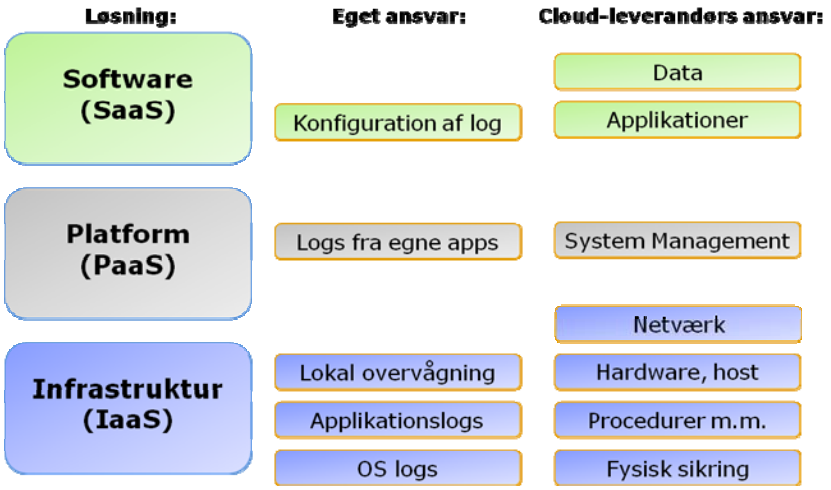
**3. Log og monitoreringsinformation**

Log og monitoreringsinformation er dynamisk information, der typisk ændrer sig hele tiden. For at kunne afsløre uautoriserede handlinger skal der logges, så man kan opdage og undersøge uønskede forhold. Løbende overvågning skal sikre, at sikringsforanstaltningerne fungerer efter hensigten.

Det kan tage tid at opdage og efterforske en potentiel hændelse. Vær opmærksom på hvor længe informationen gemmes og om informationen skal læses online i leverandørens portal, eller om der skal være API'er til at udtrække informationen til rådighed.

>

**Nogle typer audit og assurance information er man selv ansvarlig for at etablere eller konfigurere**



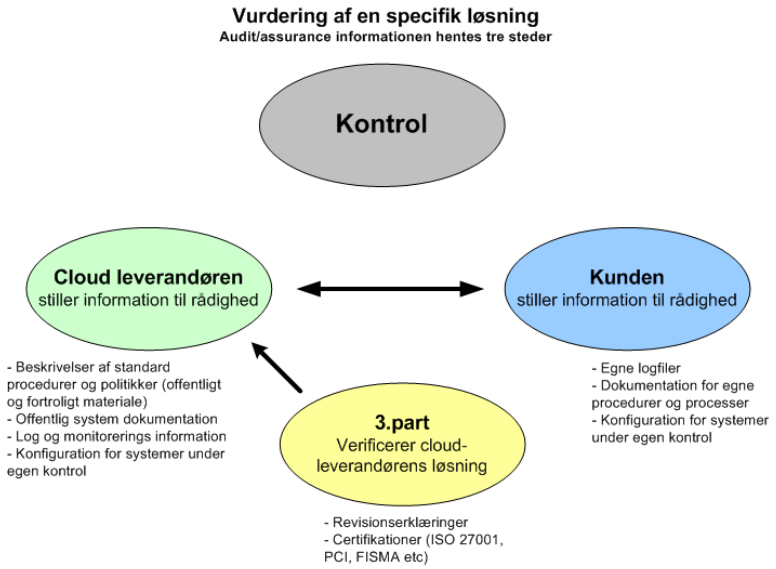

Figur 3 Delt ansvar mellem leverandør og kunden

*Cloud-leverandørens ansvar:*
Uanset hvilken løsning der overvejes, skal cloud-leverandøren altid kunne dokumentere den fysiske sikkerhed, de underliggende politikker, procedurer og konfigurationer, så både kundernes risikovurdering og eventuelle lovkrav opfyldes. For konfiguration- og loginformation er den tilgængelige information afhængig af typen af løsning (IaaS, PaaS, or SaaS) og funktionalitet som den enkelte leverandør tilbyder.

*Kundens eget ansvar:*
Vær opmærksom på hvad du som kunde selv er ansvarlig for. I en SaaS-løsning skal man muligvis konfigurere hvad der skal logges, eller sikre at kontrakten beskriver hvor længe logfiler skal gemmes. I en IaaS-løsning skal man selv definere logning i opertivsystemet og de applikationer man installerer, cloud-leverandøren har normalt ikke adgang til at gøre det for en.

I praksis er audit og assurance information således tilgængelig fra tre forskellige kilder: Materiale og information som cloud-leverandøren stiller til rådighed, materiale der er udarbejdet af en 3.part, f.eks. revisionserklæringer og leverandørcertificeringer og endelig materiale kunden selv har ansvaret for.

>




Figur 4 Audit information er tilgængelig fra flere forskellige kilder

# Cloud audit og assurance initiativer >

Der er i dag en stor del manuelle opgaver forbundet med at vurdere sikkerheden i cloud-løsninger. Der skal udtrækkes information og dokumentation fra konsoller, der skal findes information på cloud-leverandørernes portaler, holdes møder med leverandørerne osv.
Samtidig skal vurderingerne gentages, med forskellig grad af grundighed, af både cloud-leverandørene og kunderne, hver gang en ny kunde overvejer en ny cloud-løsning.

En række initiativer arbejder derfor i øjeblikket på at standardisere typen af tilgængelig information og standardisere adgangen til audit og assurance information igennem åbne standarder og igennem formelle krav til cloud-leverandørerne.

