External Regime	Citation Type	Citation ID	Requirement Summary	Requirement Type	DAGS Domain	DAGS Control ID	DAGS Control Name	Coverage Status	Evidence Artifact(s)	Residual Obligation	Assessor Notes
ISO/IEC 42001	Clause	4.1–4.4	Define organizational context and AIMS scope	Governance				Not Covered	—	Enterprise context/scope definition (outside DAGS).	DAGS is deployment-layer; assumes AIMS scope is pre-defined.
ISO/IEC 42001	Clause	5.1–5.3	Assign AI roles, responsibilities, and accountability	Oversight	D1	D1.1	System Ownership	Partial	System ownership registry; governance RACI; named system owner	Enterprise governance charter and top-management accountability remain required.	Deployment-level role assignment and ownership evidence.
ISO/IEC 42001	Clause	5.1–5.3	Establish escalation and oversight mechanisms	Oversight	D1	D1.8	Escalation Path	Partial	Escalation path; escalation SLA; decision log	Management review and board oversight remain outside DAGS.	DAGS provides inspectable escalation mechanics, not executive oversight.
ISO/IEC 42001	Clause	6.1	Identify AI risks and opportunities	Risk Identification	D4	D4.1	Defined Use Constraints	Partial	Defined use constraints; risk/constraint register; exception approvals	Risk appetite and acceptance authority remain enterprise-owned.	DAGS identifies deployment risks via enforceable constraints; does not accept risk.
ISO/IEC 42001	Clause	7.5	Control documented information	Documentation	D2	D2.9	Visibility Documentation Maintenance	Partial	Versioned visibility documentation; inventory snapshots; retention logs	Enterprise document control policy remains required.	DAGS requires maintained, traceable visibility documentation.
ISO/IEC 42001	Clause	8.1	Operational planning and control	Control Implementation	D5	D5.5	Operational Change Management	Partial	Operational change records; approvals; deployment change log	Org-wide operational planning and resource controls remain required.	DAGS enforces change management at the deployed system boundary.
ISO/IEC 42001	Clause	8.3	Supply chain and externally provided processes/products/services	Vendor/Supply Chain	D2	D2.3	Vendor Disclosure	Partial	Vendor disclosure record; vendor role documentation; vendor change notices	Supplier evaluation criteria, contracts, and procurement governance remain required.	DAGS captures vendor identity/role and change influence evidence; not
ISO/IEC 42001	Clause	9.2–9.3	Internal audit and management review	Governance				Not Covered	—	Internal audit program and management review execution (outside DAGS).	DAGS outputs are audit inputs; DAGS does not perform management review.
ISO/IEC 42001	Clause	10.1–10.2	Nonconformity, corrective action, and continual improvement	Remediation	D5	D5.3	Incident Integration	Partial	Incident integration records; corrective-action log; post-incident review	Continual improvement program and organizational learning remain required.	DAGS supports system-level nonconformity handling evidence.
NIST AI RMF	Function	GOVERN	Establish AI governance and accountability	Governance	D1	D1.5	Documented Governance Structure	Partial	Documented governance structure; RACI; oversight mechanism	Enterprise policy, risk appetite, and governance bodies remain required.	Not a governance substitute; deployment-level governance artifacts only.
NIST AI RMF	Function	MAP	Contextualize AI system purpose, dependencies, and risks	Risk Identification	D2	D2.1	Model Inventory	Partial	Model inventory; dependency list; vendor disclosure	Impact assessment and broader organizational context remain required.	DAGS focuses on actual deployed system composition.
NIST AI RMF	Function	MAP	Define intended use constraints and misuse boundaries	Risk Identification	D4	D4.1	Defined Use Constraints	Partial	Defined use constraints; misuse scenarios; exception register	Higher-level societal impact analysis remains required.	Deployment reality focus; enforceable constraints.
