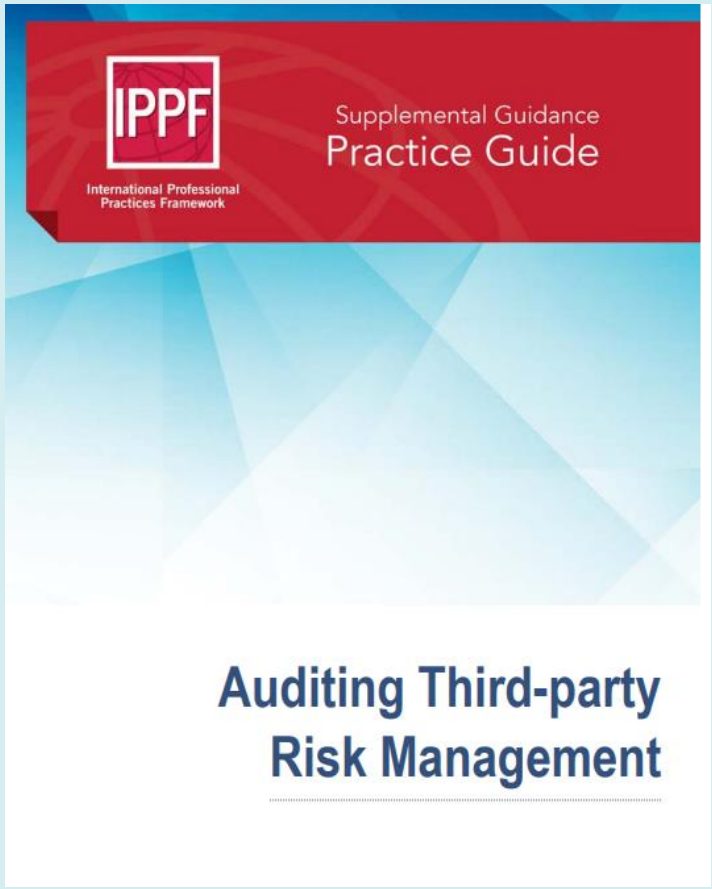
Revisjon av leverandører

Gaute Brynildsen, GSNA, CISA, CRISC, CCSK, CIA
Revisjonsdirektør Gjensidige Forsikring

29.1.2019



Tema til diskusjon

- IIA IPPF – Auditing Third-party Risk Management
- Revisjon av leverandørvalg og leverandøroppfølging
- Revisjon av leverandører
- Bygge på andres arbeid

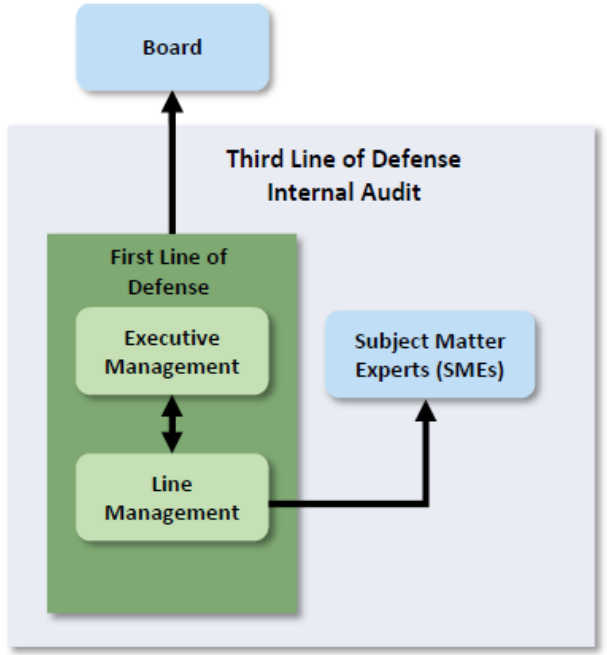
IIA IPPF – Auditing Third-party Risk Management

- Overordnet struktur på leverandørstyring
- Nøkkelfunksjoner, ansvar og risikoer innen leverandørstyring
- Internrevisjonens rolle - revisjon av leverandørstyring
- Metode for revisjon
- Vedlegg med utvalgte tema, f.eks
  - Samfunnsansvar
  - Due diligence
  - Forhold å vurdere for små internrevisjonsavdelinger
  - Tema for kontraktsarbeidet, inkludert sjekkliste
  - Eksempel på revisjonsrett
  - Eksempel på tema for revisjonsprogram
  - Eksempel på risikoer
  - Hva bør vi tenke på når det gjelder underleverandører (under-under-underleverandør?)

