DIGITAL TRANSFORMATION

IT auditorsdag 2019

Digital Transformation & Control

17 september 2019

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Algorithm Assurance & GDPR – Speakers

- Ronald Koorn (KPMG)
- Mona de Boer (PwC)
- Fokke Jan van der Tol (Data Governance Consult)
- Menno Borst (iRISK)

Algorithm Assurance & GDPR – Agenda

1. Algorithms & IT Auditors – Ronald Koorn
2. Algorithms & Recruitment – Mona de Boer
3. Algorithms & GDPR - Fokke Jan van der Tol
4. Algorithms & Cobit 2019 – Menno Borst
5. Q & A

Algorithms & IT Auditors

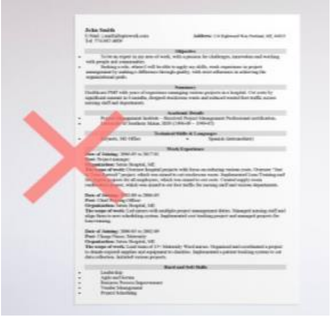
- Have you come across algorithms in your IT audits (separate / financial audit support)?
- Which criteria, standards or questionnaires have you applied?
- What methods and standards would you deem necessary for future AI audits?
- What would you always wanted to know about AI Assurance? (but were afraid to ask)

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

Algorithms we encounter in real life

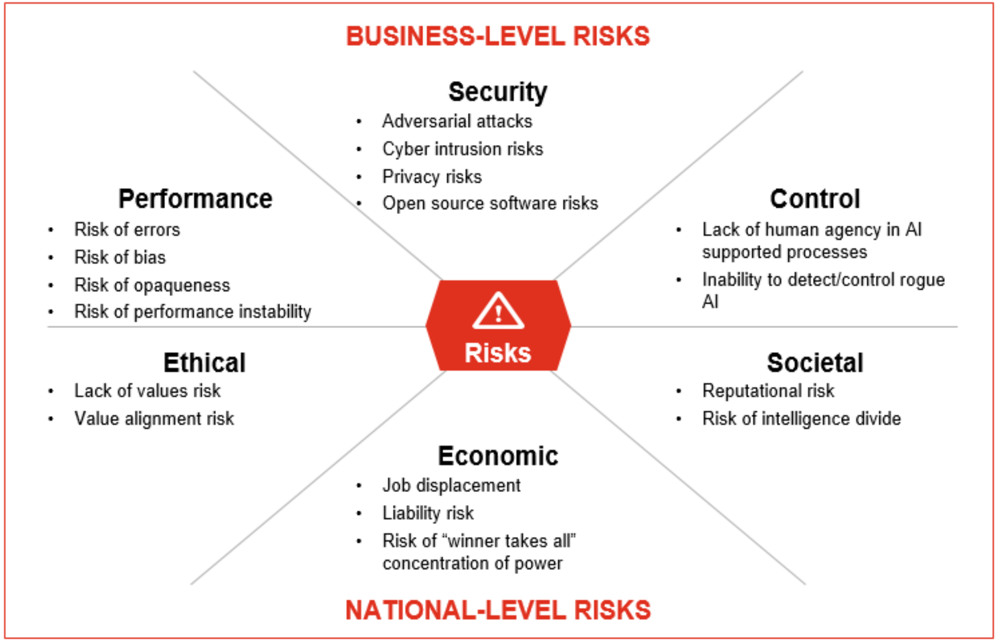
- Financial / credit risk (banking; insurance)
- Recruitment
- News & (social) media
- Consumer preferences
- Government grants
- Credit card fraud
- Medical care / diagnostics
- Logistics
- Etc

“Match–on–the–go”



- ✓ No CV, no motivation letter
- ✓ Access to e-mail account (consent)
- ✓ Deep learning model

Organisations will need to understand key risks and answer fundamental questions around design and deployment



BUSINESS-LEVEL RISKS

Security
- Adversarial attacks
- Cyber intrusion risks
- Privacy risks
- Open source software risks

Performance
- Risk of errors
- Risk of bias
- Risk of opaqueness
- Risk of performance instability

Control
- Lack of human agency in AI supported processes
- Inability to detect/control rogue AI

Risks

Ethical
- Lack of values risk
- Value alignment risk

Societal
- Reputational risk
- Risk of intelligence divide

Economic
- Job displacement
- Liability risk
- Risk of "winner takes all" concentration of power

NATIONAL-LEVEL RISKS

Source: PwC Responsible AI Framework

?