Initiativerne inddeles i det efterfølgende afsnit i følgende kategorier:

*Overordnede, ikke cloud specifikke, rammeværk*
Overordnede rammer som NIST 800-53, ISO 27001, PCI, COBIT og FISMA giver en række krav til overordnede sikkerhedskontroller, f.eks. krav som adgangs kontrol, awareness og fysisk sikkerhed. Rammeværkene stiller en række audit-krav, som en kunde potentielt skal kunne verificere finder sted.
De amerikanske cloud-leverandører vil ofte benytte NIST 800-53 som internt rammeværktøj og vil dermed tilpasse deres interne kontroller til projektet, men også ISO 27001 og PCI krav er udbredte på nuværende tidspunkt.

*Rammeværk med cloud fokus*
Da de overordnede rammeværk er skrevet inden cloud computing blev udbredt, dækker de ikke cloud-specifikke områder og tager ikke stilling til forskellene i IaaS, PaaS og SaaS-løsninger eller de væsentlige forskelle mellem public/private/community/hybrid cloud løsninger.
Der er derfor udarbejdet flere rammeværk, der er cloud-specifikke. Typisk indeholder de best practice krav og evt. specifikke spørgsmål en kunde kan stille sin cloud-leverandør. Kravene kan være mappet til et eller flere af de overordnede rammeværk og kan have forskellige fokusområder. Fælles er, at rammeværkene kan bruges som udgangspunkt for en vurdering af en specifik cloud-løsning.

*Automatiseret indsamling af audit og assurance information*
Andre projekter, som SCAP, fokuserer på at automatisere indsamlingen af audit informationen. Man kan dermed slippe for de mange manuelle processer som kunder og leverandøren skal igennem i dag.

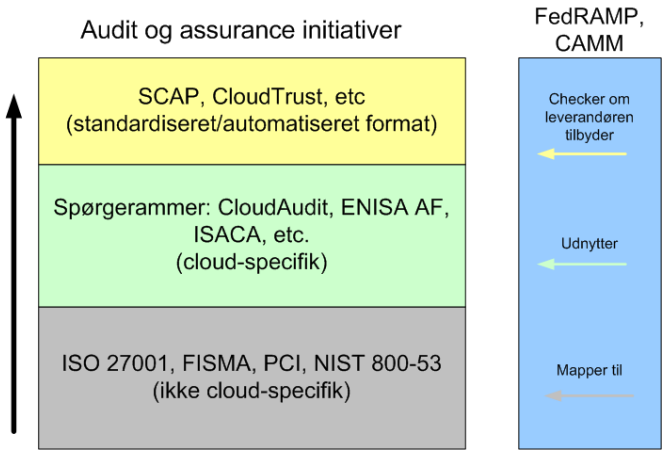
Indsamlingen af audit informationen kan potentielt automatiseres på to forskellige måder:

- ”On demand” audit information, hvor kunden initierer overførslen af information fra leverandøren når informationen er ønsket (”pull”).
- Løbende overførsel af audit og assurance dokumentation fra leverandøren til kunden (”push”).

Det må forventes, at forskellige cloud-leverandører vil tilbyde forskellige typer audit/assurance information, og at de praktiske implementeringer vil være forskellige.

>

*Nationale certificerings initiativer*
FedRAMP og CAMM vil bl.a. kunne pre-kvalificere eller certificere specifikke cloud løsninger, så ens egen vurdering af en løsning kan gennemføres hurtigere.
CAMM og FedRAMP arbejder ligeledes på at gøre det muligt at sammenligne leverandører direkte, og dermed gøre det væsentligt lettere at vurdere hvilke audit og assurance data der er tilgængelige.




## SCAP - Security Content Automation Protocol

SCAP (Security Content Automation Protocol) er en række standarder og specifikationer fra NIST til standardisering af format og navngivning af rapportering af information om bl.a. specifikke sikkerhedskonfigurationer. Det kunne f.eks. være at ”Systemet er konfigureret til at kræve et password på mindst 8 tegn” eller "Microsoft Windows XP (32-bit) SP2 er installeret”.

**Link:**
http://scap.nist.gov

**Tilgængeligt materiale**:
NIST Special Publication 800-117 (Draft), maj 2010:
http://csrc.nist.gov/publications/drafts/800-126-r1/second-public-draft_sp800-126r1-may2010.pdf

**Status**
Deadline for kommentarer til den nuværende version (second public draft SP 800-126 Revision 1) var 28/6 2010.
Tidslinien for projektet kan findes her: http://scap.nist.gov/timeline.html.
Projektet videreudvikles aktivt og flere interessenter, herunder Cloud Security Alliance, har meldt ud, at de planlægger at deltage aktivt i udviklingen af projektet da det kan komplimentere automatiseret indsamling af mere overordnet assurance information.

>

## CloudAudit og Cloud Security Alliance

CloudAudit oplyser, at man har over 250 deltagere/interessenter. Projektet har været aktivt siden januar 2010 og afholder ugentlige møder. Alle er velkomne til at deltage i projektet, i praksis sker det ved at deltage i dial-in møder via WebEx, telefonnumre offentliggøres på projektets hjemmeside.
CloudAudit blev i oktober 2010 et officielt projekt under non-profit organisationen Cloud Security Alliance (CSA), se http://www.cloudsecurityalliance.org.