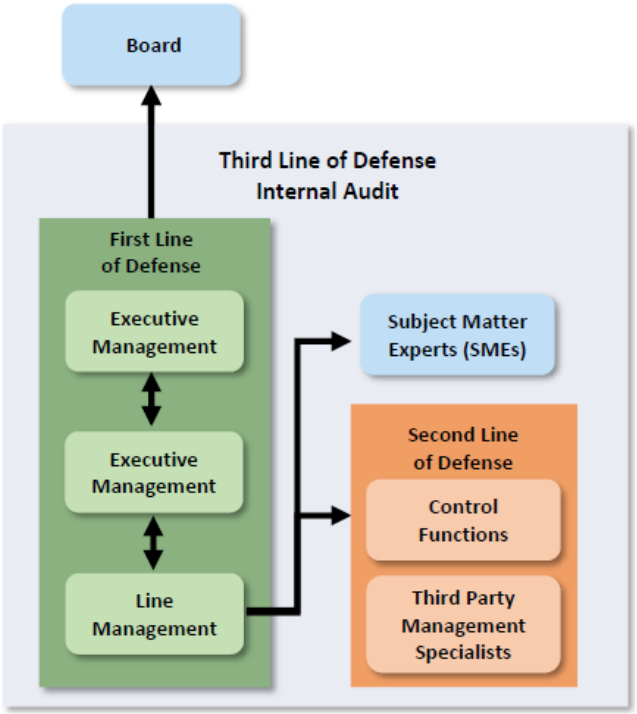
Overordnet struktur på leverandørstyring

- Risikostyring tilpasset leverandører
- Risikoappetitt
- Styrende dokumenter
- Roller og ansvar
- Prosessbeskrivelser
- Oversikt over leverandører

Figure 1: Third-party Risk Management Governance – Ba



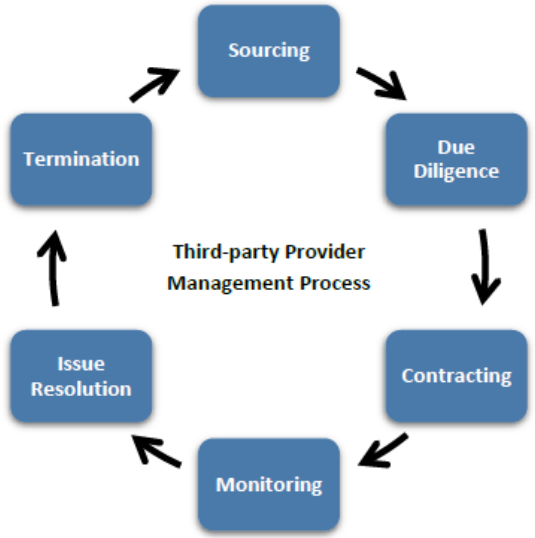
gure 3: Third-party Risk Management Governance – Standardized



Internrevisjonens rolle - revisjon av leverandørstyring

- Sourcing:
  - Business case og strategi
  - Prosess fulgt
  - Estimater på manglende leveranse og følgende av dette – BC
  - Sensitiviteten i BC
  - KPI i BC -> monitorering?
- Due diligence
- Contracting
  - Right to audit
- Monitorering
- Issue resolution
- Termination