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?

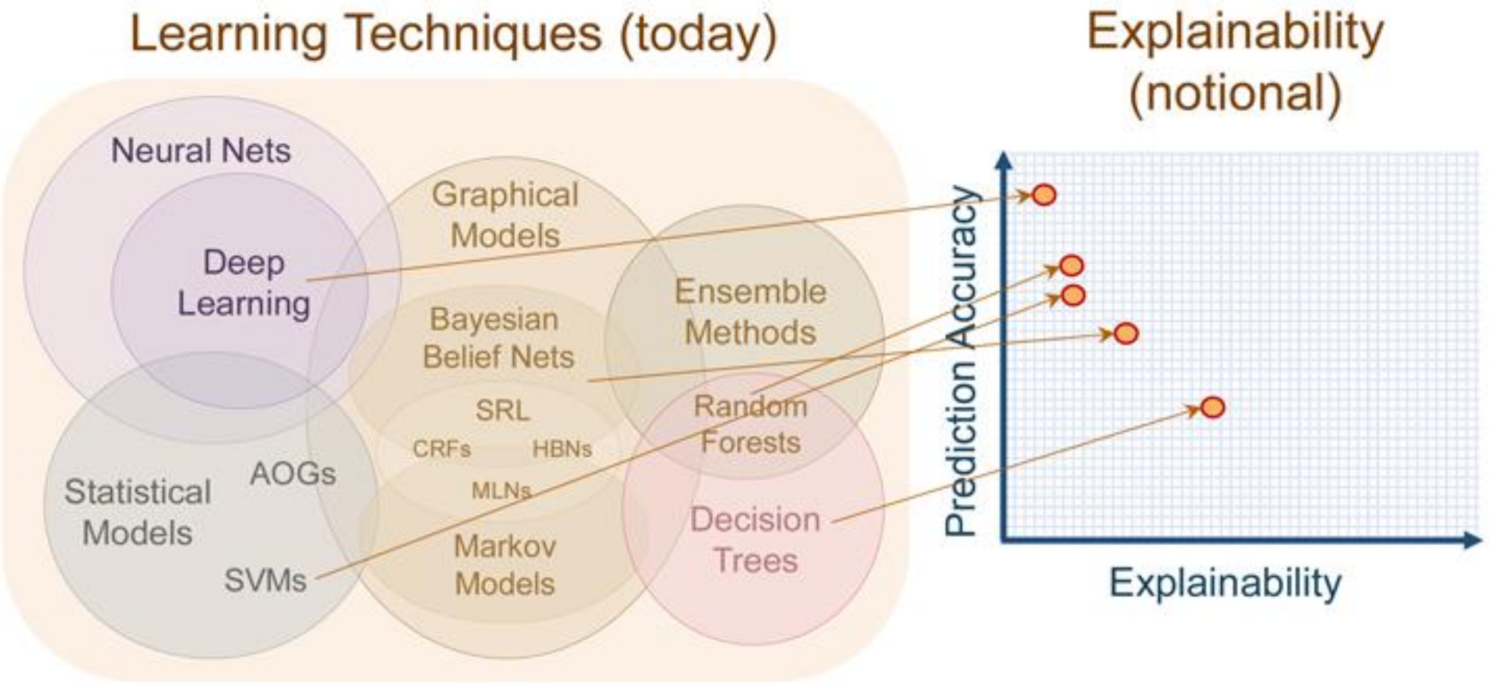
What can I do to add transparency, explainability and provability to the modelling process to improve human understanding of the model outputs?

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?

Prediction accuracy vs explainability



From ECJ Meister–case (2012) to GDPR implementation

ECJ Meister-case (2012)

- Equal treatment/no discrimination in employment - no algorithms involved yet
- Application Meister rejected (twice)
- No access to information about selection/successful candidate, unless….
- Access to information refusal might be an indicator of discrimination
- NL - Wet gelijke behandeling

GDPR as from 25 May 2018

- Governance framework for processing of personal information
- Public enforcement & sanctions

Accountability (article 24)

- Appropriate technical & organisational measures **to ensure and be able** to demonstrate that data processing is in accordance with GDPR
- Requires shift focus from ex post to ex ante (prevention)

(Joint) controlling and processing when using algorithms

- Articles 4, 24, 26, 28

GDPR provisions

- 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)

