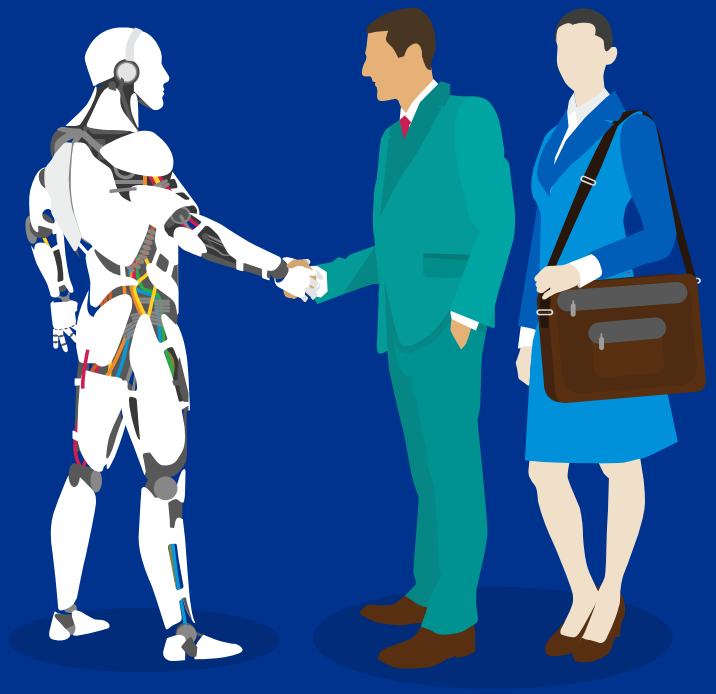
KPMG

AI Risk and Controls Matrix



Executive Summary

The era of AI is well and truly here – with huge implications for businesses across all sectors.

These are systems that can both interpret natural language and also learn to find the right answers without them having been programmed.

This innovation comes with a heightened level of risk. Businesses urgently need to recognise this new risk profile and rethink their approach to the risks and controls relating to this technology in a structured way.

This is essential for two main reasons:

1 AI will allow systems and businesses to become much more complex (to the point that it exceeds the capacity of the human mind to comprehend). The nature of this increased complexity is also self-perpetuating and although it might appear as simplification, it could well introduce 'technical debt'. Embedding controls in a system to mitigate technical debt after its implementation is typically far more costly than designing in the right controls at the start. Opportunities to build risk and control consideration by design will inevitably diminish over time and hence now is an optimal time to consider taking a positive and dynamic approach to building in control.

2 The use of such advanced technologies will become material for many organisations, possibly sooner than anyone expects. When the time arrives it will not be possible to get the right controls in place overnight and have the capability to manage the risks effectively, or to provide assurance. Hence it is key for governance, risk and compliance practices and capabilities to develop alongside the evolution of the usage of such technologies.

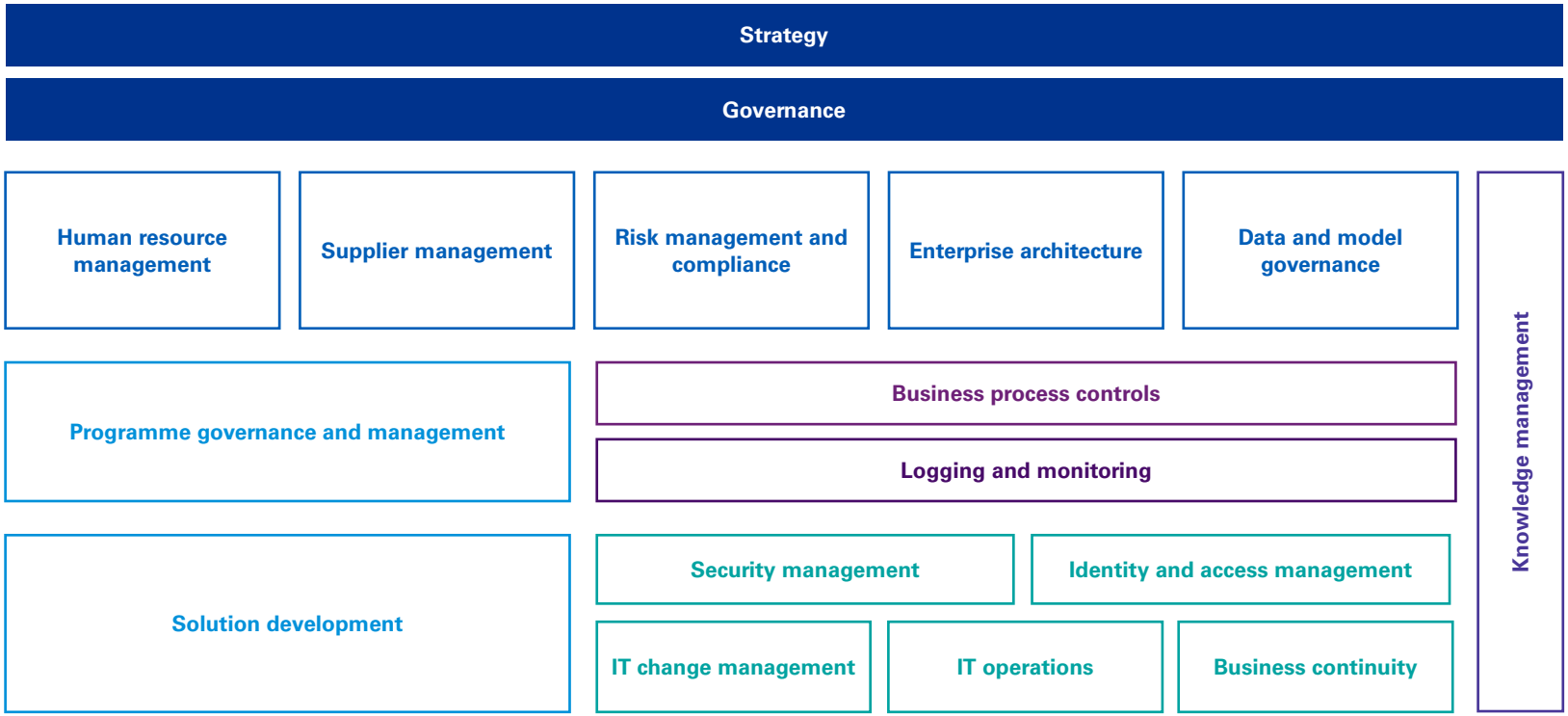
Risk and Control framework

The risk and control framework is designed to help those tasked with the safe delivery of AI. We have developed this framework specific to AI as a guide for professionals to use when confronted with the increasing use of AI in organisations across different levels of maturity. However, the guide might also be helpful for AI practitioners.

We have categorised risks into seventeen areas as set out in the diagram below and detailed further on the following page. Note that the framework represents an early attempt to provide a holistic approach to managing the risks around the use of AI, providing guidance to the audit and compliance community, and will continue to be refined over time.

We invite fellow IA professionals or AI practitioners with an interest in this area to contact **Andrew Shefford** or **Paul Holland** for further information on how to contribute and participate in this project.

With thanks to the many KPMG contributors and to Rafael Bambino, Fayyaz Cheema, Mark Kennedy, Thomas Nowacki, Paul Thomas and others for their involvement in this framework.



Please select a category for managing risks and controls for AI solutions.

Please select a category for managing risks and controls for AI solutions.

- **01 – Strategy**
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	1

Number of controls defined in the framework	2

01

Summarised risk
Lack of strategy

Control topic
Strategy

AI Risk description
Without a clear strategy toward the investment, development or application of Artificial Intelligence (AI), it can become inefficient, expose the entity to significant risk around inappropriate use of AI

AI Control description
The Enterprise has developed and maintains a strategy regarding the development and use of AI, providing direction to applying AI to deliver business value as well as to how that value is to be achieved in terms of Governance, Process, People and Technology.

AI specificity
High

COBIT process
APO02 Manage Strategy

Control subject
01-Strategy

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

02

Summarised risk
Lack of strategic alignment

Control topic
Review of the application of automation

AI Risk description
AI programmes (as well as the individual instances of AI) need to be aligned with and support the organisation's strategy, and be in line with the organisation's risk appetite.

AI Control description
AI solutions are regularly reviewed against the organisation's strategy and risk appetite to validate ongoing adherence and alignment.

This includes a regular review of what is being automated, and of the AI solutions and their learning algorithms, to ensure that the solutions still operate in line with the organisation's strategy.

AI specificity
High

COBIT process
MEA01 Monitor, Evaluate and Assess Performance and Conformance

Control subject
01-Strategy

COBIT area
Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- **02 – Governance**
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	7

Number of controls defined in the framework	8

01

Summarised risk
Compliance as a strategic objective

AI Risk description
A lack of trust in the use of innovative technologies restricts putting such solutions in production at scale, and/or further innovation investments

AI specificity
Medium

Control subject
02-Governance

Control topic
Compliance objective

AI Control description
Adequate risk management, and compliance with legal, regulatory as well as organisation's own requirements, is included as one of the strategic priorities (i.e. to drive trust in the use of innovative technologies)

COBIT process
APO02 Manage Strategy

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Misalignment to the organisation's cultural and ethical values

AI Risk description

Decisions made by the AI solution are not aligned to the organisation's cultural and ethical values, or cause bad or incorrect decisions by a human employee / AI solution, resulting in the organisation being held accountable.

Poor quality or incomplete data made available to the AI solution will impact the quality of the decision taken in terms of compliance with corporate values.

Without periodic reviews of the AI logic and the data used by the AI solution, it could deviate from the organisation's corporate values.

