IT auditorsdag 2019

Algoritmic Assurance en de AVG

17 september 2019

ISACA
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

17 september 2019

Algoritmic Assurance en de AVG

Agenda

1. Introductie in Algoritmes
2. Algoritme Assurance door IT Auditors
3. Algoritme Assurance aandachtspunten
4. ISACA Privacy Assurance Framework
5. ISACA Privacy Controls – Case Linkedin for recruiters

1 Algorithm Assurance – introductie

Algoritme, wat is het eigenlijk?

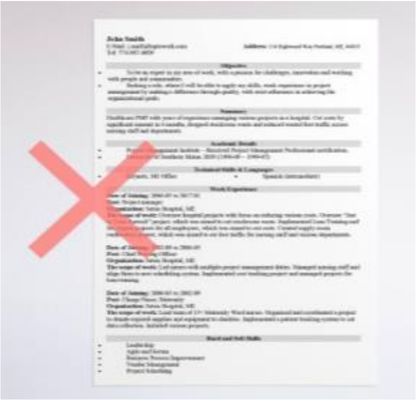
iRISK

Recruiter Algoritmes

“Match-on-the-go”

- No CV, no motivation letter
- Access to e-mail account (consent)

  Deep learning model



Meister discrimination algoritme

ECJ Meister-case (2012)

1. Equal treatment/no discrimination in employment
2. Application Meister rejected (twice)
3. No access to information about selection/successful candidate, unless….
4. Nevertheless: access to information refusal might be an indicator of discrimination
5. NL - Wet gelijke behandeling

GDPR as from 25 May 2018

1. Governance framework for processing of personal information
2. Public enforcement & sanctions

2 Algorithm Assurance – IT Auditors

Algoritme en de IT Auditor

- Have you come across algorithms in your IT audits (separate / financial audit support)?