GDPR recitals

- Information regarding processing easily accessible, easy to understand, clear and plain language (39, 58)
- Information regarding processing should include the existence and consequences of profiling (60)
- No decisions which include profiling or are based solely on automated decision-making unless explicit legal basis and safeguards for data subject (71)
- Prevention of discriminatory effects (71)
- Appropriate mathematical or statistical procedures for profiling (71)
- Factors which result in inaccuracies are corrected and the risk of errors minimised (71)
- DPIA in case of high risk processing, using new technologies, decision making after profiling; mitigation measures; consultation supervisory authorities (83, 89, 91,94)

EDPB/Article 29 WP Guidelines

- Guidelines on Automated individual decision-making and Profiling (WP251 rev.01)
- Guidelines on DPIA (WP248 rev.01) / List of processing operations supervisory authorities

Assess & consider impact of

- Intellectual property rights
- Trade secret rights

How does the IT–Auditor gain control

- Talk to the DPO (articles 37, 38, 39) / people in charge for GDPR- & relevant other compliance areas
- Consult accountability records (Article 24)
- Conduct DPIAs (Article 35)
- Conduct audits (Cobit 2019)

Cobit 2019

Privacy principles verus Cobit Controls

ISACA privacy principles

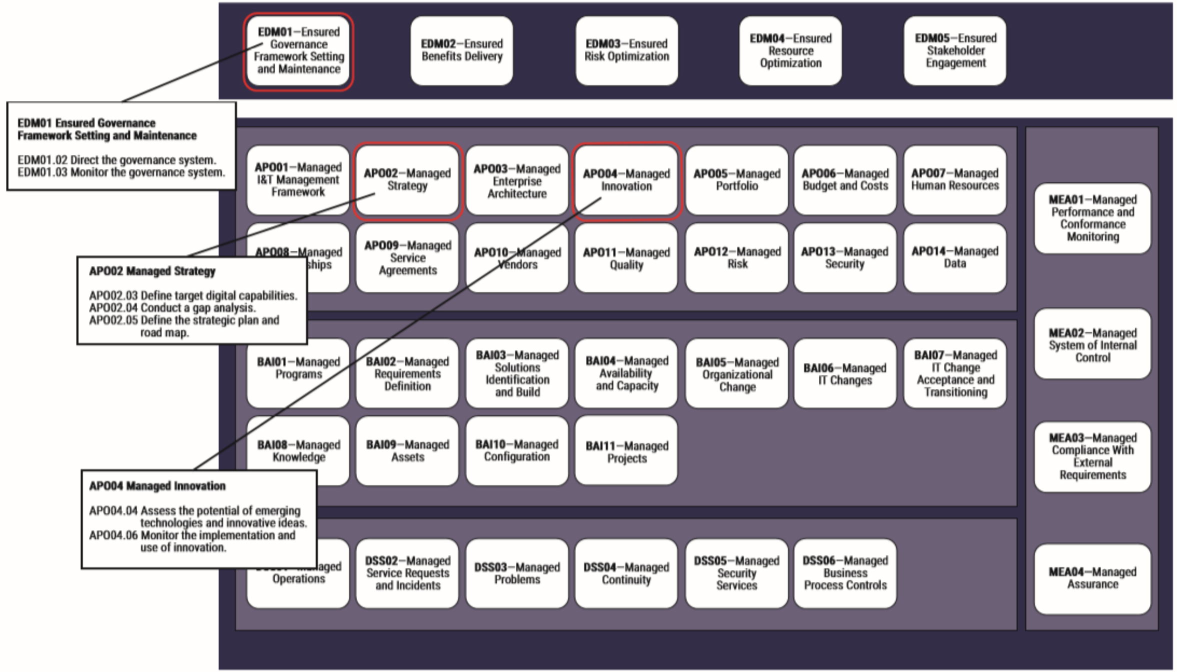
Principle 1: Choice and consent
Principle 2: Legitimate purpose specification and use limitation
Principle 3: Personal information and sensitive information life
Principle 4: Accuracy and quality
Principle 5: Openness, transparency and notice
Principle 6: Individual participation
Principle 7: Accountability
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

ISACA GUIDE

Implementing a Privacy Protection Program:

Using COBIT® 5 Enablers With the ISACA Privacy Principles

Cobit 2019 rule based mapping AI



EDM01—Ensured Governance Framework Setting and Maintenance

EDM02—Ensured Benefits Delivery

EDM03—Ensured Risk Optimization

EDM04—Ensured Resource Optimization

EDM05—Ensured Stakeholder Engagement

EDM01 Ensured Governance Framework Setting and Maintenance

EDM01.02 Direct the governance system.
EDM01.03 Monitor the governance system.