Projektet arbejder aktivt med repræsentanter fra alle store cloud-leverandører.
På hjemmesiden listes navngivne medlemmer af CloudAudits core team fra bl.a.: SUN, CSC, Akamai, Microsoft, Cisco, VMware, Google, Unisys, Amazon og Rackspace.

På nuværende tidspunkt er der god momentum i projektet. Materialet fra CloudAudit indgår i en række andre projekter og igennem Cloud Security Alliance samarbejdes der med bl.a. ENISA og en række andre organisationer.

**Link:**
http://www.cloudaudit.org

**Projektbeskrivelse:**
Målet er at danne fælles namespace og interfaces med simple åbne protokoller med god autentifikation, til at give standardiseret adgang til "Audit, Assertion, Assessment, and Assurance" information. Cloud-leverandøren åbner for adgangen til informationen deres kunder, ekstern revision osv.
Simple eksempler kan ses på http://cloudaudit.net/.well-known/cloudaudit/.

Som eksempel på en kontrol mappet til et overordnet rammeværk, siger sektion 15.3.1 i ISO 27001, at revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede.
Hvis en cloud-leverandør understøtter CloudAudit kan en kunde verificere om informationen er tilgængelig igennem nedenstående eksempel fra
https://tools.ietf.org/html/draft-hoff-cloudaudit-00

```
GET /.well-known/cloudaudit/service//org/iso/27002/v2005/15/3/1 HTTP/1.1
Host: cloud.example.com
HTTP/1.1 200 OK
Content-Length: 822
Content-Type: text/html

 <html>  <body>  <head>
<title>ISO 27002 v2005 15.3.1</title> </head>
<H1>Information systems audit controls</H1>
<UL>
<LI><a href="http://www.cloudhosting.com/.well-
known/cloudaudit/org/iso/27002/v2005/15/3/1/auditschedule.xls">Audit Schedule</a> -
<i>the 2010 audit schedule for cloud hosting inc.</i>
<LI><a href="http://www.cloudhosting.com/.well-
known/cloudaudit/org/iso/27002/v2005/15/3/1/contract.pdf">KPWEY LLP Audit Contract</a> -
<i>The audit contract with KPWEY for external audit services</i> - <span>The document
details the services procured to support the audit plan; see page 14 for specific
details.</span>
<LI><a href="http://www.cloudhosting.com/.well-
known/cloudaudit/org/iso/27002/v2005/15/3/1/auditscope.zip">Audit Scope</a> - <i>The audit
scope for the planned audits in 2010</i>
</UL>
</body>
</html>
```

>

CloudAudit projektet er samlet i CSA's "Cloud GRC (Governance, Risk management and Compliance) Stack", der inkluderer CloudAudit, CSA Cloud Controls Matrix og CSA Consensus Assessments, som er beskrevet nedenfor.

CSA har overvejet at kombinerer CloudAudit projektet med bl.a. *SCAP* projektet og lave en samlet automatiseret og standardiseret adgang til omfattende audit og assurance information. SCAP kan give information om konfiguration og sårbarheder mens CloudAudit giver information om f.eks. overholdelse af krav i sikkerhedsstandarder (assertations).
På nuværende tidspunkt (december 2010) vil CSA dog overlade udviklingen af selve automatiseringen til andre projekter. CloudAudit standarderne vil dog sandsynligvis indgå som en naturlig del af projekterne.

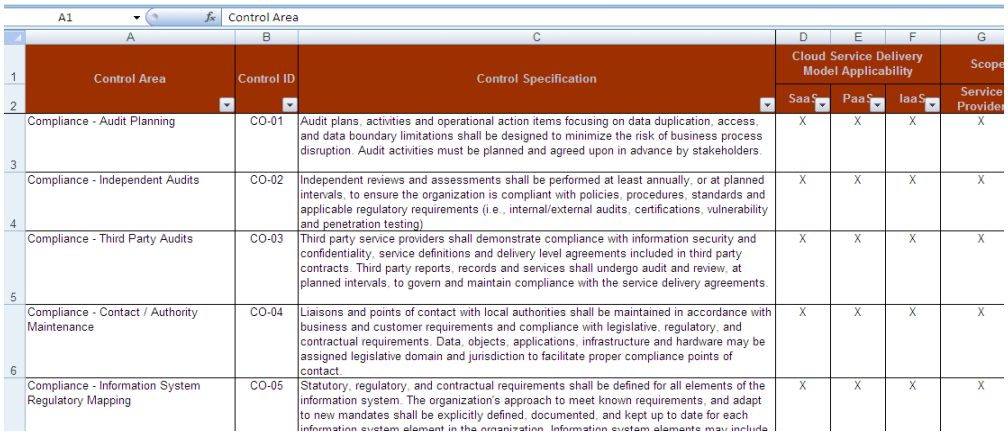
**Cloud Controls Matrix:**
Cloud Security Alliances "*Controls Matrix*" (CCM) er et overordnet cloud-security kontrol-rammeværk. Det er lavet for at give en række grundlæggende sikkerhedsprincipper en cloud-leverandør skal kunne opfylde, og samtidig hjælpe cloud-kunder til at kunne vurdere sikkerheden hos en specifik leverandør.

Rammeværket er opbygget efter Cloud Security Alliances 13 domæner (http://www.cloudsecurityalliance.org/csaguide.pdf) og er mappet til generelle rammeværk som ISO 27001/27002, ISACA COBIT, PCI DSS, HIAA, NIST 800-53 og FedRAMP. Det planlægges at udvide projektet med andre relevante frameworks, f.eks. *CAMM*, når de er relevante.