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

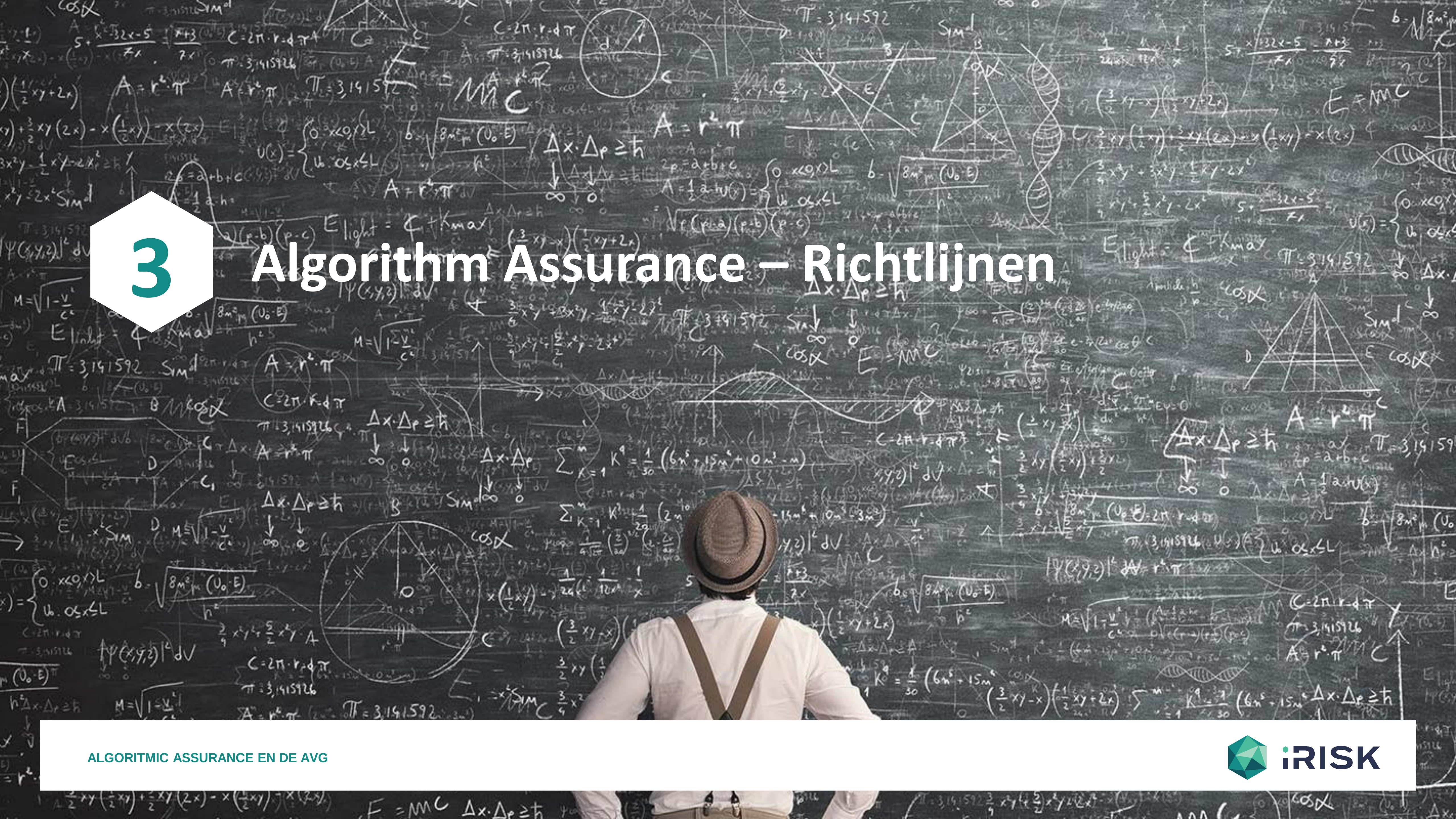
Controleren van Algoritmes in audits

1. Which criteria, standards or questionnaires have you applied?

2. What methods and standards would you deem necessary for future AI audits?

Kaders voor IT auditors in de toekomst

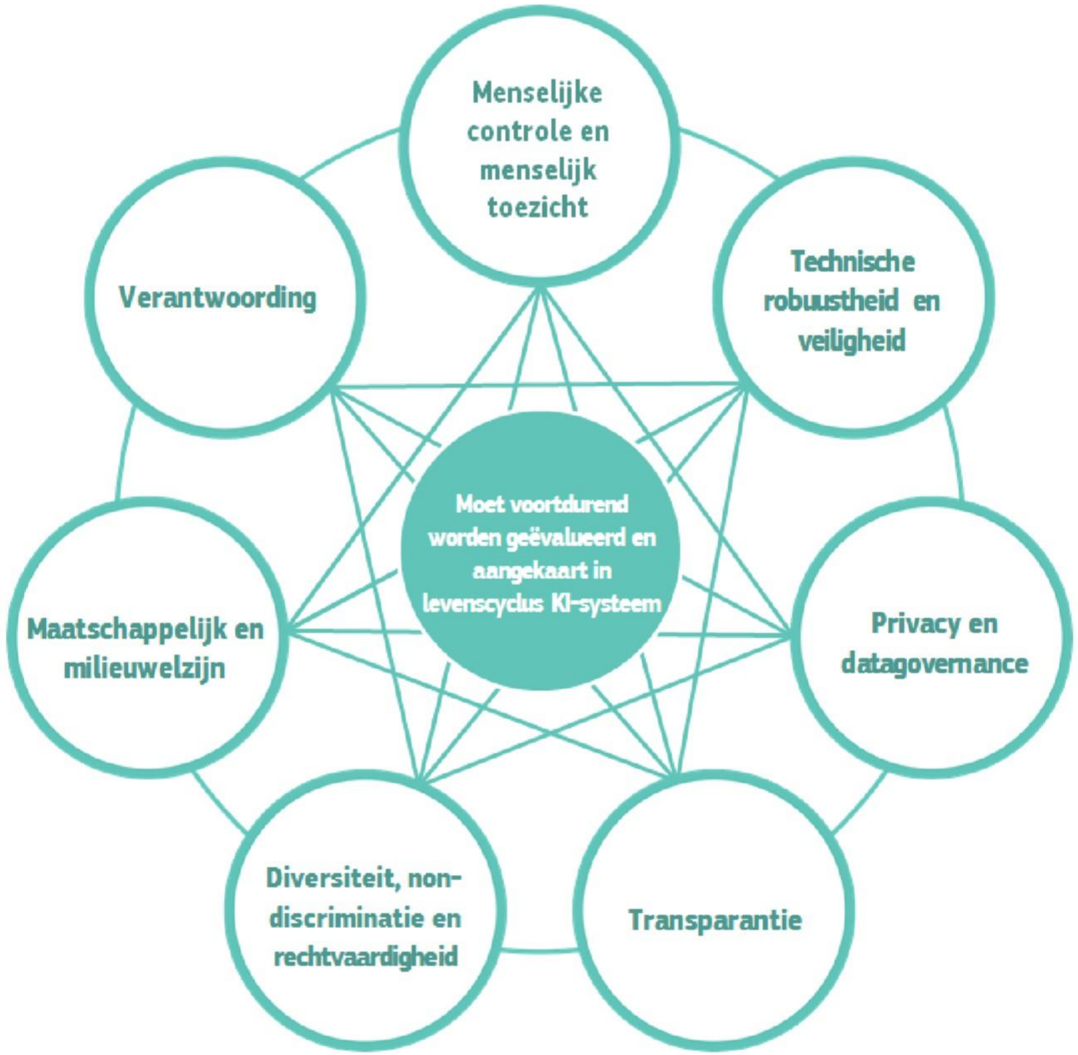
What would you always wanted to know about AI Assurance?
(but were afraid to ask)