APO01—Managed I&T Management Framework

APO02—Managed Strategy

APO03—Managed Enterprise Architecture

APO04—Managed Innovation

APO05—Managed Portfolio

APO06—Managed Budget and Costs

APO07—Managed Human Resources

APO08—Managed ships

APO09—Managed Service Agreements

APO10—Managed Vendors

APO11—Managed Quality

APO12—Managed Risk

APO13—Managed Security

APO14—Managed Data

APO02 Managed Strategy

APO02.03 Define target digital capabilities.
APO02.04 Conduct a gap analysis.
APO02.05 Define the strategic plan and road map.

BAI01—Managed Programs

BAI02—Managed Requirements Definition

BAI03—Managed Solutions Identification and Build

BAI04—Managed Availability and Capacity

BAI05—Managed Organizational Change

BAI06—Managed IT Changes

BAI07—Managed IT Change Acceptance and Transitioning

BAI08—Managed Knowledge

BAI09—Managed Assets

BAI10—Managed Configuration

BAI11—Managed Projects

APO04 Managed Innovation

APO04.04 Assess the potential of emerging technologies and innovative ideas.
APO04.06 Monitor the implementation and use of innovation.

[illegible]aged Operations

DSS02—Managed Service Requests and Incidents

DSS03—Managed Problems

DSS04—Managed Continuity

DSS05—Managed Security Services

DSS06—Managed Business Process Controls

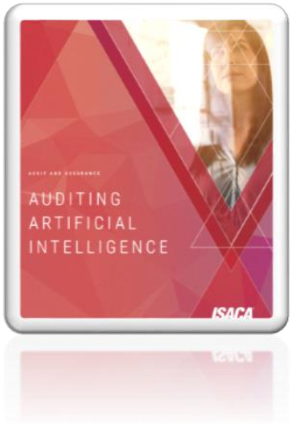
MEA01—Managed Performance and Conformance Monitoring

MEA02—Managed System of Internal Control

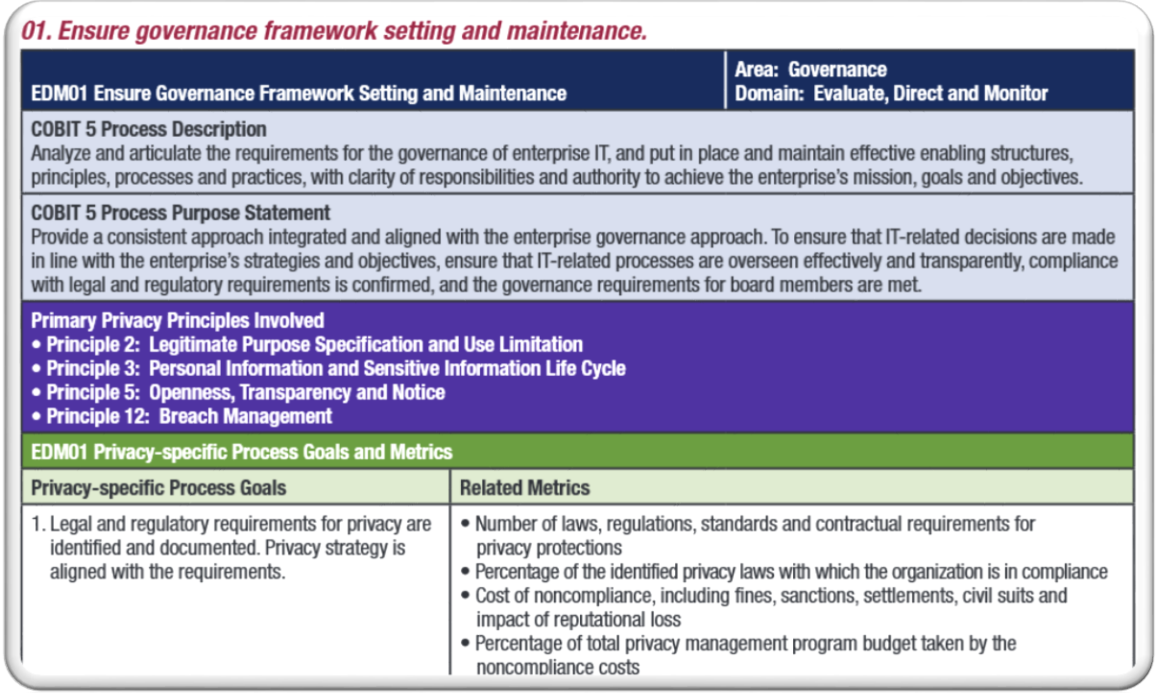
MEA03—Managed Compliance With External Requirements