AI specificity

High

Control subject

02-Governance

Control topic

Values

AI Control description

Where applicable, ethical rules and corporate values are coded into the algorithms, and controls are in place to review the output (e.g. thresholds; list of acceptable outcomes; list of unacceptable outcomes). Changes to the ethical value code go through robust change management process. The controls should match the velocity and breadth of the process being controlled

During the design phase, a multidisciplinary team brainstorms about the potential ways the AI solution or its outcomes could be misused, e.g. if its outcomes, the AI solution or the company itself falls in to the 'wrong hands'.

Data is reviewed to ensure it is complete, accurate and free from bias.

Logic is reviewed and tested to verify that it remains valid, with specific testing to ensure there are no un-intended biases.

COBIT process

MEA02 Monitor, Evaluate and Assess the System of Internal Control

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Lack of a common language

Control topic

Common language and definitions

AI Risk description

Without a common language used for types of AI, there is a risk that the various parties involved in AI governance, implementation and management will have misunderstandings, resulting in ineffective decision making and risk management.

AI Control description

Definitions of different types of AI should be documented and shared to provide a common language across an organisation, e.g. through a glossary.

AI specificity

High

COBIT process

EDM01 Ensure Governance Framework Setting and Maintenance

Control subject

02-Governance

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

An unclear, hyped expectation or overconfidence in automation capability is not aligned with system maturity resulting in ineffective outcomes

Control topic

Managing expectations

AI Risk description

Unclear or hyped expectation and overconfidence in AI capability not aligned with system maturity resulting in ineffective outcomes.

AI Control description

The limitations of AI technologies, human elements in AI, as well as the AI state of maturity should be made clear and transparent by the sponsoring organisation or team to avoid hyped expectation and overconfidence in the implementation effort.

AI specificity

High

COBIT process

EDM05 Ensure Stakeholder Transparency

Control subject

02-Governance

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

An unclear, hyped expectation or overconfidence in automation capability is not aligned with system maturity resulting in ineffective outcomes

Control topic

Controlled evolutionary change

AI Risk description

Unclear or hyped expectation and overconfidence in AI capability not aligned with system maturity resulting in ineffective outcomes.

AI Control description

There is a process in place for continual nurturing AI by humans, as it matures through specific stages, mastering new and specific capabilities that meet well-defined requirements.

AI specificity

High

COBIT process

BAI05 Manage Organisational Change Enablement

Control subject

02-Governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk

Weakening enterprise governance mechanisms

AI Risk description

The use of AI technologies negatively impact existing enterprise governance mechanisms (i.e. the enterprise's level of control over data processing is weakened)

Control topic

Enterprise governance framework for automation

AI Control description

An enterprise governance framework for the use of AI is established and provides consistent governance over the overall programme of AI/ Bot developments - and ensures consistent quality. The program governance bodies should include representation from relevant business function, IT, Ethics, Data, Human Resources, Risk and other impacted divisions.

The enterprise governance framework is aligned with the entity's strategy and risk appetite - and covers the use of 'base level' automation (i.e. replicate human data entry and processing) as well as decision making (i.e. use of technology, incl. machine learning, to suggest or make decisions previously made by human operators).

The governance body oversees that existing policies are reviewed and where necessary amended for AI considerations. Alternatively, an enterprise-wide AI policy should be in place.

AI specificity

High

COBIT process

EDM01 Ensure Governance Framework Setting and Maintenance

Control subject

02-Governance

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Lack of a clearly defined ownership or operating model

Control topic

Ownership or operating model

AI Risk description

AI programme's or solution's ownership and management roles and responsibilities are unclear, increasing the risk of unauthorised or inappropriate developments, access, change, and/or incidents

Without a clearly defined operating model, governance structure, accountability and responsibility, there is a risk that the AI solution will not be successful, i.e. designed, implemented, maintained or supported, leading to undesired business outcomes end to end.

AI Control description

Clear organisational structure covering all elements of the AI lifecycle and control framework, as well as clear roles, responsibilities, accountabilities (e.g. a RACI) - including between business, IT and the AI CoE - with consideration to skills required, segregation of duties, authorities etc. This is to lead to appropriate controls matching the entity's risk appetite. The AI solution's human owner needs to be clearly defined. As the accountable party, the owner needs to have in place appropriate monitoring and supervision controls to prevent or override AI decisions. This applies to Enterprise wide Governance but also to a specific AI solution.

Roles and responsibilities are defined in organisational charts and job descriptions. Representatives from the AI CoE or governing body, AI developers, data scientists, business process owners, technical AI owners, application owners, operations, Service Desk, and security teams required for an effective AI environment are identified and integrated with relevant management processes.

The Operating model and governance mechanism and policies and procedures are clearly defined - at the enterprise level. This should be part of - or aligned to - existing technology management frameworks as applicable.

AI specificity

Medium

COBIT process

EDM01 Ensure Governance Framework Setting and Maintenance

Control subject

02-Governance

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk

Non-compliance with internal or external requirements

Control topic

Compliance monitoring

AI Risk description

Non-compliance with internal or external requirements in terms of risk management, internal control and compliance could lead to ineffective solutions, or regulatory or market repercussions

AI Control description

Compliance of the AI solution with the organisation's regulatory, governance, security and business continuity standards is reviewed on a periodic basis. This also allows the organisation to demonstrate compliance to others (management, Audit Committee, auditors, regulators, etc.).

AI specificity

High

COBIT process

MEA01 Monitor, Evaluate and Assess Performance and Conformance

Control subject

02-Governance

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

09

Summarised risk

Lack of exit scenarios

AI Risk description

The AI solution (algorithms, learning data, etc.) has evolved to a unique and complex solution that cannot be migrated to a different provider if and when required (lock in)

Without the ability to exit from an AI vendor or solution, there is a risk that the business cannot respond to change in the environment, e.g. aging technology or different business strategy, and is tied into the use of the AI vendor or solution.

AI specificity

High

Control subject

02-Governance

Control topic

Exit strategy

AI Control description

AI design standards require that an exit strategy is developed as part of the programme/ solution design. This includes:

* Exit clauses in contracts that include IP aspects of code, data and 'learnt logic' and notice period

* Portability treated as a key requirement in the architecture - this applies to the code, data, IT infrastructure, in- and external connections, etc.

* ESCROW arrangements in place to include continual capture of logic as well as core platform.

COBIT process

APO10 Manage Suppliers

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- **03 – Human resource management**
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	4

Number of controls defined in the framework	5

01

Summarised risk

Organisational and people impact of the automation strategy insufficiently addressed

AI Risk description

Unclear resourcing requirements (capacity and capability) in the AI strategy leads to excess/ shortage of staffing, over/under utilised vendor resources and lack of skilled resources required for designing, building, operating and maintaining AI systems. An undefined organisational roadmap for AI implementation leads to ineffective resource utilisation, decentralised approaches, redundancy or shortages in people and skills.

AI specificity

High

Control subject

03-Human resource management

Control topic

Human resource requirements

AI Control description

Requirements for human resources defined (e.g. recruitment, role profiles, training, retention strategy, third-parties involvement) are aligned with the AI strategy and roadmap.

Operational teams are scaled and trained according to the required level of capability and capacity.

COBIT process

EDM04 Ensure Resource Optimisation

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Poor development and/ or retention of human talent and resources

Control topic

Human resource requirements

AI Risk description

Poor development and/ or retention of human talent and resources may have an undesired effect on AI system or on the processes it enables, resulting in ineffective processes or solutions, or not aligning to the organisation's values, mission statements and business practices.

AI Control description

HR processes are in place to recruit, develop and retain human resources to ensure ongoing ability to operate a control environment around AI solutions when designing and implementing business and functional operations. This includes both AI-skilled people, e.g. to develop AI solutions, and non-AI-skilled resources, e.g. to retain business knowledge.

AI specificity

High

COBIT process

APO07 Manage Human Resources

Control subject

03-Human resource management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Insufficient IT knowledge retained/ developed to run and maintain effective automation solutions, and to overcome major incidents

Control topic

IT knowledge management and documentation

AI Risk description

Insufficient IT knowledge (staff and/ or skills) retained/ developed to effectively run and maintain the solution where handed over to the standing organisation (i.e. once the solution moves to sustain), leading to an ineffective AI solution, or to AI solutions becoming ineffective over time, and/ or poor decision making during major incidents.

AI Control description

For all key areas (see examples listed below), specific individuals have been assigned to fulfil the 'BAU' / sustain related roles. These individuals have the right skills, have been given relevant knowledge from the Development team, and have been trained to fulfil their responsibilities (i.e. there is appropriate and regular training conducted for users who are training, testing and managing/ supervising AI solutions).

Required IT skills have been determined and prioritised by identifying critical resources, and establishing career paths to retain and develop critical skills.

HR processes are in place to retain resources to ensure ongoing ability to operate a control environment around AI solutions when designing and implementing business and functional operations. I.e. managing AI solution is reliant on extensive knowledge and subject matter expertise. As the solution matures, it becomes less reliant on SME input, however it is still required to retain the SME knowledge, also to respond to incidents.

People skills for Sustain mode, across:

- Governance / Risk management / Security
- Human resource management
- Enterprise architecture, Supplier management and Asset management
- Data and model governance
- IT operations and change management
- Business continuity, availability and disaster recovery.

AI specificity

High

COBIT process

APO07 Manage Human Resources

Control subject

03-Human resource management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	4

Number of controls defined in the framework	4

01

Summarised risk
3rd party controls

Control topic
3rd party controls

AI Risk description
Entity's risk exposure or performance are negatively impacted by 3rd parties that operate a lower level of control maturity and / or security standards

AI Control description
3rd parties are subject to at least the same level of control, either by applying the actual same controls (e.g. 3rd party users are managed just as own staff are), or through the right to audit, or through external assurance reports (e.g. ISAE3000 or 3402) that provide assurance on all relevant controls, or through other appropriate means. This includes 3rd parties being integrated with the wider governance and risk management approach. E.g. AI processes performed by vendors are included in the organisation's DR and BCP testing cycles, subject to the same security controls, etc.