3 Algorithm Assurance – Richtlijnen

Ethics – richtlijnen Europese Unie

1. Menselijke controle en menselijk toezicht
2. Technische robuustheid en veiligheid
3. Privacy en data governance
4. Transparantie
5. Diversiteit, non-discriminatie en rechtvaardigheid
6. Maatschappelijk en milieuwelzijn
7. Verantwoording



Betrouwbare Algoritmes & AI

Betrouwbare AI bestaat uit drie componenten, waaraan gedurende de volledige levenscyclus van het systeem moet worden voldaan:

1. de AI moet <u>wettig</u> zijn, door te zorgen dat aan alle toepasselijke wet- en regelgeving wordt voldaan;
2. de AI moet <u>ethisch</u> zijn, door te zorgen dat de ethische beginselen en waarden worden nageleefd; en
3. de AI moet <u>robuust</u> zijn, uit zowel technisch als sociaal oogpunt, aangezien AI-systemen ongewild schade kunnen aanrichten, zelfs al zijn de bedoelingen goed.

Technologisch robuust component

How can I improve security and robustness of AI through rigorous validation, continuous monitoring and maintenance, verification and adversarial modeling?

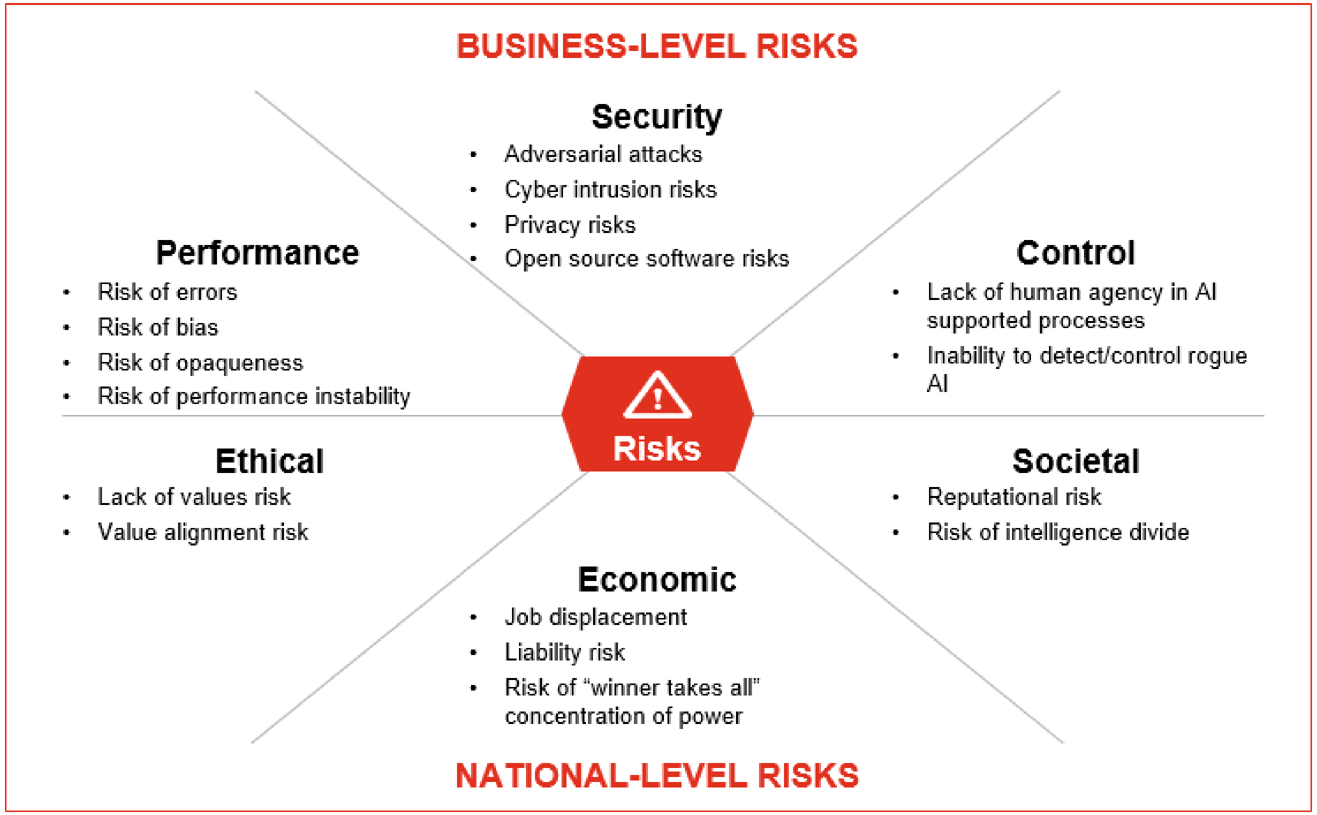
How do I test for bias in the data, model, and human use of AI algorithms to improve fairness of treatment across my organisation?

