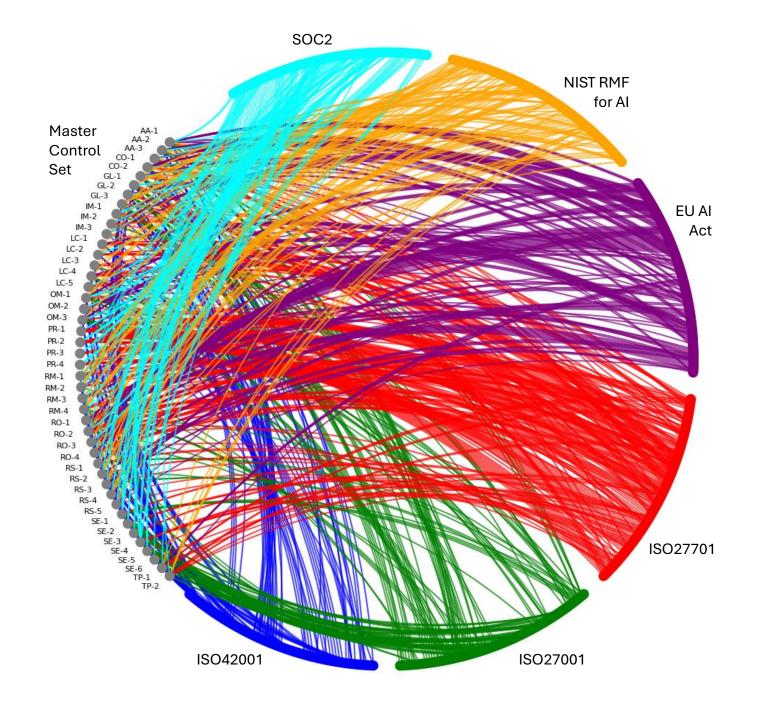
# Al Governance Master Controls

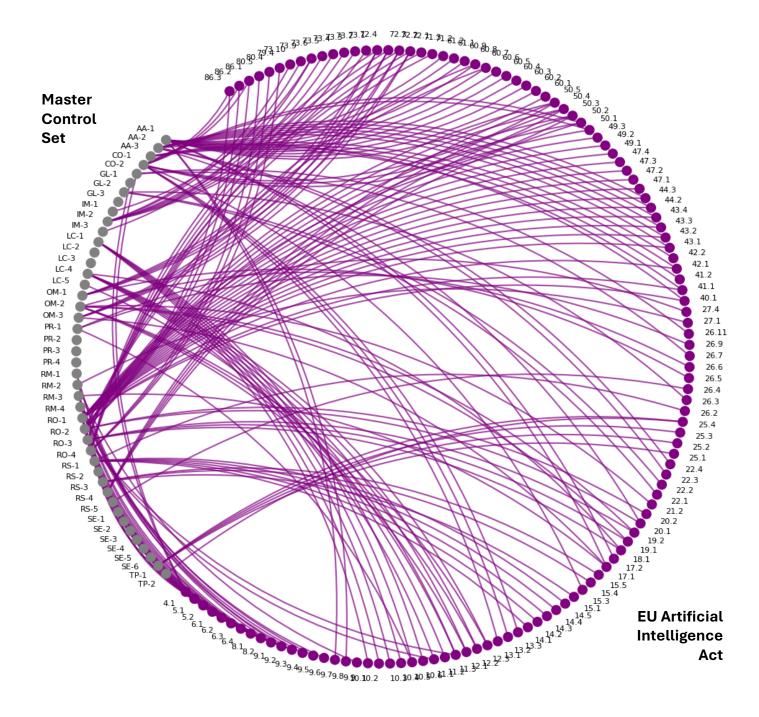
Mapping the 6 most important AI control sources into one real-world, practical framework.