AI specificity
Low

COBIT process
APO10 Manage Suppliers

Control subject
04-Supplier management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Reliance on third parties

Control topic

Third party reliance

AI Risk description

High reliance on specific 3rd party providers (supplier concentration risk) may result in single supplier dependency and concentration risk.

AI Control description

To ensure full ongoing visibility of the risk/ control as well as performance impact of using 3rd parties, both as part of the development as well as during sustain:

a) A Supplier inventory (see C.21) is complemented with information about dependencies between 3rd parties (and sub-providers) and their criticality, to manage supplier concentration and dependency risks

b) Supplier relations are formalised in contracts, with clear SLAs, SOPs, etc.

c) The performance of third parties, both on the solution's performance and risk, is frequently monitored and where necessary action is taken in a timely manner.

AI specificity

Low

COBIT process

APO08 Manage Relationships

Control subject

04-Supplier management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Lacking inventory of related service providers

Control topic

Third party identification

AI Risk description

Lack of up to date understanding of all third parties involved in the design, build and/ or operation of the AI solution undermines the effectiveness of several other controls incl. risk and compliance, security, IT operations and business continuity.

AI Control description

To ensure full ongoing visibility of all parties involved in providing the overall solution, both as part of the development as well as during sustain:

a) An inventory of all third party providers and sub-providers is maintained, including their roles

b) An assessment is performed periodically on the end-to-end 'supply chain' of third party providers and sub-providers to validate the supplier inventory is accurate.

AI specificity

Low

COBIT process

APO08 Manage Relationships

Control subject

04-Supplier management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk
Black box solution risks

Control topic
Contracts

AI Risk description
The logic within the AI solution is not fully understood, impacting the ability to recover services when issues occur, impacting business operations and resulting in financial loss (i.e. the risks around 'a black box solution') or reputational damage.

AI Control description
For third party solutions or parts thereof, the contract includes clauses for ownership of IP (i.e. ownership of data, code, models and of 'learning'); escrow agreements to have access to the code if need be, right to audit and clear supplier/customer roles and responsibilities

See also C.85 for a repository of relevant IP.

AI specificity
Medium

COBIT process
APO10 Manage Suppliers

Control subject
04-Supplier management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- **05 – Risk management and compliance**
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	2

Number of controls defined in the framework	6

01

Summarised risk

Non-compliance with internal or external requirements

Control topic

Risk management and compliance within the governance framework

AI Risk description

Non-compliance with internal or external requirements in terms of risk management, internal control and compliance could lead to ineffective solutions, or regulatory or market repercussions

AI Control description

Risk management and compliance is appropriately covered by the AI governance model and risk, compliance and security representatives are part of the governance and management mechanism where appropriate. Risk acceptance and oversight processes are in place.

Note: This control applies to the overall governance level (e.g. at programme level) and see control C.32 for the risks and internal control framework for a specific AI solution.

AI specificity

Medium

COBIT process

EDM03 Ensure Risk Optimisation

Control subject

05-Risk management and compliance

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- **05 – Risk management and compliance**
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

02

Summarised risk

Non-compliance with internal or external requirements

Control topic

Internal or external requirements

AI Risk description

Non-compliance with internal or external requirements in terms of risk management, internal control and compliance could lead to ineffective solutions, or regulatory or market repercussions

AI Control description

Internal and external requirements in terms of risk management, internal control and compliance are identified, their relevance is assessed through risk and impact analysis, and relevant requirements are incorporated in the both the programme and the sustain model. This can include requirements for Sarbanes Oxley compliance, industry-specific regulation, relevant ISO certifications, etc.

AI specificity

Low

COBIT process

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Control subject

05-Risk management and compliance

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Non-compliance with internal or external requirements

Control topic

Data protection and privacy

AI Risk description

Non-compliance with internal or external requirements in terms of risk management, internal control and compliance could lead to ineffective solutions, or regulatory or market repercussions

AI Control description

Specifically for data captured, processed and/or created through/by the AI solution, requirements for protecting the confidentiality, integrity and availability of data are assessed, evaluated and compliance thereof is monitored.

This includes data privacy, for which the European General Data Protection Regulation (GDPR) requirements are embedded within existing risk management methodologies and policies.

Data flows are mapped and privacy considerations identified, and include requirements for the secure storage and timely disposal of privacy related data.

Privacy related data inventories are maintained and compliance with privacy requirements is monitored.

Privacy notices and consent forms/tracking are issued and managed.

AI specificity

Low

COBIT process

APO12 Manage Risk

Control subject

05-Risk management and compliance

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- **06 – Enterprise architecture**
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	6

Number of controls defined in the framework	7

01

Summarised risk

Lack of Intelligent Automation architecture

Control topic

RPA architecture and development methodology

AI Risk description

AI/ Automation architecture, approach and development methodology have not been defined to ensure consistent quality and level of control, and hence the specific AI solution might not leverage the collective (planned) scale of all automated solutions to establish efficient and well controlled shared platforms.

AI Control description

An enterprise AI architecture has been defined (potentially offering multiple models for different types of solutions), covering preferred technologies, design concepts such as logging, security controls and monitoring requirements, and 'portability' (see C.17). This architecture clearly positions the AI part within the wider IT landscape (i.e. within the ecosystem within which it operates).

AI solutions should consider taking advantage of cloud computing capabilities (e.g. flexible, scalable, etc.) where appropriate.

AI specificity

Medium

COBIT process

APO03 Manage Enterprise Architecture

Control subject

06-Enterprise architecture

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Explainability not embedded in the design

Control topic

Explainability by design

AI Risk description

AI solutions lack the functionality to explain how they came to certain outcomes/ decisions/ advice - and are too complex for even their human designers to fully comprehend. As a result it may not be possible to evidence effective end-to-end controls or that risks are effectively managed.

AI Control description

W'Explainability' is integrated into the AI solution's requirements and hence included as one of the functional requirements of the overall solution and covered by other control areas such as design, build, test, etc.

'Explainability' is implemented in such a way that it ensures that it captures data that have led the solution to decide/ advise what it did, which it can generate on request, e.g. to a human SME to be able to challenge the AI solution (e.g. when the AI suggested an unusual medical procedure), or to meet external requirements (e.g. to allow the company to explain to a human consumer why their loan request has been denied). Such requirements include capturing any instances on human users 'overriding' the solutions 'advise'.

AI specificity

High

COBIT process

BAI02 Manage Requirements Definition

Control subject

06-Enterprise architecture

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Security by design' not implemented

Control topic

Security by design policies, standards and methodology

AI Risk description

Security by design' principles have not been embedded in the AI/ automation architecture, approach and development methodology to ensure appropriate and sustainable level of security.

AI Control description

A development methodology and policies and standards are in place to ensure 'security by design', i.e. that the AI solution, middleware and other relevant technology components - across the IT stack (network, OS, database and application level) - as well as (permanent and temporary) data storage, are securely configured in line with enterprise security policies and standards. Security setup of the virtual environments (e.g. hypervisor access) is aligned with the corporate security standards and practices.

This control includes 'privacy by design' considerations as required under the European General Data Protection Regulation (GDPR), see C.14.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

06-Enterprise architecture

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Software licence noncompliance

Control topic

Software licences and management

AI Risk description

Software licence requirements are not met across the AI environment and/or the connecting systems, which could have operational, financial or legal impacts.

AI Control description

Appropriate software licences have been obtained for all components of the AI solution and a mechanism is in place to renew these in a timely manner.

Potential licensing impact of the AI solutions accessing core systems has been determined and where appropriate additional licences have been obtained.

AI specificity

Low

COBIT process

BAI09 Manage Assets

Control subject

06-Enterprise architecture

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk
Lack of architectural segregation

Control topic
Architectural segregation

AI Risk description
Lack of architectural segregation, especially in a cloud / multi-tenant model, can lead to security and/ or solution and data integrity risks, which could result in financial loss or reputational damage.

AI Control description
An IT architecture principle is in place that helps ensure that AI's solution components and its data are segregated from other IT infrastructure/ cloud components, to protect AI integrity and outcomes. Robust controls should especially be in place to ensure logical segmentation of AI solutions in a multi-tenant cloud model.

AI specificity
Medium

COBIT process
APO03 Manage Enterprise Architecture

Control subject
06-Enterprise architecture

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk

Insufficient availability of automation solution

Control topic

High availability while retaining decision integrity

AI Risk description

AI solutions are insufficiently available, e.g. due to technical issues, impacting business operations and resulting in financial loss.

AI Control description

An IT architecture principle is in place that helps ensure that AI solutions are 'resilient-by-design', i.e. meet high availability requirements. However, it should prevent the 'split brain effect' (i.e. more than one instance of an AI solution running in parallel (hot-hot), both using the same data, potentially learning differently).

This means that the architecture has no single points of failure, i.e. all components and connection in the solution are (multi)redundant to ensure a truly high availability solution. This is to include external data connections and ideally also alternative data sources for such connections.

AI specificity

Medium

COBIT process

BAI04 Manage Availability and Capacity

Control subject

06-Enterprise architecture

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- **07 – Data and model governance**
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	7

Number of controls defined in the framework	10

01

Summarised risk
Unclear data governance roles and responsibilities

Control topic
Data ownership

AI Risk description
Unclear roles and responsibility within the data governance processes, resulting in regulatory, financial, resilience and reputational impact.

AI Control description
Roles to manage data and its ownership are defined (data owner, data steward, learning owner, algorithm owner, etc.)

See also C.11 and C.42.

AI specificity
Medium

COBIT process
APO03 Manage Enterprise Architecture

Control subject
07-Data and model governance

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Data corruption due to unintended interaction with other systems

Control topic

Data contamination

AI Risk description

Interaction between the AI solution and other entities, data sources or (cloud based) systems results in the corruption of data input or output, impacting business operations and resulting in financial loss or reputational damage. (see also to R.42).