What can I do to add transparency, explainability and provability to the modelling process to improve human understanding of the model outputs?

How do I assess the ethical and moral implications of the development and use of AI?

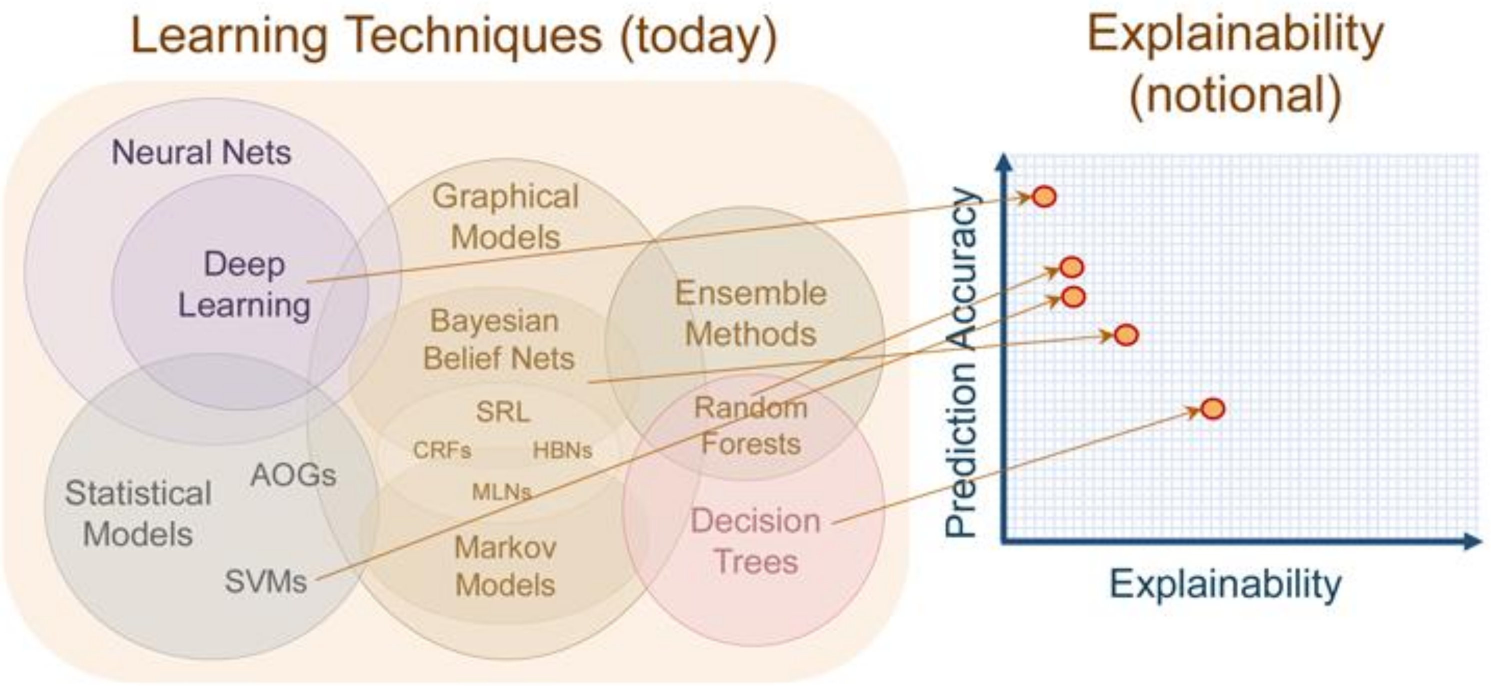
How can I track and check that AI solutions operate in compliance with relevant regulations?

How can I design effective AI operating models and processes to improve accountability and quality?