Subscribe free: ethos-ai.org

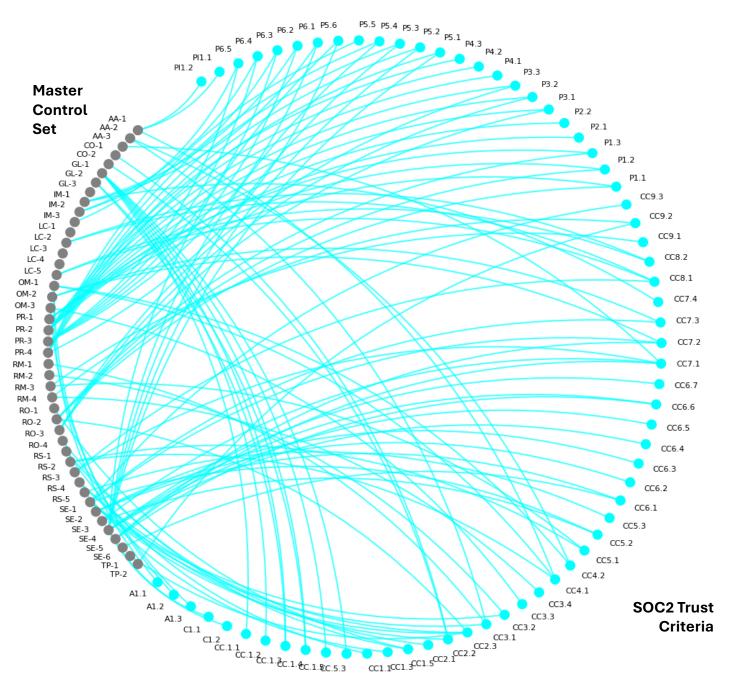


L-1	Executive Commitment and Accountability
L-2	Roles, Responsibilities & Resources
L-3	Strategic Alignment & Objectives
<b>1</b> -1	Risk Management Framework and Governance
<b>1-2</b>	Risk Identification and Impact Assessment
<b>1</b> -3	Risk Treatment and Control Implementation
<b>1</b> -4	Risk Monitoring and Response
D-1	Regulatory Compliance Framework
D-2	Transparency, Disclosure and Reporting
D-3	Record-Keeping
0-4	Post-Market Monitoring
C-1	Data Quality and Governance
C-2	System Development and Lifecycle Management
C-3	Resource Management and Infrastructure
C-4	Technical Documentation
C-5	Change Management & Version Control
-1	Security Governance, Architecture and Engineering
-2	Identity & Access Management
-3	Software Security
E-4	Data Security
E-5	Network Security
E-6	Physical Security
S-1	Human Oversight and Intervention
S-2	Safety
S-3	Robustness
6-4	Explainability and Interpretability
S-5	Fairness and Bias Management
R-1	Privacy by Design and Governance
R-2	Personal Data Management
R-3	Privacy Compliance and Monitoring
R-4	Privacy-Enhancing Technologies and Mechanisms
\-1	Internal Assessment & Audit
\-2	Independent Assessment and Certification
<b>4-3</b>	Safety and Security Validation
M-1	System Performance Monitoring
M-2	Event Logging
M-3	Continuous Improvement
P-1	Third-Party Provider Responsibilities
P-2	Supplier Risk Management
<b>D-1</b>	Al System Transparency
<b>D-2</b>	Stakeholder Engagement and Feedback
I-1	Incident Detection and Response
I-2	Incident Reporting and Notification
I-3	Incident Analysis and Improvement