NIST AI RMF	Function	MEASURE	Measure and monitor risk, performance, and anomalies	Monitoring	D5	D5.7	Ongoing Operational Oversight	Partial	Ongoing operational oversight logs; monitoring cadence record; operational reviews	Measurement methodology and benchmarks remain required.	DAGS provides evidence that monitoring occurs; does not define metrics.
NIST AI RMF	Subcategory	MEASURE 2.3	Testing and validation of AI system performance and risks	Testing/Validation	D3	D3.5	Integrity Safeguards	Partial	Integrity safeguard evidence; controlled modification logs; test evidence references (where	Formal validation plans, test design, and acceptance criteria remain required.	DAGS supports controlled change and integrity evidence; does not prescribe validation
NIST AI RMF	Function	MANAGE	Risk response, incident handling, and lifecycle management	Risk Response	D5	D5.3	Incident Integration	Partial	Incident integration; escalation records; corrective actions	Risk acceptance authority and enterprise response governance remain required.	Enables response; does not substitute enterprise risk decisions.
EU AI Act	Article	2–3	Applicability and role determination (provider/deployer/etc.)	Governance				Not Covered	—	Legal applicability and role determination (outside DAGS).	Requires legal determination; DAGS may supply deployment facts only.
EU AI Act	Article	5	Prohibited AI practices determination	Governance				Not Covered	—	Legal prohibition assessment (outside DAGS).	DAGS can support evidence once prohibition is determined; does not classify legality.
EU AI Act	Article	6; Annex III	High-risk classification determination	Risk Classification				Not Covered	—	Legal classification (outside DAGS).	DAGS supplies deployment facts; does not determine Annex III status.
EU AI Act	Article	9	Risk management system for high-risk AI	Risk Management	D4	D4.8	Review and Update of Constraints	Partial	Constraint review/update records; risk/constraint register; exception approvals	Full risk management system governance remains required.	Technical/operational evidence only; supports risk management, does not constitute it.
EU AI Act	Article	11–12	Technical documentation and record-keeping	Documentation	D2	D2.10	Traceability of Visibility Information	Partial	Traceability of visibility information; version history; retention logs	Legal sufficiency of documentation remains required.	Inspectable documentation lineage; evidence-first posture.
EU AI Act	Article	13	Transparency and information to users (high-risk obligations)	Transparency	D4	D4.9	Constraint Transparency	Partial	Constraint transparency disclosure; user-facing constraint statements; change-notice	Full legal transparency content, format, and delivery obligations remain required.	DAGS supports constraint transparency; does not author required legal disclosures.
EU AI Act	Article	14	Human oversight	Oversight	D5	D5.2	Defined Operational Roles	Partial	Defined operational roles; oversight workflow records; escalation path	Oversight design and adequacy determination remain required.	Deployment integration evidence; supports oversight implementation.
EU AI Act	Article	15	Accuracy, robustness, and cybersecurity	Security/Robustness	D3	D3.7	Security-Relevant Event Detection	Partial	Security-relevant event detection; security event logs; access control evidence	Performance thresholds and robustness testing remain required.	Evidence of control operation; not performance certification.
EU AI Act	Article	61–62	Post-market monitoring and serious incident reporting readiness	Post-Market Monitoring	D5	D5.8	Operational Reporting Paths	Partial	Operational reporting paths; incident reporting records; escalation path	Regulatory reporting obligations and timelines remain required.	Supports readiness and traceability for reporting pathways.