*Eksempel fra CSA Controls Matrix:*

**Compliance - Independent Audits**
Control ID: CO-02
Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)
**Compliance Mapping:**
COBIT: 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6
HIPAA: 45 CFR 164.308 (a)(8), 45 CFR 164.308(a)(1)(ii)(D)
ISO/IEC 27002-2005: 4.2.3e, 5.1 g, 5.2.1 d), 6, A.6.1.8
NIST SP800-53 R3: NIST SP800-53 R3 CA-1, CA-2, CA-6, RA-5
FedRAMP: NIST SP800-53 R3 CA-1, CA-2, CA-2 (1), CA-6, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (9), RA-5 (6)PCI DSS v2.0: 11.2, 11.3, 6.6, 12.1.2.b
BITS: SIG v6.0: L.2, L.4, L.7, L.9, L.11
GAPP: GAPP Ref 1.2.5, 1.2.7, 4.2.1, 8.2.7, 10.2.3, 10.2.5

>



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Control Area | Control ID | Control Specification | Cloud Service Delivery Model Applicability | | | Scope |
| 2 | | | | SaaS | PaaS | IaaS | Service Provider |
| 3 | Compliance - Audit Planning | CO-01 | Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders. | X | X | X | X |
| 4 | Compliance - Independent Audits | CO-02 | Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing) | X | X | X | X |
| 5 | Compliance - Third Party Audits | CO-03 | Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements. | X | X | X | X |
| 6 | Compliance - Contact / Authority Maintenance | CO-04 | Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact. | X | X | X | X |
| | Compliance - Information System Regulatory Mapping | CO-05 | Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each | X | X | X | X |

Fig.6 Cloud Security Alliance Cloud Controls Matrix

**Consensus Assessment Initiative Questionnaire:**
Consensus Assessment Initiative Questionnaire (CAIQ) er en spørgeliste i regnearksformat, der giver en række ja/nej spørgsmål, som en kunde eller revisor kan vælge at stille til en Iaas, Paas og SaaS cloud-leverandør.

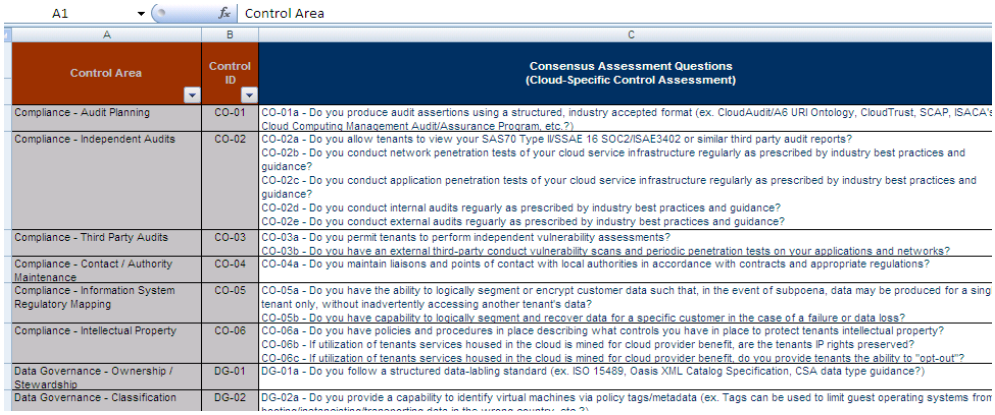
Dokumentet komplimenterer CCM-dokumentet ovenfor og er i praksis et udtræk af hovedområder, best practices og kontroller fra CSA's øvrige dokumenter, og er udarbejdet for at hjælpe organisationer til at kunne vurdere cloud-leverandørenes sikkerhed i praksis.

Dokumentet mapper til "Kontrol Område" og "Kontrol ID"-kolonnerne i Cloud Controls Matrix dokumentet beskrevet ovenfor.

*Eksempel fra CAIQ:*

```
Compliance - Independent Audits
Control ID: CO-02
CO-02a - Do you allow tenants to view your SAS70 Type II/SSAE 16
SOC2/ISAE3402 or similar third party audit reports?
CO-02b - Do you conduct network penetration tests of your cloud
service infrastructure regularly as prescribed by industry best
practices and guidance?
CO-02c - Do you conduct application penetration tests of your cloud
service infrastructure regularly as prescribed by industry best
practices and guidance?
CO-02d - Do you conduct internal audits regularly as prescribed by
industry best practices and guidance?
CO-02e - Do you conduct external audits regularly as prescribed by
industry best practices and guidance?
CO-02f - Are the results of the network penetration tests available to
tenants at their request?
CO-02g - Are the results of internal and external audits available to
tenants at their request?
```