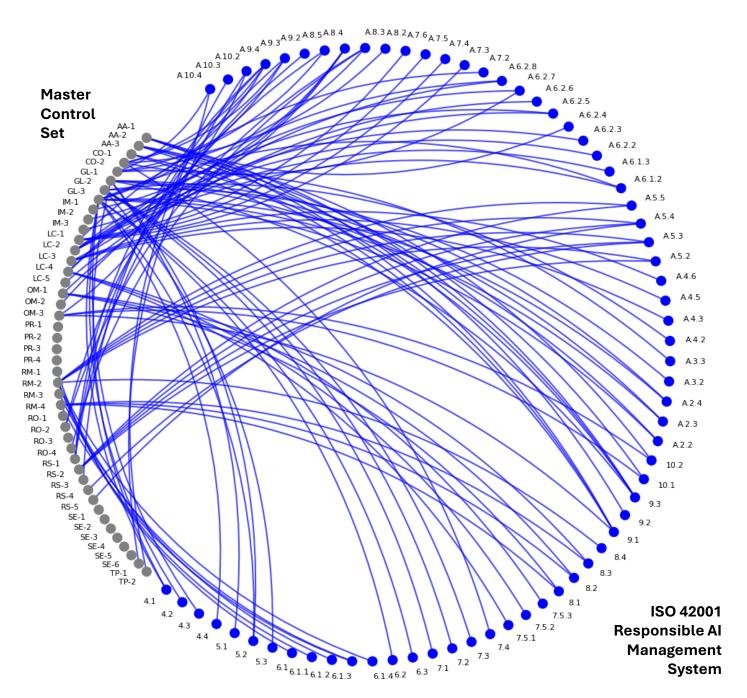


L-1	Executive Commitment and Accountability
L-2	Roles, Responsibilities & Resources
L-3	Strategic Alignment & Objectives
M-1	Risk Management Framework and Governance
M-2	Risk Identification and Impact Assessment
M-3	Risk Treatment and Control Implementation
M-4	Risk Monitoring and Response
O-1	Regulatory Compliance Framework
0-2	Transparency, Disclosure and Reporting
O-3	Record-Keeping
0-4	Post-Market Monitoring
C-1	Data Quality and Governance
C-2	System Development and Lifecycle Management
C-3	Resource Management and Infrastructure
C-4	Technical Documentation
C-5	Change Management & Version Control
E-1	Security Governance, Architecture and Engineering
E-2	Identity & Access Management
E-3	Software Security
E-4	Data Security
E-5	Network Security
E-6	Physical Security
S-1	Human Oversight and Intervention
S-2	Safety
S-3	Robustness
S-4	Explainability and Interpretability
S-5	Fairness and Bias Management
R-1	Privacy by Design and Governance
R-2	Personal Data Management
R-3	Privacy Compliance and Monitoring
R-4	Privacy-Enhancing Technologies and Mechanisms
A-1	Internal Assessment & Audit
A-2	Independent Assessment and Certification
A-3	Safety and Security Validation
M-1	System Performance Monitoring
M-2	Event Logging
M-3	Continuous Improvement
P-1	Third-Party Provider Responsibilities
P-2	Supplier Risk Management
0-1	Al System Transparency
0-2	Stakeholder Engagement and Feedback
1-1	Incident Detection and Response
1-2	Incident Reporting and Notification
1-3	Incident Analysis and Improvement