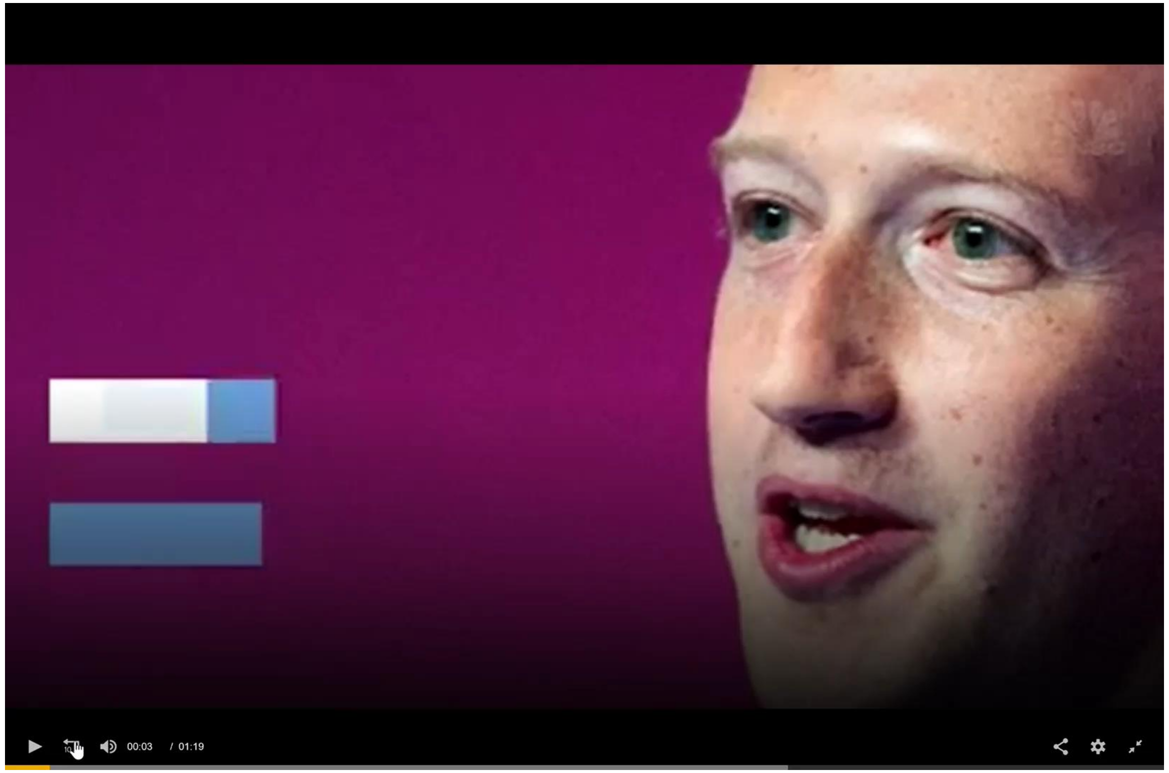


Source: PwC Responsible AI Framework

Technologisch robuust component



Ethische component



Laten we samen kiezen….

Ethische beginselen Casus – Cambridge analytica

Menselijke autonomie:
Mensen die met AI-systemen werken, moeten hun volledige en effectieve zelfbeschikking kunnen behouden en kunnen deelnemen aan het democratische proces. AI-systemen mogen mensen niet onterecht onderwerpen, dwingen, misleiden, manipuleren, conditioneren of drijven.

Preventie van schade:
Er moet specifiek aandacht worden besteed aan situaties waarin AI-systemen negatieve gevolgen kunnen veroorzaken of vergroten vanwege ongelijkheid wat betreft macht of beschikking over informatie, bijvoorbeeld tussen werkgevers en werknemers, tussen bedrijven en consumenten of tussen overheden en burgers.