MEA04—Managed Assurance

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



ISACA privacy principe linked to Cobit Control



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

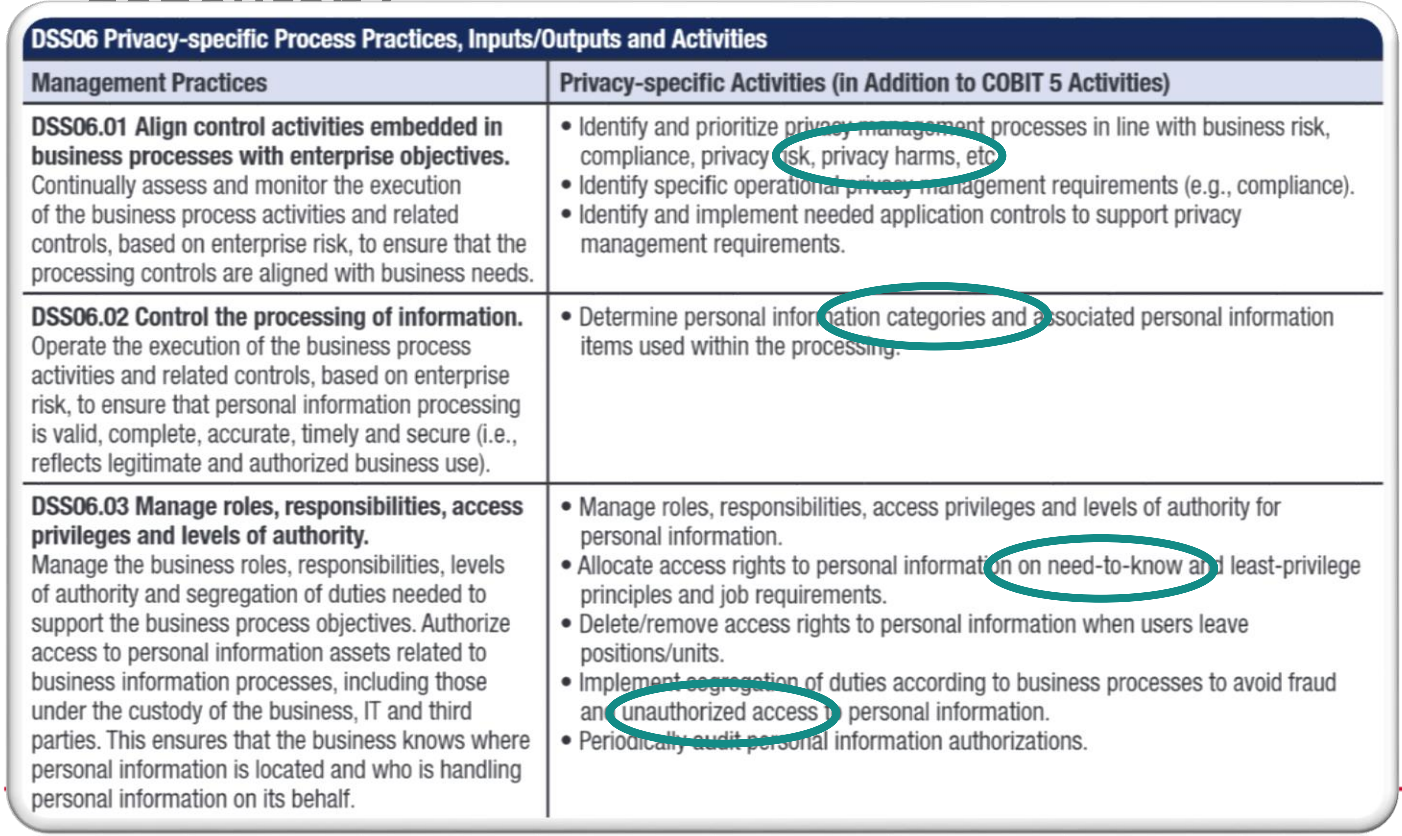
Specifiek DSS06 – Business Process Controls

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

Specifiek voor AI/Algoritmes 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 geldende wet&regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG).