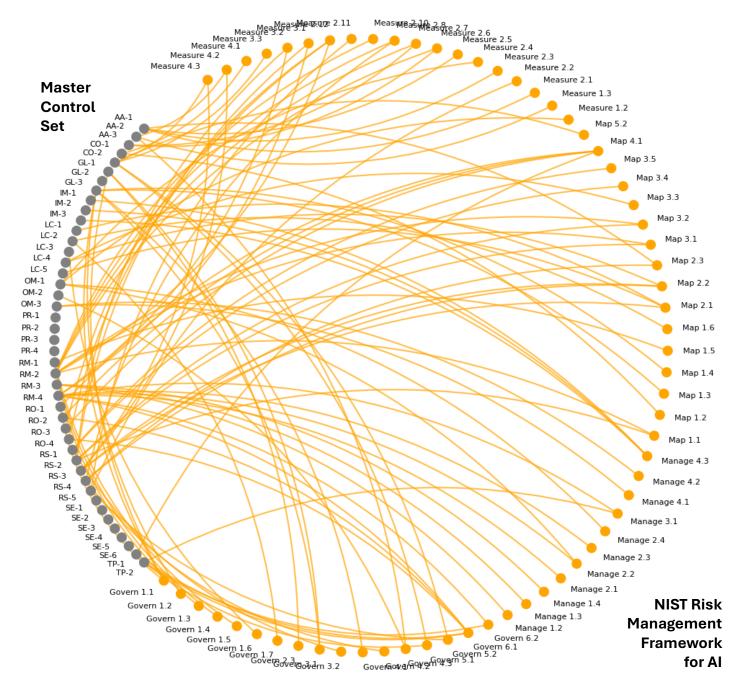


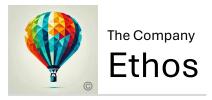
GL-1	Executive Commitment and Accountability
GL-2	Roles, Responsibilities & Resources
GL-3	Strategic Alignment & Objectives
RM-1	Risk Management Framework and Governance
RM-2	Risk Identification and Impact Assessment
RM-3	Risk Treatment and Control Implementation
RM-4	Risk Monitoring and Response
RO-1	Regulatory Compliance Framework
RO-2	Transparency, Disclosure and Reporting
RO-3	Record-Keeping
RO-4	Post-Market Monitoring
LC-1	Data Quality and Governance
LC-2	System Development and Lifecycle Management
LC-3	Resource Management and Infrastructure
LC-4	Technical Documentation
LC-5	Change Management & Version Control
SE-1	Security Governance, Architecture and Engineering
SE-2	Identity & Access Management
SE-3	Software Security
SE-4	Data Security
SE-5	Network Security
SE-6	Physical Security
RS-1	Human Oversight and Intervention
RS-2	Safety
RS-3	Robustness
RS-4	Explainability and Interpretability
RS-5	Fairness and Bias Management
PR-1	Privacy by Design and Governance
PR-2	Personal Data Management
PR-3	Privacy Compliance and Monitoring
PR-4	Privacy-Enhancing Technologies and Mechanisms
AA-1	Internal Assessment & Audit
AA-2	Independent Assessment and Certification
AA-3	Safety and Security Validation
OM-1	System Performance Monitoring
OM-2	Event Logging
OM-3	Continuous Improvement
TP-1	Third-Party Provider Responsibilities
TP-2	Supplier Risk Management
CO-1	Al System Transparency
CO-2	Stakeholder Engagement and Feedback
IM-1	Incident Detection and Response
IM-2	Incident Reporting and Notification
IM-3	Incident Analysis and Improvement