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.2	Authority to Govern	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.3	Accountability for Outcomes	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.4	Persistence of Accountability	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.6	Separation of Duties	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.7	Oversight Mechanism	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.9	Retained Accountability	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external

External Regime	Citation Type	Citation ID	Requirement Summary	Requirement Type	DAGS Domain	DAGS Control ID	DAGS Control Name	Coverage Status	Evidence Artifact(s)	Residual Obligation	Assessor Notes
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.10	Contractual Alignment	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.11	Unowned Systems Prohibited	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D1	D1.12	Implicit Governance Prohibited	Not Applicable	Ownership/RACI records; decision logs; oversight and escalation records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.2	Model Role Clarity	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.4	Vendor Role Documentation	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.5	Behavioral Dependencies	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.6	Opaque Dependency Prohibition	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.7	Vendor Change Influence	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.8	Retained Authority Over Change	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.11	Unknown Behavioral Sources Prohibited	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D2	D2.12	Assumed Visibility Prohibited	Not Applicable	Model/vendor inventory; dependency records; vendor disclosures; change notices	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.1	Restricted Access	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.2	Role-Based Control	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.3	Controlled Modification	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.4	Change Authorization	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.6	Tamper Resistance	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.8	Traceability of Security Events	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.9	Protection of Credentials	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.10	Credential Lifecycle Governance	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.11	Environment Segregation	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.12	Isolation of Control Interfaces	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.13	Uncontrolled Access Prohibited	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D3	D3.14	Implicit Security Prohibited	Not Applicable	Access control matrices; configuration baselines; security logs; credential lifecycle records	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.2	Documented Ethical Boundaries	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.3	Assigned Ethical Accountability	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.4	Persistence of Ethical Accountability	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.5	Operational Enforcement Mechanisms	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.6	Misuse Detection and Response	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.7	Oversight of Ethical Compliance	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.10	Unconstrained Deployment Prohibited	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external

External Regime	Citation Type	Citation ID	Requirement Summary	Requirement Type	DAGS Domain	DAGS Control ID	DAGS Control Name	Coverage Status	Evidence Artifact(s)	Residual Obligation	Assessor Notes
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D4	D4.11	Aspirational Ethics Prohibited	Not Applicable	Constraint register; enforcement/guardrail logs; misuse detection records; review	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.1	Operational Embedding	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.4	Accountability in Response	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.6	Lifecycle Continuity	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.9	Operational Readiness Requirement	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.10	Isolated Operation Prohibited	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external
—	—	—	No direct external regulatory analogue; internally normative DAGS control.	Internal Control	D5	D5.11	Governance by Exception Prohibited	Not Applicable	Operational runbooks; incident records; change tickets; monitoring and reporting	—	Included for complete enumeration of normative DAGS controls; absence of external