AI Control description

Identify and monitor data transfer between AI systems of entities to detect indications of compromised appropriateness (ideally through automation).

Where such a compromise is detected, take appropriate action.

Where the AI systems are in an IaaS or a PaaS environment ensure that the service provider has appropriate controls in operation and that compromises are reported promptly and fully.

See also C.51.

AI specificity

Medium

COBIT process

BAI10 Manage Configuration

Control subject

07-Data and model governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Data corruption due to unintended interaction with other systems

Control topic

Data source approval

AI Risk description

Interaction between the AI solution and other entities, data sources or (cloud based) systems results in the corruption of data input or output, impacting business operations and resulting in financial loss or reputational damage. (seel also R.41).

AI Control description

All (changes to) data sources - internally or externally - which interacts with the AI solution, are monitored and documented and changes require human approval in advance, which includes a risk assessment and an assessment to validate data quality.

AI specificity

Medium

COBIT process

BAI09 Manage Assets

Control subject

07-Data and model governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk
Poor data quality

Control topic
Data governance

AI Risk description
Inadequate data governance controls, over either learning or production data, leading to an ineffective AI solution or incorrect/ unreliable output.

AI Control description
Data governance policies, standards and processes are in place to ensure that high quality data exists throughout the complete lifecycle covering all relevant quality aspects (i.e. availability, usability, integrity and security). Relevant parts of the 'learning data' are 'held back' to be used during testing and quality control and (different) parts are retained for future verification and/or audit purposes.

AI specificity
Medium

COBIT process
BAI09 Manage Assets

Control subject
07-Data and model governance

COBIT area
Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk
Poor hypothesis quality

Control topic
Hypothesis governance

AI Risk description
Inadequate governance controls around hypotheses leading to an ineffective AI solution or incorrect/ unreliable output.

AI Control description
Hypothesis governance policies, standards and processes are in place to ensure that hypothesis remain relevant and appropriate throughout the complete lifecycle covering all relevant quality aspects (i.e. availability, usability, integrity and security).

AI specificity
High

COBIT process
BAI09 Manage Assets

Control subject
07-Data and model governance

COBIT area
Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk
Poor algorithms quality

Control topic
Algorithms governance

AI Risk description
Inadequate governance controls around algorithms leading to an ineffective AI solution or incorrect/ unreliable output.

AI Control description
Algorithms governance policies, standards and processes are in place to ensure that algorithms remain relevant and appropriate throughout the complete lifecycle covering all relevant quality aspects (i.e. availability, usability, integrity and security).

AI specificity
High

COBIT process
BAI09 Manage Assets

Control subject
07-Data and model governance

COBIT area
Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Incorrect results

Control topic

GDPR

AI Risk description

The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description

Controls are in place to maintain the ability to ensure completeness whilst adhering to GDPR and other privacy regulations, and to ensure privileged information is correctly used.

See also C.14.

AI specificity

Low

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

07-Data and model governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk
Incorrect results

Control topic
Data quality monitoring

AI Risk description
The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results

AI Control description
Controls are in place for monitoring data quality for solutions that are evolving over time (i.e. 'data drift', data changing in outcome over time, so training data may not provide the right indicators). Consider data volume in consideration of learning/ outcome quality.

AI specificity
High

COBIT process
DSS01 Manage Operations

Control subject
07-Data and model governance

COBIT area
Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

09

Summarised risk

Incomplete populations or inaccurate data used

Control topic

Completeness of data

AI Risk description

Incomplete populations or inaccurate data is used by the AI solution, resulting in a poor / incorrect outcomes/ decisions.

AI Control description

Controls are in place around the completeness and accuracy of the data sets used by the AI solution, e.g. to support the decision making process, and can be demonstrated and proven.

AI specificity

Medium

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

07-Data and model governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Incomplete populations or inaccurate data used

Control topic

Completeness of data

AI Risk description

Incomplete populations or inaccurate data is used by the AI solution, resulting in a poor / incorrect outcomes/ decisions.

AI Control description

Controls are in place to have reasonable assurance that sufficient data (e.g. covering a time period or sufficient variations in the population) was provided to enable the model to generate accurate results.

AI specificity

High

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

07-Data and model governance

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	3

Number of controls defined in the framework	4

01

Summarised risk
Lack of strategic alignment

Control topic
Business case

AI Risk description
AI programmes (as well as the individual instances of AI) need to be aligned with and support the organisation's strategy, and be in line with the organisation's risk appetite.

AI Control description
The overall AI objectives and business case is aligned to the organisation's overall strategy. Principles for determining activities that are/ are not suitable for AI must be defined. Additionally, some activities may be conditionally approved for AI, subject to having appropriate measures to mitigate the risks of migrating activities to AI. The determination of activities being suitable or not for AI will be driven by regulatory, cultural, commercial or other considerations, and should be aligned to the entity's strategy.

AI specificity
Medium

COBIT process
APO02 Manage Strategy

Control subject
08-Programme governance and management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Poor programme management methodology

Control topic

Programme management

AI Risk description

No appropriate programme management methodology is in place to manage the development of the AI solution to ensure it meets strategic and business requirements.

AI Control description

An appropriate programme management methodology is in place to manage the development of the AI solution to a successful outcome (i.e. it meets strategic and business requirements). This includes clear stage gate approvals, User Acceptance Testing (UAT), and issue and risk management, irrespective of whether a waterfall or agile development methodology is used.

AI specificity

Medium

COBIT process

BAI01 Manage Programmes and Projects

Control subject

08-Programme governance and management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Poor benefits management

Control topic

Benefits management

AI Risk description

Benefits management has not been implemented leading to lack of transparency on return on investment and realisation of strategic and business requirements.

AI Control description

The realisation of estimated 'benefits' is systematically managed and measured during the solutions life time (e.g. at short, medium and long term after go-live).

Mechanisms have been designed and implemented to measure/ articulate:

1) the total cost of ownership including trends over time

2) the realisation of expected benefits (e.g. quantitatively such as speed and accuracy of processes, FTE savings, etc. - as well as qualitatively (e.g. confidence in quality of decision making).

The realised benefits are leveraged to drive appetite and trust in innovative technologies, and possibly used to fund further investments.

AI specificity

Low

COBIT process

EDM02 Ensure Benefits Delivery

Control subject

08-Programme governance and management

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Lack of independent programme assurance (IPA)

Control topic

Programme assurance

AI Risk description

Lack of independent assurance over the programme's ability to achieve a successful outcome leaves some of the programme's risk undetected.

AI Control description

The programme has engaged an independent function or service provider to provide assurance to the Programme Sponsor, Executive Management and/or other stakeholders such as the Audit Committee, for the duration of the programme over the manner in which the programme has been set-up and managed to deliver a successful outcome (i.e. meets the requirements in terms quality, costs, benefits, internal control, compliance, etc.).

AI specificity

Low

COBIT process

EDM02 Ensure Benefits Delivery

Control subject

08-Programme governance and management

COBIT area

Evaluate, Direct and Monitor

Please select a category for managing risks and controls for AI solutions.

Number of risks defined in the framework	10

Number of controls defined in the framework	16

01

Summarised risk

Lack of business case

Control topic

Business case

AI Risk description

AI programmes without a valid business case might not deliver ultimate value to the entity, might jeopardise the programmes continuation, or might impact stakeholder's perceptions and expectations about the value AI could add to the organisation.

AI Control description

A clear business case for the AI solution is in place and formally approved by relevant stakeholders - and being kept up to date to reflect any changes in expected total cost of ownership and/or benefits.

Individual AI solutions are assessed in the context of the organisation's strategy. The expected benefits of the AI solution should be clearly articulated and tracked during the course of the program and post-implementation. Benefits may be hard (e.g. reduction in headcount) or soft (e.g. deeper understanding of a client resulting in a better interaction). Accounting policies should be leveraged, and if required enhanced, to correctly capturing the costs and the value of AI-initiatives.

AI specificity

Low

COBIT process

BAI01 Manage Programmes and Projects

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Poor design and development methodology

Control topic

Development standards

AI Risk description

AI design and development methodology are not consistently set-up to ensure a successful delivery of an AI automation programme.

AI Control description

An AI development standard is in place, is integrated with the broader development standards and is followed for all AI developments.

The standard includes defined stage gates, stage entry and exit criteria and go/no go decisions.

Examples include:

- Entanglement: Prevent machine learning systems to mix signals together, as that entangles them and makes it difficult to isolate improvements.
- Unintended use: Prevent AI's consumers to be 'undeclared', i.e. unknowingly using the output of a given AI solution or model as an input to another system which may cause interdependencies to be poorly understood and may cause hidden feedback loops.
- Unstable data dependencies: Monitor input signals to ensure continued appropriate usage, as they can change over time, possibly unknowingly e.g. when the ownership of the input signal is separate from the ownership of the model that consumes it.
- Technical debt: Prevent AI systems from becoming too complex for humans to comprehend.

AI specificity

High

COBIT process

APO11 Manage Quality

Control subject

09-Solution development

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Poor knowledge of As-Is processes

Control topic

As-is business process documentation during Design

AI Risk description

Lack of understanding of current As-Is processes, including internal controls, reduces the ability to design effective automation solutions in an efficient manner.

AI Control description

During the Design phase(s), 'pre-automation' process narratives and/or flowcharts are available including process variations and possible exceptions. The impact of automation on current processes and internal controls has been assessed, e.g. through the help of process mining software that visualises actual processes based on the organisation's transactional data.

AI specificity

Low

COBIT process

BAI02 Manage Requirements Definition

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Poor knowledge of To-Be processes

Control topic

To-be process documentation / user stories during Design

AI Risk description

To-Be process model flowcharts and user stories (including IT general and business process controls) are not complete or accurate, or have not been approved, and reduces the ability to design effective automation solutions in an efficient manner.