>



| Control Area | Control ID | Consensus Assessment Questions (Cloud-Specific Control Assessment) |
|---|---|---|
| Compliance - Audit Planning | CO-01 | CO-01a - Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP, ISACA's Cloud Computing Management Audit/Assurance Program, etc.?) |
| Compliance - Independent Audits | CO-02 | CO-02a - Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?<br>CO-02b - Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?<br>CO-02c - Do you conduct application penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?<br>CO-02d - Do you conduct internal audits regularly as prescribed by industry best practices and guidance?<br>CO-02e - Do you conduct external audits regularly as prescribed by industry best practices and guidance? |
| Compliance - Third Party Audits | CO-03 | CO-03a - Do you permit tenants to perform independent vulnerability assessments?<br>CO-03b - Do you have an external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks? |
| Compliance - Contact / Authority Maintenance | CO-04 | CO-04a - Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? |
| Compliance - Information System Regulatory Mapping | CO-05 | CO-05a - Do you have the ability to logically segment or encrypt customer data such that, in the event of subpoena, data may be produced for a sing tenant only, without inadvertently accessing another tenant's data?<br>CO-05b - Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss? |
| Compliance - Intellectual Property | CO-06 | CO-06a - Do you have policies and procedures in place describing what controls you have in place to protect tenants intellectual property?<br>CO-06b - If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?<br>CO-06c - If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to "opt-out"? |
| Data Governance - Ownership / Stewardship | DG-01 | DG-01a - Do you follow a structured data-labling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance?) |
| Data Governance - Classification | DG-02 | DG-02a - Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from |

Fig.7 Cloud Security Alliance Cloud Consensus Assessment Questions

**Tilgængeligt materiale:**
Materialet kan downloades fra CloudAudit og Cloud Securty Alliance's hjemmesider: http://www.cloudsecurityalliance.org/grcstack.html
CloudAudit 1.0 er sendt til IETF som draft: https://tools.ietf.org/html/draft-hoff-cloudaudit-00

## Cloud Trust

CloudTrust var oprindeligt et initiativ iværksat af firmaet CSC, og det oprindelige arbejde er indgået i CloudAudits protokol.
Der har over det sidste år været et omfattende samarbejde mellem CSC og Cloud Security Alliance, og det ser i øjeblikket (december 2010) ud til at navnet "Cloud Trust" samles under Cloud Security Alliance. Projektet er dog endnu ikke officielt annonceret.

Cloud Trust har været overvejet som en samlet pakke under Cloud Security Alliance med metode, inklusive protokoller og interfaces, fra bl.a. *CloudAudit* og *SCAP*, så en cloud-leverandør løbende kan dele audit og compliance information med deres kunder.
På nuværende tidspunkt ser det dog ud til, at Cloud Security Alliance overlader organiseringen af indsamling af den løbende, automatiserede indsamling af audit data til andre projekter.

Se http://wiki.cloudaudit.org/working-groups/standards/continuous-monitoring for mere information.

## ENISA Assurance Framework (EAF)

EU organisationen ENISA (European Network and Information Security Agency) udgav i 2009 et cloud computing assurance framework og udgiver en rapport om brug af cloud computing i det offentlige.
ENISA er også aktiv i *CAMM*-projektet nedenfor og det må forventes, at CAMM på sigt overtager EAF's rolle.

**Link:**
https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

## ISACA Cloud Computing Management Audit/Assurance program

Organisationen ISACA (Information Systems Audit and Control Association) arbejder med IT Governance. ISACA's audit/assurance program er et værktøj der kan benyttes som roadmap og template til gennemførsel af en revision af en cloud-leverandør, eller en revision af en virksomheds brug af en specifik cloud-løsning.

Rammen beskriver en række opgaver der kan udføres i en it-revision, best practices og krav til compliance, men er ikke tænkt som en checkliste eller et spørgeskema.

**Tilgængeligt material:**
Materialet kan downloades gratis for medlemmer af ISACA eller købes igennem http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Management-Audit-Assurance-Program.aspx

De store revisonsfirmaer udvikler deres egne cloud-revisionsmaterialer, men det er sandsynligt at ISACA materiale vil påvirke mange interne og eksterne it-revisorer. Det er derfor sandsynligt, at materialet vil påvirke de typer information cloud-leverandørerne vil stille til rådighed.
ISACA vil dog komme til at opdatere deres materiale efterhånden som CloudAudit og andre projekter udvikles.

## FedRAMP

FedRAMP (Federal Risk and Authorization Management Program) er etableret som en standardiseret tilgang for amerikanske offentlige myndigheder, til at vurdere cloud tjenester og cloud produkter.
Tanken er, at en cloud-leverandør formelt forhåndsgodkendes én gang af FedRAMP fra centralt hold, hvorefter alle offentlige amerikanske virksomheder kan benytte tjenesten, uden at skulle gentage den samme sikkerhedsgennemgang hver gang.

FedRAMP projektet vil beskrive sikkerhedskrav, der dækker alle offentlige myndigheder i USA, herunder krav til cloud-leverandørene om løbende overvågning

og rapportering af sikkerhedsstatus til FedRAMP. Cloud-leverandører vil her kunne benytte projekter som CloudAudit til at levere den krævede information.

**Link:**
http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP

**Status:**
Der arbejdes i øjeblikket (december 2010) intensivt på at udvikle FedRAMP.
Den første version blev mødt af en del kritik, herunder at den var for fokuseret på SaaS-løsninger, og det må forventes, at de kommende versioner vil være væsentlig anderledes end den nuværende.
Det må forventes, at alle amerikanske cloud-leverandører vil arbejde imod en pre-kvalifikation fra FedRAMP.

Eksempler på diskussion og kritik af første version:
- http://www.rationalsurvivability.com/blog/?p=2723
- http://blog.isc2.org/isc2_blog/2010/11/fedramp-series-cloud-computing-security-requirement-baseline.html
- http://blog.isc2.org/isc2_blog/2010/11/fedramp-series-continuous-monitoring.html

## CAMM

CAMM (Common Assurance Maturity Model) er et samarbejde med deltagelse af bl.a. ENISA og Cloud Security Alliance.
Målet er, at etablere en ramme, med en række spørgsmål en potentiel kunde kan stille til en cloud-leverandør. CAMM refererer til bl.a. ISO 27001 og COBIT, dvs eksisterende certifikationer kan genbruges. Kontroller i CAMM er ligeledes mappet til de mest kendte cloud frameworks, som CloudAudit.