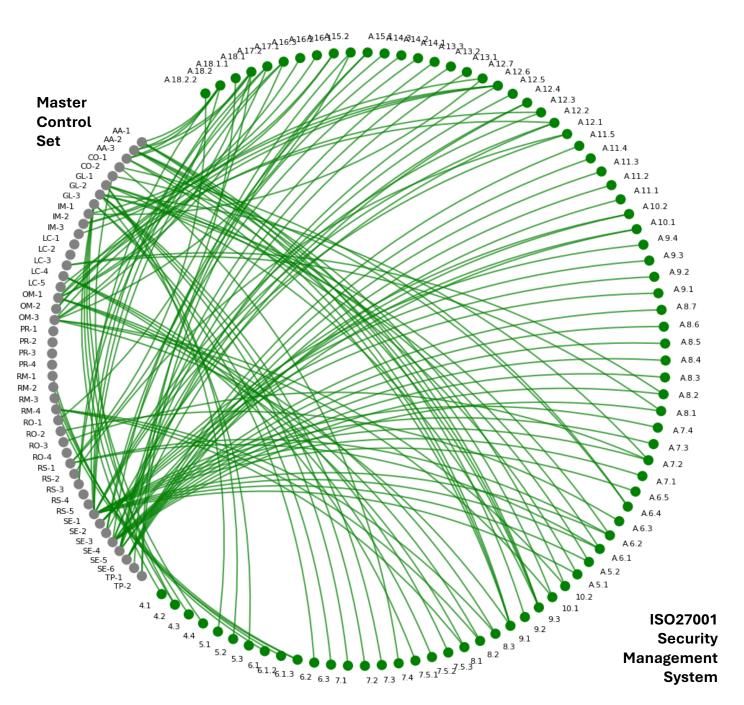


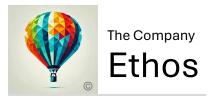
GL-1	Executive Commitment and Accountability
GL-2	Roles, Responsibilities & Resources
GL-3	Strategic Alignment & Objectives
RM-1	Risk Management Framework and Governance
RM-2	Risk Identification and Impact Assessment
RM-3	Risk Treatment and Control Implementation
RM-4	Risk Monitoring and Response
RO-1	Regulatory Compliance Framework
RO-2	Transparency, Disclosure and Reporting
RO-3	Record-Keeping
RO-4	Post-Market Monitoring
LC-1	Data Quality and Governance
LC-2	System Development and Lifecycle Management
LC-3	Resource Management and Infrastructure
LC-4	Technical Documentation
LC-5	Change Management & Version Control
SE-1	Security Governance, Architecture and Engineering
SE-2	Identity & Access Management
SE-3	Software Security
SE-4	Data Security
SE-5	Network Security
SE-6	Physical Security
RS-1	Human Oversight and Intervention
RS-2	Safety
RS-3	Robustness
RS-4	Explainability and Interpretability
RS-5	Fairness and Bias Management
PR-1	Privacy by Design and Governance
PR-2	Personal Data Management
PR-3	Privacy Compliance and Monitoring
PR-4	Privacy-Enhancing Technologies and Mechanisms
AA-1	Internal Assessment & Audit
AA-2	Independent Assessment and Certification
AA-3	Safety and Security Validation
OM-1	System Performance Monitoring
OM-2	Event Logging
OM-3	Continuous Improvement
TP-1	Third-Party Provider Responsibilities
TP-2	Supplier Risk Management
CO-1	Al System Transparency
CO-2	Stakeholder Engagement and Feedback
IM-1	Incident Detection and Response
IM-2	Incident Reporting and Notification
IM-3	Incident Analysis and Improvement