AI Control description

Documentation of user stories and end-to-end process flows, including the parts that are to be automated by AI, is available, kept up to date, with evidence of appropriate consideration of business input, and approved by the programme sponsor.

Internal controls (including financial and operational controls) are documented and linked within the design documentation, and are designed to ensure a consistent effective operation of the AI solution as well as to detect potential exceptions.

AI specificity

Medium

COBIT process

BAI02 Manage Requirements Definition

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

Risks and controls not been defined

Control topic

Risks and controls framework

AI Risk description

Risks and controls have not been explicitly defined for the solution, or controls have not been optimised, causing either an ineffective or inefficient internal controls environment.

AI Control description

Risks and controls overviews have been established for all key areas, including the solution, self learning capabilities, interfaces, management processes, KPIs, etc.

Completeness of risks has been ensured through a structured risk assessment process with involvement of all stakeholders.

Controls are in place to effectively and efficiently address the identified risk in a sustainable manner.

An assessment of the post-deployment process, incorporating the AI solution, is completed to validate that the solution will operate in compliance with the organisation's policies and procedures, and any applicable regulations.

AI specificity

Low

COBIT process

APO12 Manage Risk

Control subject

09-Solution development

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk
Not all controls are implemented

Control topic
Implement controls

AI Risk description
The developed solution does not include all designed processes and internal controls requirements and as a result does not offer an effective automation solution.

AI Control description
The development process has been set-up to ensure that processes and internal controls are developed in line with the design, i.e. are either configured or hard-coded within the AI solution.

AI specificity
Low

COBIT process
DSS06 Manage Business Process Controls

Control subject
09-Solution development

COBIT area
Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Activities performed by the Bot cannot be traced back to a specific solution or account

Control topic

Bot identification

AI Risk description

The design does not ensure that activities performed by - or through - a Bot / an AI solution can be traced back to a specific Bot or user account, which limits the effectiveness of the logging and monitoring activities.

AI Control description

The AI solution's activities can be traced back to a unique Bot (e.g. through static IP address).

An end-to-end audit trail is in place to log activities.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

09-Solution development

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk

Inappropriate relationships between variables/ hypotheses

Control topic

Relationship models

AI Risk description

The relationship between variables / events, or between hypotheses, are incorrectly defined resulting in incorrect results, e.g. mistaking correlation for causality.

AI Control description

Quality controls exist to help ensure the appropriate relationships between variables / events and hypotheses are defined, including interdependencies and distinguishing correlation and causality (e.g. through Bayesian statistics, Hybrid Monte Carlo methods, or causal models such as Granger non-linear causality, Neyman–Rubin, Pearl and/or Granger).

AI specificity

High

COBIT process

BAI02 Manage Requirements Definition

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

09

Summarised risk

Insufficient testing of the automation solution

Control topic

Develop and test environments

AI Risk description

Insufficient testing of the automation solution, resulting in a solution that does not meet business requirements and strategic objectives.

AI Control description

Separate environments (e.g. virtual servers matrix) are available and are consistent, and used for development, QA/ test and production, to allow for testing being performed with a due diligence in the environment identical to production (Note: AI has a dynamic element that will make this only partially effective).

AI specificity

Medium

COBIT process

BAI04 Manage Availability and Capacity

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

10

Summarised risk

Insufficient testing of the automation solution

Control topic

Test approach

AI Risk description

Insufficient testing of the automation solution, resulting in a solution that does not meet business requirements and strategic objectives.

AI Control description

Testing and Production/Go-live strategy and approach are defined and followed, including data migration between environments and contingency planning.

AI specificity

Low

COBIT process

BAI07 Manage Change Acceptance and Transitioning

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk
Insufficient testing of the automation solution

Control topic
Test approvals

AI Risk description
Insufficient testing of the automation solution, resulting in a solution that does not meet business requirements and strategic objectives.

AI Control description
Appropriate User Acceptance Testing (UAT) for the solution is performed with appropriate consideration of business input for design, execute and approve testing, and signed off prior to be accepted. Documentation of test cases and approvals for each AI solution is retained.

AI specificity
Low

COBIT process
APO11 Manage Quality

Control subject
09-Solution development

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Incorrect results

Control topic

Next best action

AI Risk description

The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description

The code is designed to ensure that the algorithms determine 'the next best alternative action' when an initially preferred option is not available (e.g. "blocked roads").

AI specificity

High

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk
Incorrect results

Control topic
Unbiased

AI Risk description
The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description
Controls are in place to consider sensitivities when dealing with different ethical/ political/ ethnic/ race/ gender/ cultural etc. groups.

AI specificity
High

COBIT process
BAI03 Manage Solutions Identification and Build

Control subject
09-Solution development

COBIT area
Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk
Incorrect results

Control topic
Sensitivities

AI Risk description
The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description
Learning data is reviewed for data bias and validated through testing.

AI specificity
High

COBIT process
BAI03 Manage Solutions Identification and Build

Control subject
09-Solution development

COBIT area
Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Incorrect results

Control topic

Timely sync of data

AI Risk description

The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description

Controls are in place to ensure that when data is sourced/ used, the time scale of the data from the source is aligned with the time scale the AI system is using.

AI specificity

Medium

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Incorrect results

Control topic

Duplicate data processing

AI Risk description

The results from the AI solution are incorrect or otherwise inappropriate, e.g. due to the model not accurately reflecting the true underlying quantitative parameters, or because the logic makes inaccurate decisions or uses flawed assumptions, leading to incorrect results.

AI Control description

Controls are in place to prevent the AI solution from processing the same data more than once, including file and data validation checks.

AI specificity

Medium

COBIT process

BAI03 Manage Solutions Identification and Build

Control subject

09-Solution development

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- **10 – Business process controls**
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	Number of controls defined in the framework
To be determined for each solution	To be determined for each solution

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- **11 – Logging and monitoring**
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	2	Number of controls defined in the framework	3

01

Summarised risk

Lack of monitoring of the outcomes of automation solutions

Control topic

Monitoring of outcomes

AI Risk description

Without adequate monitoring of the outcomes of the solution, it could:

a. not behave as intended when designed and implemented (outcomes monitoring against original business requirements / ethics requirements / corporate values etc.)

b. have bad responses or decision times

AI Control description

Through use of Data Analytics / MI on the audit trails, management regularly reviews the solution outcomes (e.g. reports that have been designed and built to measure the performance of the AI solution) against the business requirements from ethical to functional. Controls work at the same pace as the activities that are monitored (decision and operational velocity)

See C.80 for Operational monitoring and C.15 and C.33 for risk monitoring.

AI specificity

High

COBIT process

MEA01 Monitor, Evaluate and Assess Performance and Conformance

Control subject

10-Logging and monitoring

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Inadequate monitoring impacts overall effectiveness

AI Risk description

Auditability or monitoring requirements for AI operations are not implemented, impacting the ability to monitor continued effectiveness of operations, as well as the analysis of / timely response to potential incidents.

AI specificity

High

Control subject

10-Logging and monitoring

Control topic

Operational monitoring

AI Control description

An overall real-time monitoring/ alerting framework/ mechanism is in place to detect any anomalies in the end-to-end operation of the AI processes, controls, systems and/or data.

Sensors and detailed logging is enabled to capture and review each AI solution's transactions/ activities.

Both KPIs (Key Performance Indicators) and KRIs (Key Risk Indicators) have been defined to form the basis for effective monitoring and include the operation of business process controls.

Operational events have been defined to trigger alerts which are followed-up on where relevant.

Detailed logs are maintained to obtain last execution status in case the AI solution fails.

See also C.19 around overall management review of performance and C.12/ C.33 re monitoring risk.

COBIT process

MEA01 Monitor, Evaluate and Assess Performance and Conformance

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Inadequate monitoring impacts overall effectiveness

Control topic

Operational monitoring

AI Risk description

Auditability or monitoring requirements for AI operations are not implemented, impacting the ability to monitor continued effectiveness of operations, as well as the analysis of / timely response to potential incidents.

AI Control description

Automated stop/loss controls should be considered in the technical design of the AI solution so that unintended behaviour is stopped or paused in a timely manner.

An override process is in place for exceptions (whether this requires escalation / emergency 'stop button' / automated stop and hold until released after human interaction etc.)

Exceptions are assessed for risk and performance against risk appetite and business impact/ criticality, and take inter-dependencies in to consideration.

Where appropriate, automated checks exist to help manage exceptions.

AI specificity

Medium

COBIT process

MEA01 Monitor, Evaluate and Assess Performance and Conformance

Control subject

10-Logging and monitoring

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	5

Number of controls defined in the framework	5

01

Summarised risk
Inconsistent security management

Control topic
Security management

AI Risk description
Security over the AI environment or related systems is not controlled with consistently quality, increasing the risk of unauthorised changes, system availability, data loss and other incidents

AI Control description
The AI environment follows a consistent security management approach with clear procedures and work instructions. This approach is integrated with the 'regular' security management approach to ensure a consistent approach across the AI and related environments. This applies to code, algorithms, configuration, IT infrastructure, applications, data structures and data classification and related management processes. Security management is aligned to good practice standards (e.g. ISO 27001).

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
11-Security management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Inconsistent security management

Control topic

Auditability

AI Risk description

Security over the AI environment or related systems is not controlled with consistently quality, increasing the risk of unauthorised changes, system availability, data loss and other incidents

AI Control description

Data and algorithms used for generating AI results/ decisions, including data used for system learning, are stored securely, can be retrieved in a timely manner and in accordance with regulations (e.g. data privacy) so provenance of decisions can be provided and hence AI outcomes can be independently validated. This include access controls, controls to prevent data from being overwritten or simplified (loss of context), controls around log generated data.