Artifact	DAGS-STD-040 Regulatory Crosswalk
Version	v1.0
Date	2025-12-28
Authority	This spreadsheet is the authoritative, normative crosswalk for DAGS v0.1.
Completeness	All normative DAGS controls listed in DAGS_Control_Index are enumerated in STD-040_Master. Controls with no external regulatory analogue are explicitly classified as Not Applicable.
Coverage Philosophy	Coverage Status indicates whether a specific external requirement is supported by DAGS evidence-producing controls (Partial) or is outside DAGS scope (Not Covered).
Use	Use filters on External Regime and Coverage Status for regulator/insurer views. The master sheet remains the single source of truth.

DAGS Domain	DAGS Domain Name	DAGS Control ID	DAGS Control Name	Normative
D1	Governance and Accountability	D1.1	System Ownership	Yes
D1	Governance and Accountability	D1.2	Authority to Govern	Yes
D1	Governance and Accountability	D1.3	Accountability for Outcomes	Yes
D1	Governance and Accountability	D1.4	Persistence of Accountability	Yes
D1	Governance and Accountability	D1.5	Documented Governance Structure	Yes
D1	Governance and Accountability	D1.6	Separation of Duties	Yes
D1	Governance and Accountability	D1.7	Oversight Mechanism	Yes
D1	Governance and Accountability	D1.8	Escalation Path	Yes
D1	Governance and Accountability	D1.9	Retained Accountability	Yes
D1	Governance and Accountability	D1.10	Contractual Alignment	Yes
D1	Governance and Accountability	D1.11	Unowned Systems Prohibited	Yes
D1	Governance and Accountability	D1.12	Implicit Governance Prohibited	Yes
D2	Model and Vendor Visibility	D2.1	Model Inventory	Yes
D2	Model and Vendor Visibility	D2.2	Model Role Clarity	Yes
D2	Model and Vendor Visibility	D2.3	Vendor Disclosure	Yes
D2	Model and Vendor Visibility	D2.4	Vendor Role Documentation	Yes
D2	Model and Vendor Visibility	D2.5	Behavioral Dependencies	Yes
D2	Model and Vendor Visibility	D2.6	Opaque Dependency Prohibition	Yes
D2	Model and Vendor Visibility	D2.7	Vendor Change Influence	Yes
D2	Model and Vendor Visibility	D2.8	Retained Authority Over Change	Yes
D2	Model and Vendor Visibility	D2.9	Visibility Documentation Maintenance	Yes
D2	Model and Vendor Visibility	D2.10	Traceability of Visibility Information	Yes
D2	Model and Vendor Visibility	D2.11	Unknown Behavioral Sources Prohibited	Yes
D2	Model and Vendor Visibility	D2.12	Assumed Visibility Prohibited	Yes
D3	Security and Controls	D3.1	Restricted Access	Yes
D3	Security and Controls	D3.2	Role-Based Control	Yes
D3	Security and Controls	D3.3	Controlled Modification	Yes
D3	Security and Controls	D3.4	Change Authorization	Yes
D3	Security and Controls	D3.5	Integrity Safeguards	Yes

DAGS Domain	DAGS Domain Name	DAGS Control ID	DAGS Control Name	Normative
D3	Security and Controls	D3.6	Tamper Resistance	Yes
D3	Security and Controls	D3.7	Security-Relevant Event Detection	Yes
D3	Security and Controls	D3.8	Traceability of Security Events	Yes
D3	Security and Controls	D3.9	Protection of Credentials	Yes
D3	Security and Controls	D3.10	Credential Lifecycle Governance	Yes
D3	Security and Controls	D3.11	Environment Segregation	Yes
D3	Security and Controls	D3.12	Isolation of Control Interfaces	Yes
D3	Security and Controls	D3.13	Uncontrolled Access Prohibited	Yes
D3	Security and Controls	D3.14	Implicit Security Prohibited	Yes
D4	Ethics and Responsible Use	D4.1	Defined Use Constraints	Yes
D4	Ethics and Responsible Use	D4.2	Documented Ethical Boundaries	Yes
D4	Ethics and Responsible Use	D4.3	Assigned Ethical Accountability	Yes
D4	Ethics and Responsible Use	D4.4	Persistence of Ethical Accountability	Yes
D4	Ethics and Responsible Use	D4.5	Operational Enforcement Mechanisms	Yes
D4	Ethics and Responsible Use	D4.6	Misuse Detection and Response	Yes
D4	Ethics and Responsible Use	D4.7	Oversight of Ethical Compliance	Yes
D4	Ethics and Responsible Use	D4.8	Review and Update of Constraints	Yes
D4	Ethics and Responsible Use	D4.9	Constraint Transparency	Yes
D4	Ethics and Responsible Use	D4.10	Unconstrained Deployment Prohibited	Yes
D4	Ethics and Responsible Use	D4.11	Aspirational Ethics Prohibited	Yes
D5	Operational Integration	D5.1	Operational Embedding	Yes
D5	Operational Integration	D5.2	Defined Operational Roles	Yes
D5	Operational Integration	D5.3	Incident Integration	Yes
D5	Operational Integration	D5.4	Accountability in Response	Yes
D5	Operational Integration	D5.5	Operational Change Management	Yes
D5	Operational Integration	D5.6	Lifecycle Continuity	Yes
D5	Operational Integration	D5.7	Ongoing Operational Oversight	Yes
D5	Operational Integration	D5.8	Operational Reporting Paths	Yes

DAGS Domain	DAGS Domain Name	DAGS Control ID	DAGS Control Name	Normative
D5	Operational Integration	D5.9	Operational Readiness Requirement	Yes
D5	Operational Integration	D5.10	Isolated Operation Prohibited	Yes
D5	Operational Integration	D5.11	Governance by Exception Prohibited	Yes