Figure 4: The Elements of Third-party Provider Management Processes



Appendix B - samfunnsansvar

A Third-party Evaluation Using the 10 Principles of the UN Global Compact			
Hypothetical example: ABC Consulting Company providing model validation services in the US, UK, and Australia			
Principle	**Contributing factors**	**Mitigating factors**	**Risk level**
1. Businesses should support and respect the protection of internationally proclaimed human rights.	Vendor's website contains a statement supporting the UN Global Compact.	Vendor's offices are located in the U.S., U.K., and Australia, which all have a system of law and order that aim to protect human rights.	1
2. Businesses should make sure that they are not complicit in human rights abuses.	Consultants are deployed all over the world potentially in countries that restrict human rights.	Vendor has never been cited for human rights abuses. Vendor has a code of conduct and ethics program that aim to prevent them from deploying consultants to countries with known human rights issues. Staffing is regularly reviewed by managing partners.	1
3. Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining.	Vendor is not unionized and no record of their views on collective bargaining are known.	Vendor is located in countries with strict labor laws that aim to protect the worker, guarantee medical leave and vacation, and have a minimum wage.	1
4. Businesses should uphold the elimination of all forms of forced and compulsory labour.	N/A	Vendor performs a lucrative service and operates mostly in the U.S., U.K., and Australia where slavery is prohibited by law.	1

A Third-party Evaluation Using the 10 Principles of the UN Global Compact (continued)			
Principle	**Contributing factors**	**Mitigating factors**	**Risk level**
5. Businesses should uphold the effective abolition of child labour.	Vendor has made no statements concerning their views on child labor.	Vendor is located in countries with strict labor laws that aim to protect the worker, guarantee medical leave and vacation, and have a minimum wage. Vendor is located in countries where child labor is prohibited by law.	1
6. Businesses should uphold the elimination of discrimination in respect of employment and occupation.	Publicly available reports indicate that the vendor's workforce is predominantly male. Females comprise approximately 30% of the consultants employed at the vendor.	Vendor is located in countries with government agencies that aim to monitor and prosecute violations of employment discrimination laws.	1
7. Businesses should support a precautionary approach to environmental challenges.	Vendor's workforce travels a great deal (e.g., 5 days per week), which creates a large carbon footprint per consultant. Vendor is located in countries without strict environmental protection laws regarding recycling, efficient cars, and other protections.	Vendor has provided their statement of sustainability that outlines their commitment to paperless working, limiting long distance travel when possible, office recycling, and other initiatives taken by both the vendor and their parent company regarding environmental sustainability.	2
8. Businesses should undertake initiatives to promote greater environmental responsibility.	See above.	See above.	1
9. Businesses should encourage the development and diffusion of environmentally friendly technologies.	See above.	See above.	1
10. Businesses should work against corruption in all its forms, including extortion and bribery.	Vendor does business in countries known as problem areas for corruption, bribery, kidnapping, etc.	Vendor's code of conduct explicitly forbids employees to engage in bribery or other corrupt practices in accordance with the U.S. law, the Foreign Corrupt Practices Act.	2
		Total Risk Score	12
1–Low (10-17)	**2–Medium (18-23)**	**3–High (24-30)**	

Source: Adapted from the United Nations Global Compact, "The Ten Principles of the UN Global Compact." https://www.unglobalcompact.org/what-is-gc/mission/principles. Accessed on August 27, 2018.

Appendix C – Due dilligence

Table 1: Key Topics and Questions to Determine Eligibility of Potential Third-party Vendors
Ownership structure and background
▪ What is the legal structure of the organization (a corporation, limited liability corporation, not-for-profit entity, etc.)?
▪ Who owns the organization? Obtain details of the ownership.
Company performance and financial health
▪ Is the company solvent? Obtain financial statements.
▪ Is the company a likely candidate for a buyout or hostile takeover?
▪ Is the company party to any lawsuits or subject to any fines or civil penalties?
Company location
▪ Is the organization licensed to do business with the country/state in which its business and any other offices reside?
▪ Is the company located in a geographical area far from your organization's location or in an area at-risk for any of the organization's red flags?
Business model and practices
▪ Obtain a summary of the company's business strategies and direction for the next three years.
▪ Why should the company be considered (or why was it considered) for a strategic alliance with the organization?
▪ Does the company have a stated philosophy or mission statement that indicates they would be a "good match" for the organization?
References
▪ How many clients does the company currently serve? How many are significant to the organization's operations (i.e., to what extent is the entity dependent on a few large customers)?
▪ How many clients have terminated their relationship with the company in the last 12 months? Why?
▪ Obtain a list of other clients in the organization's industry that are doing business with the company.
Service delivery capability, status, and effectiveness
▪ What materials/services would be received as part of the service/product (analyses, bids, etc.)?
▪ What training does the company provide for the service/product?
▪ Is training provided by on-site qualified trainers or delivered electronically using qualified trainers?
Pricing and billing
▪ How is the service/product currently priced?
▪ Does the company expect this pricing structure to change? How often?
▪ What is the company's billing process?