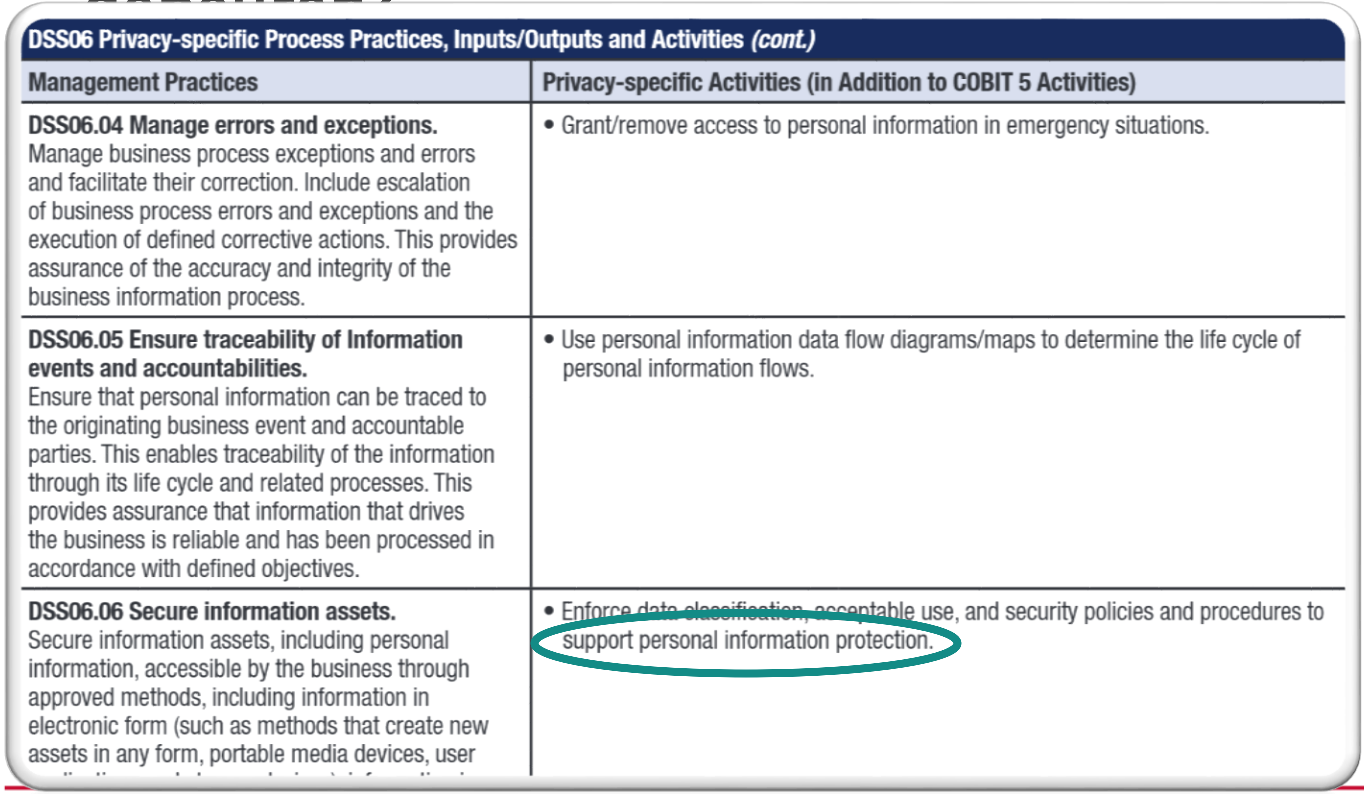
ISACA Cobit privacy – Wat moet er gebeuren?



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.

ISACA Cobit privacy – Wat moet er gebeuren?



DSS06 Privacy-specific Process Practices, Inputs/Outputs and Activities *(cont.)*

Management Practices	Privacy-specific Activities (in Addition to COBIT 5 Activities)
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate their correction. Include escalation of business process errors and exceptions and the execution of defined corrective actions. This provides assurance of the accuracy and integrity of the business information process.	• Grant/remove access to personal information in emergency situations.
DSS06.05 Ensure traceability of Information events and accountabilities. Ensure that personal information can be traced to the originating business event and accountable parties. This enables traceability of the information through its life cycle and related processes. This provides assurance that information that drives the business is reliable and has been processed in accordance with defined objectives.	• Use personal information data flow diagrams/maps to determine the life cycle of personal information flows.
DSS06.06 Secure information assets. Secure information assets, including personal information, accessible by the business through approved methods, including information in electronic form (such as methods that create new assets in any form, portable media devices, user	• Enforce data classification, acceptable use, and security policies and procedures to support personal information protection.

Algorithm Assurance & GDPR

- Questions?