This could be achieved through applying the 'vault principle', i.e. an automated solution that securely stores any decision made by the solution, as well as the data the decision was based on, and the latest version of the algorithm. See also C.23 and C.80.

AI specificity

High

COBIT process

APO13 Manage Security

Control subject

11-Security management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Insufficient protection against malware

Control topic

Vulnerability and malware management

AI Risk description

Malware or new vulnerabilities might not be detected and expose the AI environment to security risks, leading to operational, financial or reputational losses.

AI Control description

Malware protection is in place and availability of new patches is continuously monitored, and where applicable an impact assessment is performed before the patch gets implemented in a timely manner.

Specifically for self-learning components, besides system and data protection, 'malware controls' are also to include protection of the 'learning', i.e. protect against mailicious attacks to attempt to influence the learning capabilities in an inappropriate manner.

Also see Control C.24 for the server hardening control.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

11-Security management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk
Insecure data

Control topic
Security management

AI Risk description
Data used for learning and automated processing is inappropriately changed, leading to operational, financial or reputational losses.

AI Control description
AI's input datasets are configured securely against human or machine intervention. Where relevant, completeness and accuracy checks are automatically performed on the data input.

AI specificity
Medium

COBIT process
APO11 Manage Quality

Control subject
11-Security management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk
Insecure temporary data

Control topic
Security management

AI Risk description
Creation and usage of insecure temporary files leaves AI solution, or related systems vulnerable to unauthorised data manipulation or loss.

AI Control description
Code and data storage as well as network communications to/ from/ within the AI solution are adequately encrypted.

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
11-Security management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk
Security testing

Control topic
Security management

AI Risk description
Security weaknesses might not be detected and expose the AI environment to security risks, leading to operational, financial or reputational losses.

AI Control description
Penetration tests or 'Red-team' reviews are performed to assess the AI environment's exposure to vulnerabilities.

Periodic security testing is performed to ensure security controls, sensors, and monitoring is operational.

AI specificity
Low

COBIT process
DSS05 Manage Security Services

Control subject
11-Security management

COBIT area
Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- **13 – Identity and access management**
- 14 – IT change management
- 15 – IT operations
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	7

Number of controls defined in the framework	13

01

Summarised risk
Unique accounts

Control topic
Access accountability for Bot accounts

AI Risk description
Lack of ownership and accountability for access to the AI solution - and/or for the Bots' access to connecting systems - increases the risk of inappropriate access, leading to operational, financial or reputational losses.

AI Control description
All accounts used by AI/ Bots are unique, and have been assigned to a human with ultimate responsibility for these.

For each Bot, usage of its account is tracked in between applications and services, to ensure that for each activity it is clear which Bot triggered an interface or web-service.

In case shared or system accounts are required, compensating controls are in place where appropriate..

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
12-Identity & access management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Unique accounts

Control topic

Access accountability for human accounts

AI Risk description

Lack of ownership and accountability for access to the AI solution - and/or for the Bots' access to connecting systems - increases the risk of inappropriate access, leading to operational, financial or reputational losses.

AI Control description

Wherever possible human accounts to access the AI environment are personal and unique, and the individuals have ultimate responsibility for these.

In case shared or system accounts are required, compensating controls are in place where appropriate.

Access to system logic and algorithms are appropriately restricted to authorised individuals.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

12-Identity & access management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk
Inappropriate access to the solution

Control topic
'Bot's access authorisation

AI Risk description
Access to, or through, the Bot and/or relevant systems and data is inappropriate and/or unauthorised, leading to operational, financial or reputational losses.

AI Control description
The Bot's access rights to relevant systems are set-up and assigned on a 'need to have' basis. Bot access is constrained to applications and data required for specific, intended transactions only.

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
12-Identity & access management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk
Inappropriate access to the solution

Control topic
User access authorisation

AI Risk description
Access to, or through, the Bot and/or relevant systems and data is inappropriate and/or unauthorised, leading to operational, financial or reputational losses.

AI Control description
User access to the Bot's IT environment (e.g. the AI solution itself, additional (permanent or temporary) data storage facilities, log files, and other relevant components) is set-up and assigned on a 'need to have' basis.

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
12-Identity & access management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

Unique accounts

Control topic

Account provisioning procedures (user and Bot)

AI Risk description

Access to, or through, the Bot and/or relevant systems and data is inappropriate and/or unauthorised, leading to operational, financial or reputational losses.

AI Control description

Access provisioning procedures are in place for the creation of (human) user and Bot accounts and assigning user privileges to new or existing accounts. Formal approval is required by appropriate business representatives for the establishment of users and granting of access rights, both the human and robotic accounts.

AI specificity

Low

COBIT process

APO01 Manage the IT Management Framework

Control subject

12-Identity & access management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk

Inappropriate access to the solution

Control topic

Access revocation procedures (user and Bot)

AI Risk description

Access to, or through, the Bot and/or relevant systems and data is inappropriate and/or unauthorised, leading to operational, financial or reputational losses.

AI Control description

User provisioning procedures are in place for the timely deletion or locking of user accounts and their privileges when an employee leaves or when the employee or the Bot no longer needs this access due to a change in role or decommissioning.

AI specificity

Low

COBIT process

APO01 Manage the IT Management Framework

Control subject

12-Identity & access management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Inappropriate access not detected

Control topic

'Bot's accounts and access rights reviews

AI Risk description

Weaknesses in access authorisations and/or revocations are not detected in time, leading to operational, financial or reputational losses.

AI Control description

The Bot's access accounts and their system privileges are reviewed periodically. The reviews are formalised and documented, including appropriate sign-off.

Any exceptions detected by the reviews are acted upon in a timely manner.

Exceptions are investigated to determine whether the account has been used inappropriately (e.g. used after the Bot's access was no longer required) and whether this access exposed any particular risk (e.g. if any significant access rights were used).

AI specificity

Low

COBIT process

MEA02 Monitor, Evaluate and Assess the System of Internal Control

Control subject

12-Identity & access management

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk

Inappropriate access not detected

Control topic

User accounts and access rights reviews

AI Risk description

Weaknesses in access authorisations and/or revocations are not detected in time, leading to operational, financial or reputational losses.

AI Control description

User accounts and system privileges that have access to the Bot's IT environment (e.g. the AI solution itself, additional (permanent or temporary) data storage facilities, log files, and other relevant components) are reviewed periodically. The reviews are formal and documented, including appropriate sign-off.

Any exceptions detected by the reviews are acted upon in a timely manner.

Exceptions are investigated to determine whether the account has been used inappropriately (e.g. used after the user's access was no longer required) and whether this access exposed any particular risk (e.g. if any significant access rights were used).

AI specificity

Low

COBIT process

MEA02 Monitor, Evaluate and Assess the System of Internal Control

Control subject

12-Identity & access management

COBIT area

Monitor, Evaluate and Assess

Please select a category for managing risks and controls for AI solutions.

09

Summarised risk

Inappropriate powerful access

Control topic

Privileged access (super user access)

AI Risk description

Privileged access rights are insufficiently protected to prevent unauthorised access to the system or its data, leading to operational, financial or reputational losses.

AI Control description

Access to powerful user accounts (such as those which can be used to perform user access administration, change system configuration or can directly access interfaces or data), are restricted to a defined set of system administration personnel for each of the IT components and across the IT stack (network, OS, database, application).

Access to these powerful accounts is subject to additional security, e.g. through a secure network, data encryption, stronger authentication controls such as 2-factor authentication or through additional means such as privileged access management tooling.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

12-Identity & access management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

Summarised risk

Segregation of duties conflicts

Control topic

IT Segregation of Duties

AI Risk description

Assigned access rights violate segregation of duty requirements, leading to operational, financial or reputational losses.

AI Control description

Access rights have been assigned to ensure compliance with the following SoD requirements:

* no single human can create user accounts and assign access privileges to these accounts without approval by another operator.

* no single human can make changes to the AI solution or its data directly in production, or make those change in a development environment which that operator would then be able to migrate to the production environment - without the approval by another operator.

* no single human can raise and approve the same change request.

AI specificity

Low

COBIT process

APO13 Manage Security

Control subject

12-Identity & access management

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

Summarised risk
Poor authentication

Control topic
Authentication, e.g. password controls

AI Risk description
Account authentication mechanisms are insufficient to prevent unauthorised access to systems or data, leading to operational, financial or reputational losses.

AI Control description
Effective authentication controls are in place, e.g. through the use of password controls or biometrics, in line with the IT security policy for systems in scope across the IT stack (network, OS, database, applications and utilities). These controls apply to all user accounts, including admin accounts and automation authentication, and cover elements such as (encrypted storage, and passwords are to be changed upon first usage, password length/ complexity and with a min and max lifetime).

In case certain accounts (e.g. system accounts or Bot accounts) do not have passwords controls in place, or are required to use hard coded passwords, compensating controls exist to mitigate the risk that unauthorised individuals can use the relating accounts to access to data or systems.

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
12-Identity & access management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

Summarised risk
Inappropriate access by 3rd parties

Control topic
3rd party access

AI Risk description
Inappropriate access by 3rd parties, leading to operational, financial or reputational losses.

AI Control description
Access by 3rd party users, and user access to 3rd party data or data processing facilities is subject to the same level of controls as 'regular' users, data, and data processing facilities.

See also C.05.

AI specificity
Low

COBIT process
APO13 Manage Security

Control subject
12-Identity & access management

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

Number of risks defined in the framework	4	Number of controls defined in the framework	5

01

Summarised risk

Inappropriate changes to the solution

AI Risk description

Changes to the AI environment or related systems and data are not controlled with consistent quality, increasing the risk of unauthorised changes and incidents, which in turn leads to loss of reliability/ quality of the solution, and to operational, financial or reputational losses.