Table 2: Documentation That May Be Gathered to Assist in Determining Eligibility of Potential Third-party Vendors
Financials
▪ Financial statements/annual reports.
Business continuity
▪ Policies and/or procedures regarding granting, restricting, and terminating access to data.
▪ Business continuity/disaster recovery plans and testing results.
▪ Incident response procedures.
▪ Insurance certificates.
Cybersecurity
▪ Information stating where data is processed and stored and evidence of compliance with relevant regulations.
Contractual obligations
▪ Letters/memoranda of understanding.
▪ Nondisclosure agreements.
Ethics policies
▪ Codes of conduct.
▪ Relevant ethics policies including whistleblower policies and procedures.
Controls
▪ Assurance Reports on Controls at a Service Organization as required by International Standards for Assurance Engagements (ISAE) No. 3402 for international organizations or by Statement on Standards for Attestation Engagements No. 18 (SSAE-18) for United States organizations.

Appendix E: Tema for kontrakt

Table 2: Sample Contract Review Checklist (continued)

Reports	Yes	No
The contract specifies the type and frequency of management information reports to be received from the service provider/vendor.	☐	☐
The contract outlines routine reports, such as performance reports, audits, financial reports, security reports, exception reports, and business resumption testing reports, to be provided and that serve as notification of changes or problems that could affect the relationship or pose a risk to the organization.	☐	☐
Audit	**Yes**	**No**
The contract specifies the institution's right to audit the third party, including by engaging an independent auditor, as needed to monitor performance under the contract.	☐	☐
The contract ensures the third party's internal control environment as it relates to the service or product being provided is sufficiently audited.	☐	☐
The contract includes authorization for the appropriate federal and state regulatory agencies to have access to records as is necessary or appropriate to evaluate compliance with laws, rules, and regulations.	☐	☐
Confidentiality and security	**Yes**	**No**
The contract prohibits the service provider/vendor and its agents from using or disclosing data or information, except as necessary to perform the functions designated by the contract.	☐	☐
The contract specifies nonpublic personal information must be handled in accordance with applicable privacy laws and regulations.	☐	☐
The contract states that breaches in the security and confidentiality of information, including unauthorized intrusion, are required to be fully and promptly disclosed to the organization.	☐	☐

Table 1: Contract Terms to Consider

Operational

- A statement that the third party is a valid enterprise operating in compliance with all applicable laws and regulations.
- A statement requiring the third party to immediately report any changes in its ownership or change in structure that would affect its risk profile.
- Arrangements if a third party is unable to operate due to unforeseeable circumstances beyond their control (e.g., weather events or geopolitical issues, also known as force majeure).
- Hold harmless clauses.
- Bank guarantees are valid up to the expiry date of the contract (this may be missed if the contract is automatically extended).

Monitoring, issue resolution, termination

- The third party's representation and warranty of the quality of their product or service.
- Penalties for breach of contract (e.g., failure to deliver products or services on time and of acceptable quality according to the SLA, also known as liquidated damages).
- Conditions allowing the third party to rectify issues related to quality, delivery, or other issues within certain time frames and conditions.
- Dispute resolution protocols.
- Customer complaints (e.g., the contract should define what constitutes a customer complaint and state who is empowered to make decisions according to specified criteria).
- Specific termination conditions and any costs associated with early termination, including the ability to terminate a third-party relationship due to change of control or management within the third-party organization among other reasons. Termination conditions should also outline the support requirements during the transition and the retention/return of data expectations.

Ethics/code of conduct

- A statement that the third party will abide by the contracting organization's third-party code of conduct, ethics standards, policies, procedures, and values.
  - This statement may be followed by a requirement that all employees of the third party who work on the contract be educated regarding the contracting organization's standards, culture, compliance requirements, etc., including a stipulation that employees certify their understanding in writing.
- Clauses regarding anti-corruption and anti-retaliation.