Ethische beginselen Casus – Cambridge analytica

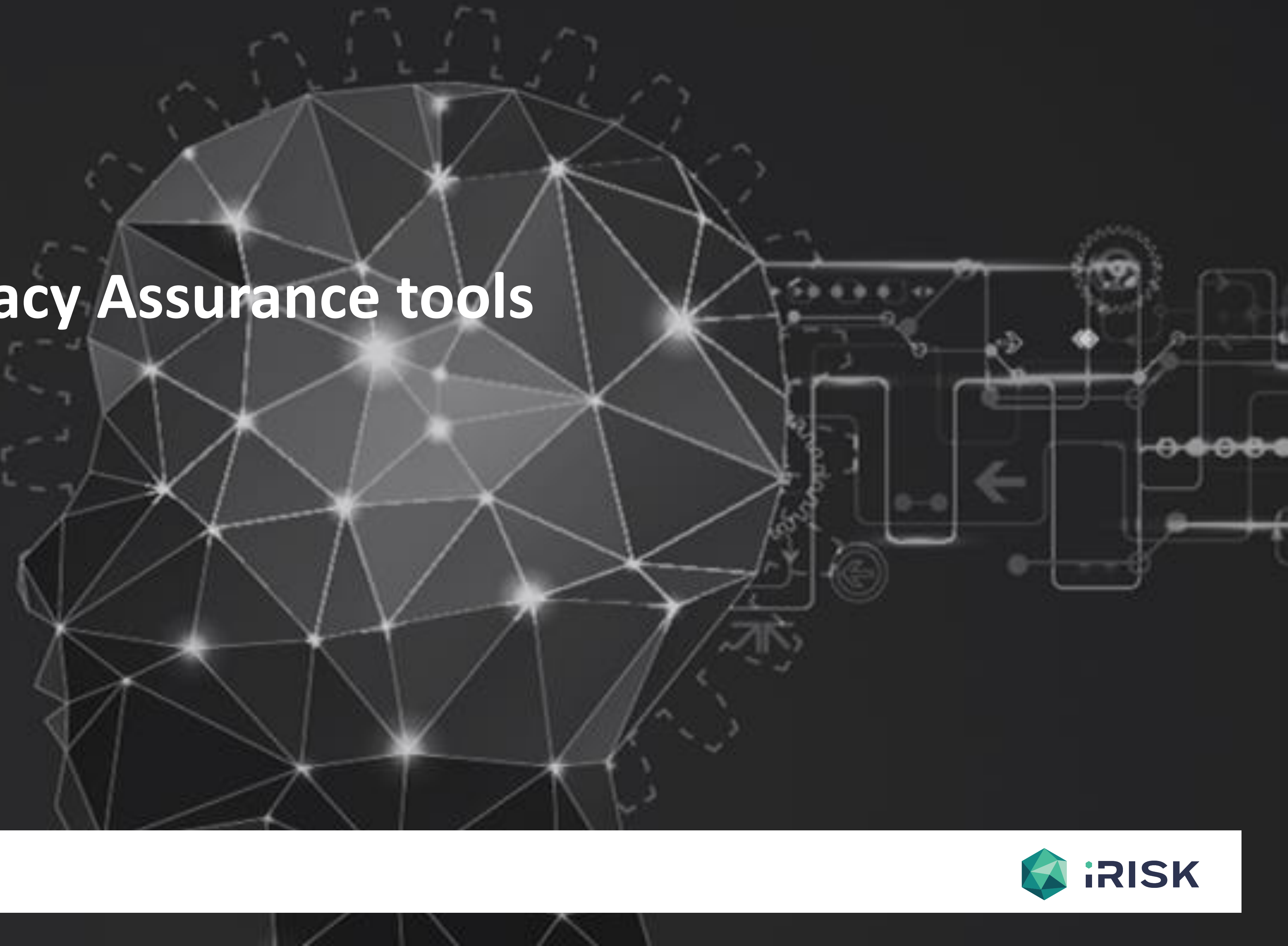
Rechtvaardigheid:
Gelijke kansen wat betreft toegang tot onderwijs, goederen, diensten en technologie moeten worden bevorderd. Daarnaast mag het gebruik van AI-systemen nooit tot gevolg hebben dat de (eind)gebruikers worden misleid of worden beperkt in hun keuzevrijheid.

Verantwoording:
"blackbox"-algoritmen vereisen speciale aandacht. In die situaties kunnen andere verantwoordings-maatregelen (zoals traceerbaarheid, controleer-baarheid en transparante communicatie over de capaciteiten van het systeem) nodig zijn, mits het systeem als geheel de grondrechten eerbiedigt

Juridisch component

- Fairness & transparency of data processing (article 5)
- Accuracy of data processing (article 5)
- Information te be provided to data subject (articles 13, 14)
- Access rights of data subject (article 15)
- Right to object, profiling, automated individual decision-making (articles 21, 22)
- Data protection by design and by default (Article 25)