AI specificity

Low

Control subject

13-IT change management

Control topic

IT Change Management

AI Control description

For as far as is feasible (i.e. acknowledging the limitations of change control in a self learning environment), the AI environment follows a consistent change management approach with clear procedures and work instructions around changes to IT infrastructure, AI models and algorithms, data, etc. This approach is integrated with the 'regular' change management approach to ensure a consistent approach across the AI and related environments. Change management is aligned to good practice standards (e.g. ITIL).

Versioning is in place for for business processes, code, Bot configuration, applications, data structures and data classification.

See also for:

- segregate environments: C.51
- recording changes/ take snapshots: C.56/ C.87
- risk of black box: R.40
- regular testing/ monitoring: C.19 and C.81
- quality control: C.36.

COBIT process

BAI06 Manage Changes

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Inappropriate changes to the solution

Control topic

IT Change Management

AI Risk description

Changes to the AI environment or related systems and data are not controlled with consistent quality, increasing the risk of unauthorised changes and incidents, which in turn leads to loss of reliability/ quality of the solution, and to operational, financial or reputational losses.

AI Control description

Data governance inventories, including data classification inventory, data asset flagging, and data flow maps, are maintained as part of the change management process.

AI specificity

Low

COBIT process

BAI02 Manage Requirements Definition

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Inappropriate changes to the solution

Control topic

IT Change Management

AI Risk description

Changes to the AI environment or related systems and data are not controlled with consistent quality, increasing the risk of unauthorised changes and incidents, which in turn leads to loss of reliability/ quality of the solution, and to operational, financial or reputational losses.

AI Control description

The organisation has an established procedure that limits production changes to appropriate change management personnel.

Production is locked for direct changes and should only be unlocked for a requested period of time. Direct changes require approval from appropriate personnel prior to unlocking of production. If direct changes cannot inherently be prevented, then direct changes to production should be monitored on an ongoing basis.

Changes caused by the dynamic nature of machine learning are covered by additonal measures, such as loggoing and review of any modifications and/or periodic comparison of the solutions at different time stamps to identify any changes made.

AI specificity

Low

COBIT process

BAI07 Manage Change Acceptance and Transitioning

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Changes made by the solution impact other IT services

Control topic

IT Change Management

AI Risk description

The AI solution makes decisions or amends how it operates which may impact other processes, systems or services impacting operational integrity of the solution and the organisation.

AI Control description

The impact of changes to AI processing and outputs on other IT services are assessed and monitored. Design standards are in place which include 'black-list' behaviours - those that may not be adjusted by AI, and human oversight exists in Operations. 'Staggered learning' is used to introduce a new/ changed model/ approach for a limited scope first, and when necessary, it is possible to set the AI solution to stop learning (temporarily).

AI specificity

High

COBIT process

BAI06 Manage Changes

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

Inappropriate changes to the automation solution do not get detected

Control topic

Testing

AI Risk description

Either through deliberate or eroneous changes, or changes made by the AI solution itself, the overall effectiveness of the solutions is compromised without it being detected by the business, leading to operational, financial or reputational losses.

AI Control description

Automated testing packs (test cases/ scripts + test data) are in place, e.g. for when major changes are introduced such as new data source to the AI solution or machine learning upgrade. Adequate, automated (wherever possible) testing of all new Bots and changes to Bots is in place, including testing of controls, using predefined test scripts, to help ensure that the AI solution remains valid. Design tests take place in parallel with changes and establish production readiness thresholds.

AI specificity

Medium

COBIT process

BAI07 Manage Change Acceptance and Transitioning

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk

Inappropriate changes to the automation solution do not get detected

Control topic

Ongoing testing

AI Risk description

Either through deliberate or eroneous changes, or changes made by the AI solution itself, the overall effectiveness of the solutions is compromised without it being detected by the business, leading to operational, financial or reputational losses.

AI Control description

Continual testing of the end-to-end AI solution is in place, by Business and IT, using a variety of dynamic and evolving testing methodologies to reflect the constant learning nature of AI based on business objectives and specific functional requirements.

AI specificity

High

COBIT process

BAI07 Manage Change Acceptance and Transitioning

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Insufficient testing of changes to the automation solution

Control topic

Test approvals

AI Risk description

Insufficient testing of the AI solution leads to non-detection of incidents or quality or integrity issues.

AI Control description

UAT for changes is performed with appropriate consideration of business input for design, execute and approve testing, and signed off prior to be accepted. Documentation of test cases and approvals for each AI solution (or component thereof) is retained. Where possible, automation is applied to help ensure an efficient and high quality UAT process.

AI specificity

Low

COBIT process

BAI07 Manage Change Acceptance and Transitioning

Control subject

13-IT change management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- **15 – IT operations**
- 16 – Business continuity
- 17 – Knowledge management

Number of risks defined in the framework	7

Number of controls defined in the framework	7

01

Summarised risk
Lacking inventory of all intelligent automation solutions

Control topic
Inventory of intelligent automation solutions

AI Risk description
Without a complete and detailed inventory of all AI or other similar solutions (e.g. RPA), including dependencies between solutions, an entity is not able to ensure AI is being applied in line with the strategy and its risk appetite.

AI Control description
An inventory of all AI platforms, solutions and use cases exists, is complete and kept up to date. The specific owner of each AI solution is captured in the inventory.

AI specificity
Low

COBIT process
APO05 Manage Portfolio

Control subject
14-IT operations

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Lacking control over the use of IT system resources

Control topic

Management of IT consumption

AI Risk description

The AI solution makes decisions about the system resources it requires, such as processing time, capacity, processes with other systems etc., that may impact the cost and efficacy of the overall system. E.g. the AI solution may require an increasing amount of a finite processing window that could crowd out other processes, or require a larger window to interface with another system that may impact on how the other system runs, or requires an additional service such as a new databases to be set up, which may not be licensed or efficient.

AI Control description

Controls are in place to monitor IT resource demands, more closely than other systems because AI systems might be more likely to be more unpredictable/ dynamic.

AI specificity

Medium

COBIT process

BAI04 Manage Availability and Capacity

Control subject

14-IT operations

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Errors in the solution's operation remain undetected

Control topic

Incident management

AI Risk description

Errors in the AI's operation remain undetected or are detected late, or are not acted upon appropriately, increasing the risk of unauthorised changes, system availability, data loss and other incidents.

Traditional incident detection systems may not be designed to identify AI-generated incidents such as misalignment with culture or minor errors in processing; and by extension problems may not be identified and managed because of a lack of identification or logging of incidents. This may result in outages or non-availability of systems or data, or information security breaches.

AI Control description

The AI environment follows a consistent incident management approach with clear procedures and work instructions that are to ensure timely resolution of incidents with appropriate escalation where required. This approach is integrated with the 'regular' incident management approach to ensure a consistent approach across the AI and related environments. Incident management is aligned to good practice standards (e.g. ITIL).

AI specificity

Medium

COBIT process

DSS02 Manage Service Requests and Incidents

Control subject

14-IT operations

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Errors in the solution's operation remain undetected

Control topic

Error resolution

AI Risk description

Errors in the AI's operation remain undetected or are detected late, or are not acted upon appropriately, increasing the risk of unauthorised changes, system availability, data loss and other incidents.

Traditional incident detection systems may not be designed to identify AI-generated incidents such as misalignment with culture or minor errors in processing; and by extension problems may not be identified and managed because of a lack of identification or logging of incidents. This may result in outages or non-availability of systems or data, or information security breaches

AI Control description

Processing exceptions, and error resolution (from operations or maintenance activities), is performed on a timely basis by appropriate personnel (exception management guidelines and approach). This includes issue and performance monitoring (application, system and network).

AI specificity

Medium

COBIT process

DSS01 Manage Operations

Control subject

14-IT operations

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

Errors in the solution's operation remain undetected

Control topic

Job monitoring

AI Risk description

Errors in the AI's operation remain undetected or are detected late, or are not acted upon appropriately, increasing the risk of unauthorised changes, system availability, data loss and other incidents.

Traditional incident detection systems may not be designed to identify AI-generated incidents such as misalignment with culture or minor errors in processing; and by extension problems may not be identified and managed because of a lack of identification or logging of incidents. This may result in outages or non-availability of systems or data, or information security breaches.

AI Control description

Appropriate job monitoring processes are followed to monitor system jobs and interfaces to ensure completeness and timeliness of system and data processing, and to identify any interruptions in a timely manner.

AI specificity

Medium

COBIT process

DSS01 Manage Operations

Control subject

14-IT operations

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk

IP not accessible or protected

Control topic

IP protection

AI Risk description

The AI solution's IP/ code is not accessible (e.g. held by a third party) or not adequately protected from IP loss/ theft, and impacts the ability to maintain effective automation solutions in an efficient manner, or otherwise impact the AI business case.

AI Control description

A repository of relevant IP (i.e. data, code, models and 'learning data') is set-up and accessible in-house, secured, and protected with regular back-ups using the son, father, grand-father principle.

See also C.49.

In interaction with parties outside the organisation, the risk of IP loss is considered and adequate mitigating measures are taken (e.g. use of encryption to prevent the code from being read.

AI specificity

Low

COBIT process

DSS01 Manage Operations

Control subject

14-IT operations

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Lack of knowledge of all related IT components

Control topic

Asset and Configuration management

AI Risk description

Lack of up to date understanding of the IT and data components of the overall AI environment and their relationships undermines the effectiveness of several other controls incl. security, software licences, IT operations and business continuity.

AI Control description

A configuration management database ('CMDB', i.e. a database with all the Configuration Items ('Cis')) is established and maintained to ensure a complete understanding of all the IT and data components and their relationships. This repository feeds in to other processes such as Risk and Security Management and IT Operations, and is updated as part of the Change management processes.