Technology

- Confidentiality and data protection/cybersecurity requirements, which may be stringent depending on the applicable regulations.
- Requirements to disclose data breaches within a certain period of time based on the time of detection.

Fourth parties

- Approval requirements should a third party engage subservice agents (fourth parties) to fulfill obligation.
- Fourth-party usage conditions or restrictions.

Appendix F: Revisjonsrett

Examples of Condition Statements for a Right-to-Audit Statement (continued)

Right to evaluate vendor's IT processes

Sample condition statement	Purpose and considerations
The client has the right to request and obtain, at client's discretion, a current and appropriate Service Organization Control (SOC) report and/or other applicable and relevant independent assessment report(s) that encompasses the vendor's IT processes. SOC reports will be full Type II reports that include the vendor's description of control processes, and the independent auditor's evaluation of the design and operating effectiveness of controls.	SOC 1 reports are for financial reporting. SOC 2 reports cover IT processes and focus on one or more of American Institute of Certified Public Accountants (AICPA's) defined Trust Principles™: ▪ Security. ▪ Availability. ▪ Confidentiality. ▪ Processing Integrity. ▪ Privacy. Other independent assessment reports such as PCI or ISO certifications may be appropriate but must be accepted at the organization's discretion.
In addition to receiving any independent assessment report, the client reserves the right to conduct relevant and applicable IT assessments above and beyond the SOC testing to assure that the client's information assets are properly protected. Areas that may be included in such testing include, but are not limited to vendor's: ▪ Business continuity including disaster preparedness and recovery. ▪ Ability for client to attend one of the vendor's recovery and readiness tests. ▪ Backup, recovery, and data transfer procedures, including verification that backup media is readable and access to observe and verify off-site records/data management facility(s). ▪ Security and privacy procedures and conditions including right to perform a security/privacy baseline assessment, periodic security/privacy test re-performance, and planned or surprise penetration testing.	The receipt and evaluation of an adequate and appropriate SOC report will likely suffice, but internal auditors must ensure they have a right to and can perform their own independent assessment of appropriate procedures and controls. Note that with the right to perform their own system and network penetration testing planned and surprise the vendor may justifiably necessitate limitations if vendor IT resources (databases, etc.) are shared with other clients. Limitations under these circumstances are appropriate, but should be documented in the contract. The organization should expect the vendor to make the same conditions effective if another client requested similar rights.

Appendix H: Eksempler på risikoer

Table 1: Sample Third-party Risks

Risk Category	Risks
Strategic	▪ Not achieving the objectives of the relationship. ▪ Reputational damage. ▪ Loss of intellectual property.
Operational	▪ Physical security. ▪ Fourth parties. ▪ Quality – failure to perform according to SLA. ▪ Records retention pre- and post-termination. ▪ Concentration of critical services to too few third parties. ▪ Inadequate, unreliable, or untimely performance of risk assessments. ▪ Failure to integrate SMEs into the due diligence and contracting process steps.
Human resources	▪ Inadequate training. ▪ Lack of personnel.
Financial	▪ Cost overruns. ▪ Failure to collect penalties. ▪ Misuse of funds.
Legal/compliance	▪ Corruption. ▪ Conflict of interest. ▪ Fraud. ▪ Lawsuits. ▪ Civil damages.
Technology	▪ Business continuity and disaster recovery. ▪ Failure to test compensating controls indicated as required by the third party. ▪ Security, privacy, and confidentiality of information, especially sensitive or nonpublic information that is available to, accessed by, or maintained by the vendor.

Table 2: Red Flags/Warning Signs

Category	Signs
Regional characteristics	▪ Third parties are geographically remote from the organization. ▪ Third parties work in different cultures with different customs, language, and expectations. ▪ A representative for the third party has been referred to the organization by a government official. ▪ The region, country, or industry in which the third party participates has a history of corruption.
Contracting and monitoring	▪ The third party requests a contract that has little detail regarding the work being performed or service provided. ▪ The third party rejects a right to audit clause in the contract. ▪ Third parties are not familiar with the organization's rules or have no incentives to comply with those rules. ▪ The third party utilizes shell companies in its corporate structure.
Financials	▪ The third party or its representative is requesting or granted an unusually high commission. ▪ The third party has been granted unusual payments or financial arrangements. ▪ The third party is not transparent with its financial records. ▪ The third party requests payment before the work is completed. ▪ The third party requests to be paid in cash (undocumented or otherwise unaccounted for), or in a country other than where the work is actually performed.