4 Privacy Assurance tools

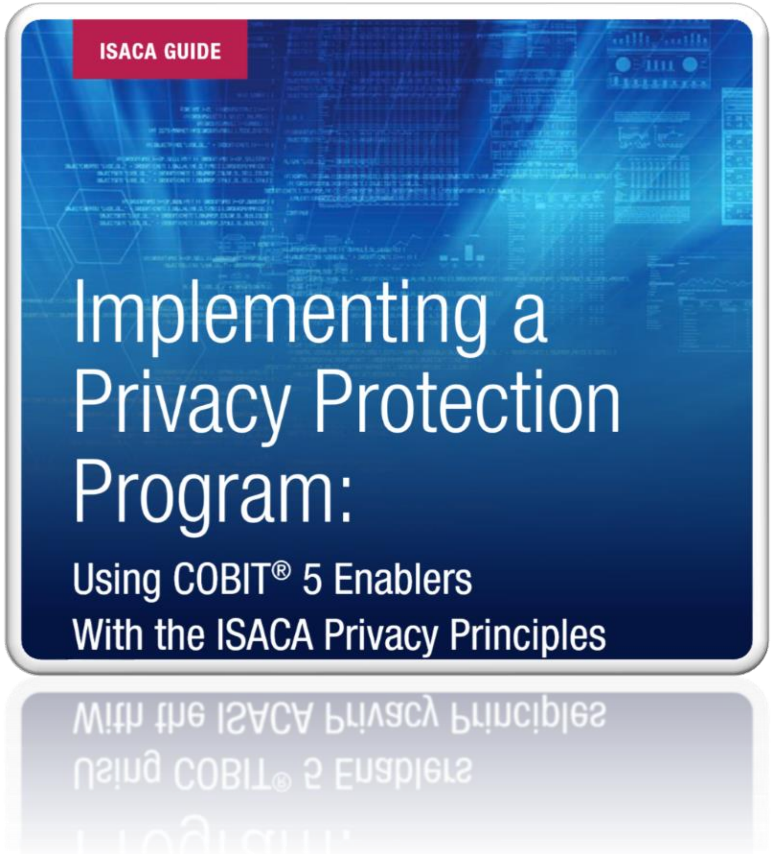


Privacy AVG over algoritmes

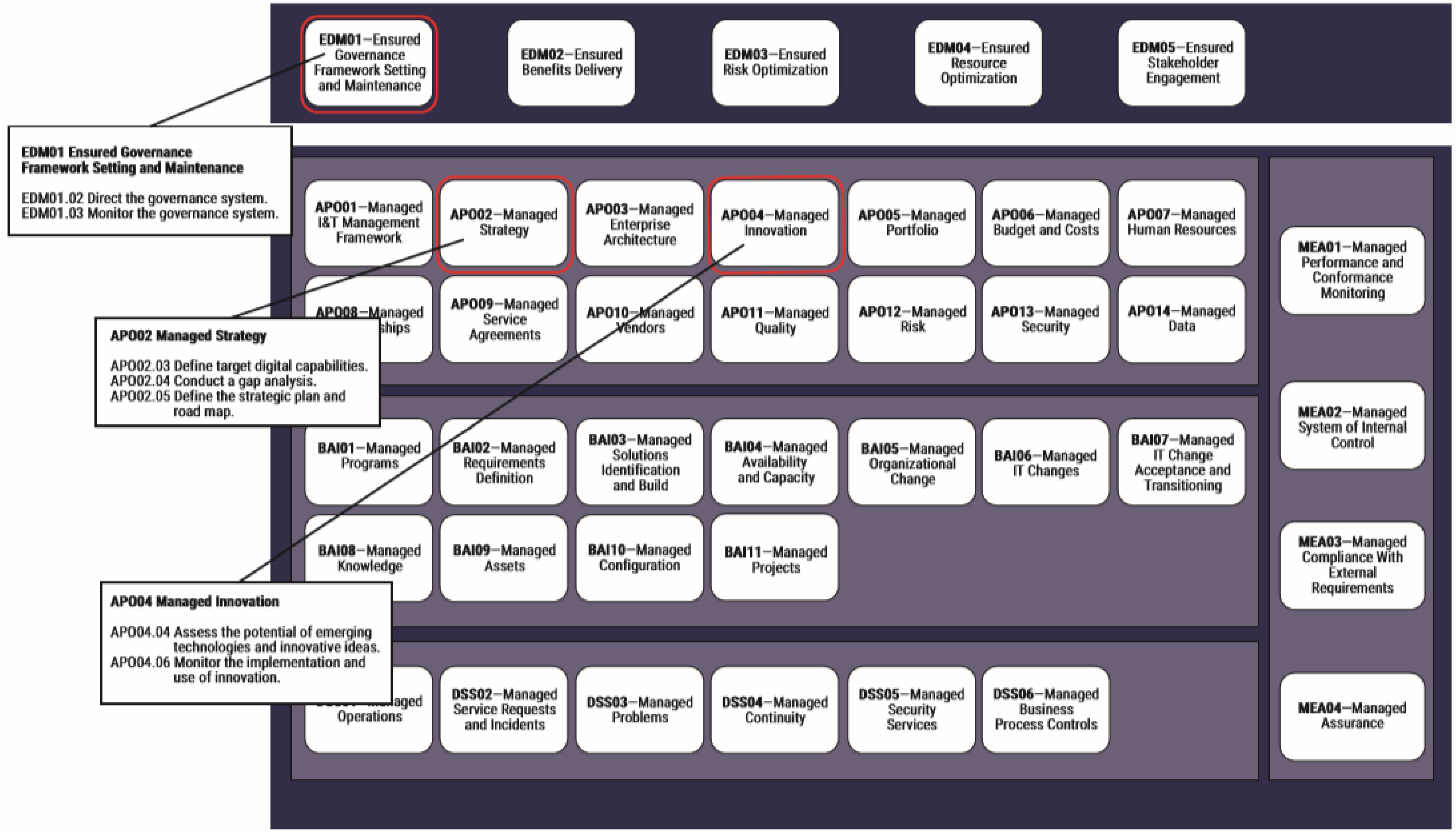
Fokke Jan aanvullen

ISACA privacy principes

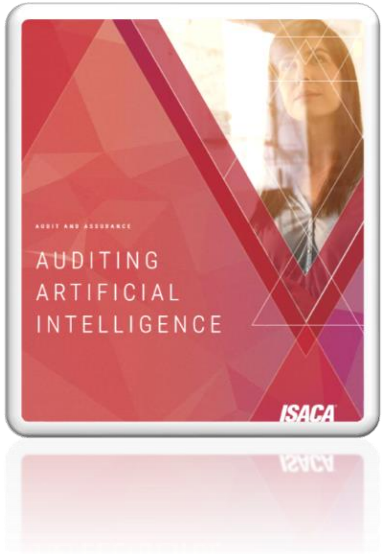
Principle 1: Choice and consent
Principle 2: Legitimate purpose specification and use limitation
Principle 3: Personal information and sensitive information life cycle
Principle 4: Accuracy and quality
Principle 5: Openness, transparency and notice
Principle 6: Individual participation
Principle 7: Accountability
Principle 8: Security safeguards
Principle 9: Monitoring, measuring and reporting
Principle 10: Preventing harm
Principle 11: Third party/vendor management
Principle 12: Breach management
Principle 13: Security and privacy by design
Principle 14: Free flow of information and legitimate restriction



Cobit 2019 mapping AI



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018



iRISK

ISACA privacy principe – Cobit Controls link

01. Ensure governance framework setting and maintenance.

EDM01 Ensure Governance Framework Setting and Maintenance	Area: Governance Domain: Evaluate, Direct and Monitor
COBIT 5 Process Description Analyze and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.	
COBIT 5 Process Purpose Statement Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.	
Primary Privacy Principles Involved • Principle 2: Legitimate Purpose Specification and Use Limitation • Principle 3: Personal Information and Sensitive Information Life Cycle • Principle 5: Openness, Transparency and Notice • Principle 12: Breach Management	
EDM01 Privacy-specific Process Goals and Metrics	
Privacy-specific Process Goals	**Related Metrics**
1. Legal and regulatory requirements for privacy are identified and documented. Privacy strategy is aligned with the requirements.	• Number of laws, regulations, standards and contractual requirements for privacy protections • Percentage of the identified privacy laws with which the organization is in compliance • Cost of noncompliance, including fines, sanctions, settlements, civil suits and impact of reputational loss • Percentage of total privacy management program budget taken by the noncompliance costs

iRISK

5 Privacy controls voor Algorithms

Privacy en Linkedin als recruiterplatform

Met ruim 600 miljoen actieve zakelijke professionals op LinkedIn is dit platform enorm geschikt om een baan te zoeken, te netwerken en content te delen. Dit is dus hét geschikte social-mediakanaal om in een business-to-business-omgeving in te zetten. Veel beslissers in de B2B-markt vertrouwen op LinkedIn en de inzichten die het platform kan bieden bij het maken van bedrijfsbeslissingen. Bekijk jij zelf bijvoorbeeld ook niet eerst het LinkedIn-profiel van een nieuwe klant, verkoper of potentiële nieuwe collega?