Europæiske ENISA planlægger bl.a. at bruge CAMM, som det amerikanske FedRAMP projekt, til at harmoniserer offentlige organisationers krav til cloud-leverandørerne.

**Tilgængeligt materiale:**
Projektets hjemmeside: http://common-assurance.com

**Roadmap:**
ENISA planlægger at frigive første version af CAMM i Q1 2011, sammen med en opfølgende rapport om cloud computing.

Det må forventes, at projektet, med stor involvering af bl.a. ENISA og Cloud Security Alliance, bliver et de vigtige projekter i Europa.

>

## ACEML (Automatic Compliance Expert Markup Language)

ACEML er et projekt under Open Group.

**Projektets egen beskrivelse:**
Standarden for Automated Compliance Expert Markup Language (ACEML) skal gøre det muligt for virksomheder at automatisere security compliance for deres systemer på en konsistent måde så der opnås compliance med applicable regulations sammen med store besparelser. IT-revisorer vil kunne udføre konsistente og mere komplette revisioner på kortere tid og til lavere pris.

**Link:**
http://opengroup.org

**Offentliggjort materiale:**
Draft:
https://www.opengroup.org/projects/security/ace/protected/uploads/30/22803/ts_aceml_crdraft.doc (kræver tilmelding)

**Status:**
Projektet har været sendt til review som draft standard til 28. September 2010. Efter gennemgang af ændringsforslag sendes standarden til Open Groups Board of Governors for godkendelse til at offentliggøre ACEML som en Open Group teknisk standart.

ACEML har fået mindre opmærksomhed end en række af de øvrige initiativer og det anses i øjeblikket mindre sandsynligt, at ACEML vil opnå udbredelse blandt de store cloud-leverandører.

## Store cloud-leverandører

De store cloud-leverandører, som Microsoft, Amazon og Google, tilbyder i dag alle forskellige muligheder for adgang til audit og assurance information, herunder logdata.
De store leverandørers særlige interfaces, protokoller eller nye typer assurance data kan blive de facto standarder blandt andre cloud-leverandører.

>

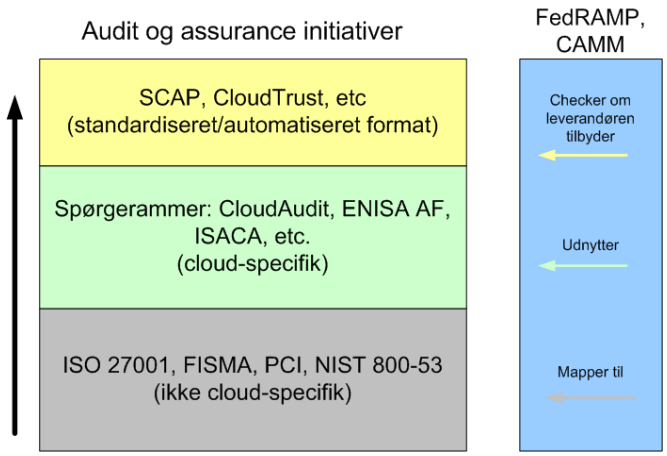
## Opsummering

Det er i dag muligt at opnå tilstrækkelig information til at imødekomme danske behov for audit og assurance. På nuværende tidspunkt kan det dog kræve en række manuelle opgaver fra både kunden og cloud-leverandøren.

Standard rammeværk og certificeringer som *ISO27001, PCI, COBIT, NIST 800-53, BS 25999* osv. giver en baseline, som cloud-løsningerne kan vurderes ud fra. Og en række projekter arbejder på at mappe cloud-specifikke spørgsmål til standard rammeværkene, og give cloud-specifikke spørgsmål. Derved opnår kunderne tilstrækkelig viden og dokumentation for de specifikke løsninger uden at skulle opfinde spørgsmålene hver gang. Cloud-leverandørerne kan ligeledes finde svar og dokumentation for de mest almindelige og relevante spørgsmål på forhånd, hvorved deres belastning lettes.

Projekter som *SCAP* og *CloudTrust* arbejder på at standardisere, og på sigt automatisere, indsamlingen af materiale. Derved slipper kunder og leverandører for mange af de manuelle processer.

Endelig kan projekter som *CAMM* og *FedRAMP* gøre det muligt at sammenligne cloud-leverandører og bl.a. pre-kvalificere specifikke cloud-løsninger.
Ens egen vurdering af løsningen, herunder en vurdering af hvilke audit og assurance data der er tilgængelige, kan således gennemføres hurtigere.



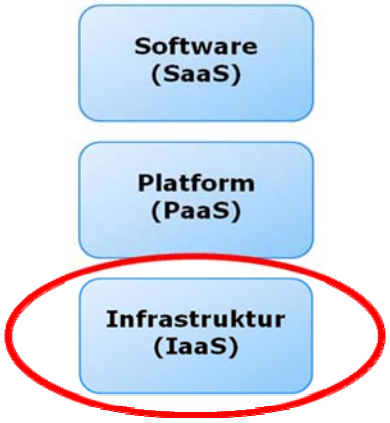

Se også hjemmesiden http://cloud-standards.org for en oversigt over igangværende projekter indenfor standardisering af cloud-ydelser, herunder indenfor audit og assurance.