AI specificity

Low

COBIT process

BAI10 Manage Configuration

Control subject

14-IT operations

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk

Insufficient capacity or availability

Control topic

Availability and capacity management, and the scalability of the solution

AI Risk description

The AI solution is not able to meet the evolving demand, impacting the organisation's ability to maintain the solution sufficiently available and effective to adequately support relevant business processes.

AI Control description

For the IT infrastructure as well as the AI solution, adequate availability and capacity management processes are in place and scalability has been embedded in the design of the solution.

See also C.55.

AI specificity

Medium

COBIT process

BAI04 Manage Availability and Capacity

Control subject

14-IT operations

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

- 01 – Strategy
- 02 – Governance
- 03 – Human resource management
- 04 – Supplier management
- 05 – Risk management and compliance
- 06 – Enterprise architecture
- 07 – Data and model governance
- 08 – Programme governance and management
- 09 – Solution development
- 10 – Business process controls
- 11 – Logging and monitoring
- 12 – Security management
- 13 – Identity and access management
- 14 – IT change management
- 15 – IT operations
- **16 – Business continuity**
- 17 – Knowledge management

Number of risks defined in the framework	6

Number of controls defined in the framework	8

01

Summarised risk

Insufficient fall back facilities

AI Risk description

No fall back or alternative processing facility is available for a fully functioning AI solution (consisting of hardware, software, process data and learning data and encompassing solutions required for the effective functioning of the solution). This includes:

* an IT infrastructure risk (i.e. not having core processing facilities available in time, including all the required interfaces, access to data etc.),

* a solution/ functional risk (i.e. not having an alternative AI solution in place in time that provides the same functionality, learnings, access to same data, etc.)

* a business/ operational risk (i.e. not being able to manually - or otherwise - operate relevant business processes without an effective AI solution in place).

Control topic

BCP fall-back environment

AI Control description

Fall back/ alternative processing possibilities have been explored, risk and impact assessment have been made, and where feasible such alternative processing opportunities have been put in place to cover one or more of the three risks listed (i.e. AI has a dynamic element that will make this only partially effective).

AI specificity

Medium

COBIT process

DSS04 Manage Continuity

Control subject

15-Business continuity

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Lack of Business continuity arrangements, and testing thereof

Control topic

BCP

AI Risk description

Business continuity plans are not in place to provide the required structure to limit the impact of a major incident, and/or such plans/ facilities are not operating as required at the time these are needed

AI Control description

The AI environment follows a consistent business continuity management approach with clear procedures and work instructions. This approach is integrated with the 'regular' business continuity management approach to ensure a consistent approach across AI and related environments. Business continuity management is aligned to good practice standards (e.g. ISO 22301).

Effective Business continuity plans have been developed, approved and are being maintained adequately.

AI specificity

Low

COBIT process

DSS04 Manage Continuity

Control subject

15-Business continuity

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Lack of Business continuity arrangements, and testing thereof

Control topic

BCP testing

AI Risk description

Business continuity plans are not in place to provide the required structure to limit the impact of a major incident, and/or such plans/ facilities are not operating as required at the time these are needed.

AI Control description

Regular BCP simulations, incl. testing of alternative facilities, are performed to ensure plans and facilities are effective, and that staff are well trained to operate under such conditions (i.e. to ensure people, process and technology are ready when needed).

AI specificity

Low

COBIT process

DSS04 Manage Continuity

Control subject

15-Business continuity

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk
Black box solution risks

Control topic
Warranty

AI Risk description
The logic within the AI solution is not fully understood - or is not accessible to the organisation - impacting the ability to recover services when issues occur, impacting business operations and resulting in financial loss (i.e. the risks around 'a black box solution') or reputational damage.

AI Control description
Formal advanced support and 'warranty' arrangements have been made with the AI vendor, also during the post go-live/ stabilisation phase, to maintain a sufficiently available and effective solution to adequately support relevant business processes. Clear and tangible service levels and monitoring thereof is in place.

AI specificity
Medium

COBIT process
APO09 Manage Service Agreements

Control subject
15-Business continuity

COBIT area
Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

05

Summarised risk

Insufficient capabilities, incl. human capacity

Control topic

Human resource requirements

AI Risk description

Insufficient capabilities, incl. human capacity. to overcome a major incident, impacting business operations and resulting in financial loss or reputational damage.

AI Control description

Roles and responsibilities related to operating the AI solution, as well as capacity and skills (see C.40 and C.42) take business continuity requirements in to consideration (i.e. capacity and capabilities are appropriate to overcome major incidents).

AI specificity

Medium

COBIT process

APO07 Manage Human Resources

Control subject

15-Business continuity

COBIT area

Align, Plan and Organise

Please select a category for managing risks and controls for AI solutions.

06

Summarised risk
Unclear BCP roles and responsibilities

Control topic
BCP roles and responsibilities

AI Risk description
Unclear roles and responsibility within the BCP process limit the organisation's ability to overcome a major incident, impacting business operations and resulting in regulatory, financial, resilience and reputational impact.

AI Control description
Roles and responsibilities within the end to end BCP process - including 3rd party suppliers - are clearly defined and relevant staff are well trained in these.

See also C.42.

AI specificity
Low

COBIT process
Deliver, Service and Support

Control subject
15-Business continuity

COBIT area
Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

07

Summarised risk

Inability to recover after an incident

Control topic

Roll-back and adapt

AI Risk description

Inability to accurately identify and recover from the last known good AI and machine learning state, e.g. due to inherent black box nature, to help overcome an incident at time of crisis.

AI Control description

In case the AI solution becomes ineffective (i.e. a major incident occurs or the solution has inappropriately evolved/ learned), a roll-back mechanism is in place (see C.56) and/or processes, algorithms and cleansed data are available to get the solution to be implemented and (re)trained quickly to reflect new/ changed requirements

AI specificity

High

COBIT process

BAI02 Manage Requirements Definition

Control subject

15-Business continuity

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

08

Summarised risk

Automation services cannot be restored completely and accurately

Control topic

Backups

AI Risk description

AI services cannot be restored completely and accurately, impacting business operations and resulting in financial loss.

AI Control description

Appropriate backup of the AI solution - including frequent snapshots of relevant parts (incl. learning) - for grandfather/father/son recording is in place, including the ability to roll back (see also C.54). Fail-safe appetite needs to be considered to prevent and detect unexpected failure ('black-swan effect'), potentially within the machine learning capability.

If needed, the 'vault principle' should be applied, i.e. an automated solution that securely stores any decision made by the solution, as well as the data the decision was based on, and the latest version of the algorithm(s) and code.

AI specificity

High

COBIT process

DSS04 Manage Continuity

Control subject

15-Business continuity

COBIT area

Deliver, Service and Support

Please select a category for managing risks and controls for AI solutions.

Number of risks defined in the framework	3

Number of controls defined in the framework	3

01

Summarised risk

Wrong decisions are made unknowingly

Control topic

Knowledge retention

AI Risk description

Without a strategy for managing knowledge related to decisions to be made - or supported - by the AI solution (business knowledge / AI solution knowledge – data / technology / algorithm etc.) there is a risk that the entity (unknowingly) may make the 'wrong' decisions.

AI Control description

Throughout solution design and development, sufficient documentation and MI structures (e.g. decision making intelligence) is built in to enable the required knowledge to be retained and maintained that supports decision making.

AI specificity

High

COBIT process

BAI08 Manage Knowledge

Control subject

16-Knowledge management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

02

Summarised risk

Insufficient IT knowledge retained/ developed to run and maintain effective automation solutions, and to overcome major incidents

Control topic

IT knowledge management and documentation

AI Risk description

Insufficient IT knowledge (staff and/ or skills) retained/ developed to effectively run and maintain the solution once handed over to the standing organisation (i.e. once the solution moves to sustain), leading to an ineffective AI solution, or to AI solutions becoming ineffective over time, and/ or poor decision making during major incidents.

AI Control description

Solution and IT management processes, incl. process, technology and data requirements, are well documented and maintained for the end to end process for each AI solution. Documentation is kept up to date through automated logging and reporting of changes (e.g. through an audit trail of changes to decision logic).

AI specificity

High

COBIT process

BAI08 Manage Knowledge

Control subject

16-Knowledge management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

03

Summarised risk

Insufficient IT knowledge retained/ developed to develop/ train new effective automation solutions

Control topic

IT knowledge management and documentation

AI Risk description

Insufficient IT knowledge (staff and/ or skills) retained/ developed to effectively design and build effective AI solution(s).

AI Control description

Development methodology, architectural standards and other technical and data related documentation is available to sufficiently skilled resources to support the development of new solutions, or new parts of existing solutions. In case external vendors are/ were used to develop solutions, adequate knowledge transfer has been designed and executed to retain relevant knowledge within the organisation.

AI specificity

High

COBIT process

BAI08 Manage Knowledge

Control subject

16-Knowledge management

COBIT area

Build, Acquire and Implement

Please select a category for managing risks and controls for AI solutions.

04

Summarised risk

Insufficient business knowledge retained/ developed to develop/ train new effective automation solutions

Control topic

Business knowledge management and Documentation

AI Risk description

Insufficient business knowledge retained/ developed to develop/ train new effective AI solutions. Subject matter expertise, thought leadership and traditional business knowledge if not retained may prevent the organisation from developing new AI capabilities effectively.

AI Control description

Functional and business processes are well documented and maintained for the end to end process for each AI solution.

Detailed process narratives and/or flowcharts (incl. data flows) are available, incorporating all use cases and process variations, as well possible exceptions. Current internal controls have been documented as an integrated part of the overall process documentation.

AI specificity

High

COBIT process

BAI08 Manage Knowledge

Control subject

16-Knowledge management

COBIT area

Build, Acquire and Implement

www.kpmg.com/uk

Create Graphics I CRT102763 I September 2018