Specifiek DSS06 – Business Process Controls

Control: Waarborgen dat herleidbaarheid en verantwoordelijkheid voor alle informatie events aanwezig is.

Specifiek voor AI betekent dit er voldoende informatie wordt opgeslagen in het audittrail om het rationele besluit in voldoende mate te begrijpen.

Het geautomatiseerde rationale besluit dient ten alle tijde te blijven voldoen aan gelden wet&regelgeving zoals de Algemene Verordening Gegevensbescherming (Privacy).

iRISK

ISACA Cobit privacy – Wat moet er gebeuren?

DSS06 Privacy-specific Process Practices, Inputs/Outputs and Activities

Management Practices	Privacy-specific Activities (in Addition to COBIT 5 Activities)
DSS06.01 Align control activities embedded in business processes with enterprise objectives. Continually assess and monitor the execution of the business process activities and related controls, based on enterprise risk, to ensure that the processing controls are aligned with business needs.	• Identify and prioritize privacy management processes in line with business risk, compliance, privacy risk, privacy harms, etc. • Identify specific operational privacy management requirements (e.g., compliance). • Identify and implement needed application controls to support privacy management requirements.
DSS06.02 Control the processing of information. Operate the execution of the business process activities and related controls, based on enterprise risk, to ensure that personal information processing is valid, complete, accurate, timely and secure (i.e., reflects legitimate and authorized business use).	• Determine personal information categories and associated personal information items used within the processing.
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage the business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to personal information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where personal information is located and who is handling personal information on its behalf.	• Manage roles, responsibilities, access privileges and levels of authority for personal information. • Allocate access rights to personal information on need-to-know and least-privilege principles and job requirements. • Delete/remove access rights to personal information when users leave positions/units. • Implement segregation of duties according to business processes to avoid fraud and unauthorized access to personal information. • Periodically audit personal information authorizations.

Remedie – wat moet er gebeuren?

1. BIAS detection
2. Minimisation strategy
3. Data scientist audits
4. Trusted third parties certification

Dankuwel.

iRISK
Pettemerstraat 7, 1823 CW Alkmaar
Telefoon +31 (0) 72 82 00 353
www.irisk.nl, info@irisk.nl