Se det efterfølgende afsnit for en gennemgang at aktuelle muligheder for at få audit og assurance information fra fire store cloud-leverandører.

# Eksempler på tilgængelig audit information fra fire forskellige cloud-leverandører >

## Amazon Web Services

Amazon leverer Intrastructure as a Service (IaaS) løsninger.




Audit og assurance-information gøres tilgængeligt på Amazons hjemmeside under portalen AWS Security Center:
http://aws.amazon.com/security

Se f.eks. nedenstående links og dokumenter:
http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf
http://awsmedia.s3.amazonaws.com/Whitepaper_Security_Best_Practices_2010.pdf
http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf
http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

Amazons portal udbygges løbende med assurance specifik information.

**Dokumentation for underliggende procedure, standarder, politikker**
Adgang til Amazons fulde SAS70 rapport kan opnås ved at underskrive en non-disclosure aftale (NDA). Amazon er desuden ISO 27001 certificeret.
Amazon.com er Safe Harbor certificeret, certificeringen inkluderer Amazon Web Services http://safeharbor.export.gov/companyinfo.aspx?id=9319.

**Adgang til konfigurationsinformation**
Da Amazon ikke tilgår kundernes systemer er det Amazons holdning, at det er kundernes eget ansvar at udtrække dokumentation for opsætningen fra Management Console. Yderligere konfigurationsinformation kan fås ved at benytte Amazon Cloudwatch http://aws.amazon.com/cloudwatch.

Opsætning af den fysiske hardware og hypervisor, der er under Amazons ansvar, er overordnet dokumenteret i sikkerhedsdokumentationen. Yderligere specifik information kan normalt indhentes ved at kontakte Amazons technical support.
Da Amazon er en IaaS-løsning kan kunderne naturligvis altid udtrække information fra kundens egne virtuelle servere.

>

**Adgang til log og monitoreringsinfo**
Logning kan aktiveres for hver enkelt service i Amazon igennem kundens Management Console samt igennem API'er.
F.eks. kan en "Amazon S3 bucket" konfigureres til at logge adgangen til bucket'en og hvert objekt deri. Når kunden aktiverer logning, samles logfilerne i den bucket det specificeres, der skal logges til. Ligeledes kan man, når man opretter eller ændrer en CloudFront distribution, slå access logning til, hvorefter loginformation skrives til den S3-bucket man specificerer.

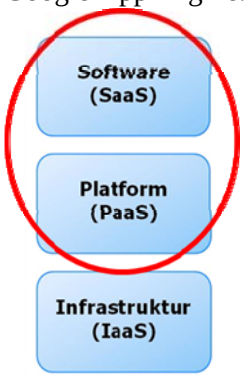
Ved at benytte Amazon CloudWatch gives der adgang til yderligere udvidet logning. Se f.eks.
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/index.html?using-cloudwatch.html

**Deltagelse i audit initiativer**
Amazon oplyser, at man aktivt deltager i flere initiativer, men at det af juridiske årsager ikke offentliggøres, hvilke specifikke projekter det drejer sig om eller status for arbejdet.
Amazon oplyser, at man har integreret interne kontroller med industri-definerede cloud control objektives og specifikke kontroller, som de der offentliggøres af Cloud Security Aliance og NIST.
Amazons cloud er certificeret som PCI Level 1 compliant. Systemer, der benytter løsningen skal naturligvis selv certificeres, hvis de er underlagt krav om PCI-certificering.

>

## Google

Google leverer Software as a Service tjenester, samt Platform as a Service igennem Google App Engine.




Audit og assurance-information er tilgængelig på Googles hjemmesider, se f.eks.
http://www.google.com/intl/en/corporate/security.html
http://www.google.com/apps/intl/en/business/infrastructure_security.html

**Dokumentation for underliggende procedure, standarder, politikker**
Google er Safe Harbor certificeret:
http://safeharbor.export.gov/companyinfo.aspx?id=10543
Adgang til Googles fulde SAS70 rapport kan opnås ved at underskrive en non-disclosure aftale (NDA). Google er FISMA certificeret.

**Adgang til konfigurationsinformation**
Google har etableret et Audit API til at udtrække konfigurationsinformation, som man i øjeblikket kan få adgang til programmatisk. Der er flere virksomheder der har udviklet Apps til at udtrække informationen, applikationerne er tilgængelige igennem Google Apps Marketplace.
Google arbejder på at indbygge funktionalitet til at udtrække informationen i administrationskonsollen.

**Adgang til log og monitoreringsinfo**
*App Engine*
Google App Engine kan indsamle logbeskeder sendt til og fra kundernes applikationer. Logs kan ses fra ”Logs” linket i Admin Console ligesom logfilerne kan indsamles via API-kald.
Som i andre PaaS-løsninger er det i App Engine kunden selv der er ansvarlig for at udvikle, eller få udviklet, sine applikationer så applikationerne opfylder egne krav til logning.

*Google Apps*
For Google Apps arbejdes der aktivt på et audit-API. Løsningen er offentligt annonceret og opdateres jævnligt:
http://googleappsupdates.blogspot.com/2010/05/new-api-released-google-apps-audit-api.html. Adgang til logfilerne vil ske igennem Apps Admin Console, ligesom det kan ske programmatisk via API-kald.