IKT-forskrift – god praksis

- **§ 12.*Utkontraktering***
- Foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.
- Avtalen skal videre sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket.
- Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.

- **EBA Guidelines on outsourcing arrangements**

Finans Norge

- Drivere:
  - Tilgang til ressurser og kompetanse
  - Fokus på egen kjernekompetanse
  - Lavere produksjonskostnad
  - Fleksibel tjenesteproduksjon
  - Forbedret tjenestekvalitet
  - Redesign av forretningsprosesser
  - Akseptert praksis i bransjen
  - Press fra konkurrenter
  - Tilgang til nye markeder/vekst

- Risikoer:
  - Utilstrekkelig servicekvalitet
  - Mangel på kompetanse om bedriften
  - Høy turnover hos leverandør
  - Mister kompetanse
  - Mister kontroll
  - Inkompatibilitet mellom systemer
  - Infrastrukturproblemer
  - Vanskeligheter ift. bedriftskultur
  - Kontraktuell og juridisk risiko
  - Språkproblemer
  - Tidsforskjell arbeidstid
  - Politiske vanskeligheter
  - Mangel på aksept hos kunder
  - Bekymring for industrielle relasjoner

Revisjon – leverandørvalg og leverandøroppfølging

- Vurdering og valg - er dette noe vi skal bygge internt eller kjøpe
  - Begge deler innbærer en risiko og et prosjekt der revisjonen kan ha en rolle
- Business case og strategi – rasjonale
- Anbud – RFP
- Implementeringsprosjekt
- Overgang til drift
- Intern kompetanse, prosesser og teknologi for å følge opp leverandøren.
  - Kompetanse internrevisor

Revisjon av leverandører

- Hvilke leverandører er relevante? Hvordan fanger man opp nye leverandører. Kan det være at relevans endrer seg over tid?
  - Hvem håndterer verdipapirer og kontoer med likvide midler?
  - Shadow-IT

- Ikke bruk sjekklister – tilpass til relevant risiko
- Men det finnes mange kilder som kan inspirere for å identifisere risikoer, relevante kontroller og nivå som bør forventes.

- Start internt – hvem gjør hva med å følge opp leverandøren? Første linje, andre linje.
- Forstå tredjeparts bekreftelser, eksempelvis ISAE 3402 og scope for sertifiseringer.
- Har leverandøren en internrevisjon? Eventuelt sikkerhetsavdeling som er uavhengige nok.

Case –Dutch Ministry of Security and Justice DPIA MS

- Avvik identifisert Office 365
- 23.000-25.000 event typer i office sendes til USA, f.eks emnefeltet i mails.
- Vs 10.000 i Windows 10.

- Hva slags kompetanse kreves for å finne et slikt avvik?

Erfaringer revisjon

- Bli med på RFP
- Samarbeid med andre miljøer internt og eksternt
- Bruk revisjonserklæringer aktivt
- Gjør også teknisk testing
- Observer katastrofetester

Eksempel skyleverandør

- Bilder fra Microsoft Azure Service Trust Portal ble vist, bruk denne linken for å ta en titt selv:
- https://servicetrust.microsoft.com/ComplianceManager

- Amazon Web services (AWS)
- https://aws.amazon.com/compliance/soc-faqs/

- Google Cloud
- https://cloud.google.com/security/compliance/soc-2/
-

Eksempler på kilder

- IT
  - ISF Standard of Good Practice for Information Security
    - Supplier Security Evaluation Tool (SSET)
  - NIST Cybersecurity Framework
  - CIS Top 20 Critical Security Controls for Effective Cyber Defense
  - Payment Card Industry Data Security Standard (PCI DSS) version 3.1
  - ISO/IEC 27002: 2013
  - COBIT 5 for Information Security
  - Cloud Controls Matrix
  - ISACA Cloud Computing Audit program