>

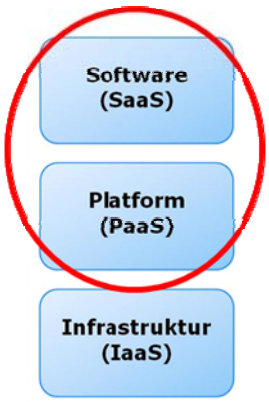
Det forventes, at logfilerne bliver tilgængelige igennem API'et i løbet af Q1 2011. For kunder der anvender Google Message Discovery (arkivering) optionen kan adgang til logfilerne i dag opnås ved at kontakte Googles support.

**Deltagelse i audit initiativer**
Google oplyser, at det aktivt undersøges, hvilke audit og assurance initiativer Google skal være medlem af.

>

## Salesforce

Salesforce leverer Software as a Service igennem Salesforce.com, samt Platform as a Service løsninger fra Force.com platformen.




Audit og assurance-information er primært tilgængelig fra Salesforces sikkerhedsportal:
https://trust.salesforce.com/security.htm

Se f.eks. nedenstående links og dokumenter for yderligere information:
http://wiki.developerforce.com/index.php/Security
https://trust.salesforce.com/trust/privacy/tools
http://wiki.developerforce.com/index.php/Security

**Dokumentation for underliggende procedure, standarder, politikker**

Salesforce er ISO 27001 og SAS70 type II certificeret. Adgang til Salesforces fulde SAS70 rapport kan opnås ved at underskrive en Non-disclosure aftale (NDA).
Salesforce er Safe Harbor certificeret:
http://safeharbor.export.gov/companyinfo.aspx?id=9994

**Adgang til konfigurationsinformation**

*Salesforce.com*
Konfigurationsændringer logges i den indbyggede Setup Audit Trail, der er tilgængelig via Systemadministrator værktøjerne i Salesforce.com. Hvis det kræves, kan kunden derved selv eksportere seneste 6 måneders audit log som dokumentation for opsætningen af egne løsninger.

*Force.com*
Der kan udtrækkes information om metadata-strukturen igennem Metadata-API'et i både Force.com og Salesforce.com. Ved at benytte Force.com EDI'et til Eclipse kan man udtrække en XML-beskrivelse af eventuelle tilpasninger. Kunden kan på den måde selv udvikle en løsning til at dokumentere standard opsætning og eventuelle kundespecifikke tilpasninger.
Der eksisterer ligeledes flere virksomheder der har udarbejdet partner-løsninger, disse kan findes igennem Salesforce AppExchange.

>

**Adgang til log og monitoreringsinfo**
*Salesforce.com*
Der er mulighed for log på samtlige felter i Salesforce.com. Detaljeret logning kan defineres på det enkelte objekt, på felt, på side etc.
Den enkelte kunde definerer og konfigurerer selv, hvor meget man ønsker at logge.
Kunden har mulighed for at lave specifikke rapporter på de loggede aktiviteter.
Rapporter kan køres realtime, herunder med opsætning af triggers for alarmering.

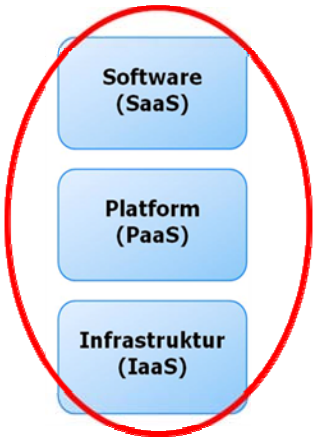
*Force.com*
Force.com giver mulighed for at indsamle logbeskeder sendt til og fra kundernes applikationer. Logs kan ses fra konsollen ligesom logfilerne kan indsamles via API-kald.
Som i andre PaaS-løsninger er det kunden selv, der er ansvarlig for at udvikle (eller få udviklet) sine applikationer, så applikationerne opfylder egne krav til logning.

**Deltagelse i audit initiativer**
Salesforce oplyser, at det undersøges aktivt, hvilke audit og assurance initiativer Salesforce skal understøtte.

>

## Microsoft

Microsoft leverer Software-as-a-Service igennem Microsoft Online Services, Platform-as-a-Service i gennem Azure Platform, Infrastructure-as-a-Service vil blive leveret igennem Azure Platform.




Audit og assurance-information gøres tilgængeligt på Microsofts cloud security portal http://www.globalfoundationservices.com/security/index.html og generelle cloud hjemmesider: http://www.microsoft.com/cloud.

Se f.eks. følgende links og dokumenter:
http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=5736aaac-994c-4410-b7ce-bdea505a3413
http://www.globalfoundationservices.com/documents/MicrosoftComplianceFramework1009.pdf

**Dokumentation for underliggende procedure, standarder, politikker**
Microsoft er SAS70 og ISO 27001 certificeret. Adgang til yderligere underliggende dokumentation kan opnås ved at underskrive en non-disclosure aftale (NDA).
Microsoft er Safe Harbor certificeret:
http://safeharbor.export.gov/companyinfo.aspx?id=9838

**Adgang til log og monitoreringsinfo**
Som i andre PaaS-løsninger er det i Azure Platformen kunden selv, der er ansvarlig for at udvikle (eller få udviklet) sine applikationer, så applikationerne opfylder egne krav til logning.
For Microsoft Online Services stiller Microsoft log- og monitoreringsinformation til rådighed igennem konsollen.

**Deltagelse i audit initiativer**
Microsoft deltager i flere audit initiativer, status for arbejdet er dog ikke offentliggjort på nuværende tidspunkt.

<