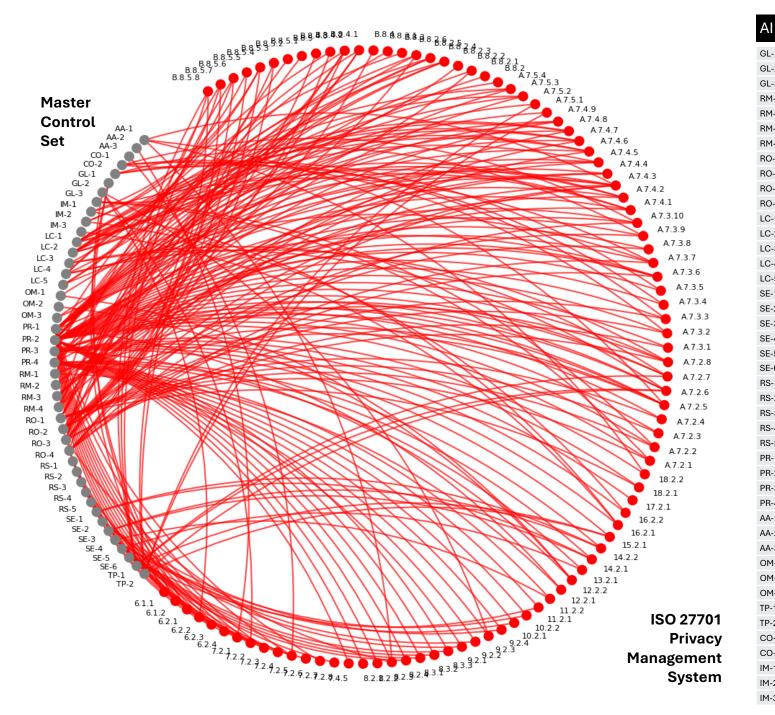


GL-2 Roles, Responsibilities & Resources GL-3 Strategic Alignment & Objectives RM-1 Risk Management Framework and Governance RM-2 Risk Identification and Impact Assessment	
RM-1 Risk Management Framework and Governance	
RM-2 Risk Identification and Impact Assessment	
RM-3 Risk Treatment and Control Implementation	
RM-4 Risk Monitoring and Response	
RO-1 Regulatory Compliance Framework	
RO-2 Transparency, Disclosure and Reporting	
RO-3 Record-Keeping	
RO-4 Post-Market Monitoring	
LC-1 Data Quality and Governance	
LC-2 System Development and Lifecycle Management	
LC-3 Resource Management and Infrastructure	
LC-4 Technical Documentation	
LC-5 Change Management & Version Control	
SE-1 Security Governance, Architecture and Engineering	ng
SE-2 Identity & Access Management	
SE-3 Software Security	
SE-4 Data Security	
SE-5 Network Security	
SE-6 Physical Security	
RS-1 Human Oversight and Intervention	
RS-2 Safety	
RS-3 Robustness	
RS-4 Explainability and Interpretability	
RS-5 Fairness and Bias Management	
PR-1 Privacy by Design and Governance	
PR-2 Personal Data Management	
PR-3 Privacy Compliance and Monitoring	
PR-4 Privacy-Enhancing Technologies and Mechanism	S
AA-1 Internal Assessment & Audit	
AA-2 Independent Assessment and Certification	
AA-3 Safety and Security Validation	
OM-1 System Performance Monitoring	
OM-2 Event Logging	
OM-3 Continuous Improvement	
TP-1 Third-Party Provider Responsibilities	
TP-2 Supplier Risk Management	
CO-1 Al System Transparency	
CO-2 Stakeholder Engagement and Feedback	
IM-1 Incident Detection and Response	
IM-2 Incident Reporting and Notification	
IM-3 Incident Analysis and Improvement	





GL-1	Executive Commitment and Accountability
GL-2	Roles, Responsibilities & Resources
GL-3	Strategic Alignment & Objectives
RM-1	Risk Management Framework and Governance
RM-2	Risk Identification and Impact Assessment
RM-3	Risk Treatment and Control Implementation
RM-4	Risk Monitoring and Response
RO-1	Regulatory Compliance Framework
RO-2	Transparency, Disclosure and Reporting
RO-3	Record-Keeping
RO-4	Post-Market Monitoring
LC-1	Data Quality and Governance
LC-2	System Development and Lifecycle Management
LC-3	Resource Management and Infrastructure
LC-4	Technical Documentation
LC-5	Change Management & Version Control
SE-1	Security Governance, Architecture and Engineering
SE-2	Identity & Access Management
SE-3	Software Security
SE-4	Data Security
SE-5	Network Security
SE-6	Physical Security
RS-1	Human Oversight and Intervention
RS-2	Safety
RS-3	Robustness
RS-4	Explainability and Interpretability
RS-5	Fairness and Bias Management
PR-1	Privacy by Design and Governance
PR-2	Personal Data Management
PR-3	Privacy Compliance and Monitoring
PR-4	Privacy-Enhancing Technologies and Mechanisms
AA-1	Internal Assessment & Audit
AA-2	Independent Assessment and Certification
AA-3	Safety and Security Validation
OM-1	System Performance Monitoring
OM-2	Event Logging
OM-3	Continuous Improvement
TP-1	Third-Party Provider Responsibilities
TP-2	Supplier Risk Management
CO-1	Al System Transparency
CO-2	Stakeholder Engagement and Feedback
IM-1	Incident Detection and Response
IM-2	Incident Reporting and Notification
IM-3	Incident Analysis and Improvement



GL-1	Executive Commitment and Accountability
GL-2	Roles, Responsibilities & Resources
GL-3	Strategic Alignment & Objectives
RM-1	Risk Management Framework and Governance
RM-2	Risk Identification and Impact Assessment
RM-3	Risk Treatment and Control Implementation
RM-4	Risk Monitoring and Response
RO-1	Regulatory Compliance Framework
RO-2	Transparency, Disclosure and Reporting
RO-3	Record-Keeping
RO-4	Post-Market Monitoring
LC-1	Data Quality and Governance
LC-2	System Development and Lifecycle Management
LC-3	Resource Management and Infrastructure
LC-4	Technical Documentation
LC-5	Change Management & Version Control
SE-1	Security Governance, Architecture and Engineering
SE-2	Identity & Access Management
SE-3	Software Security
SE-4	Data Security
SE-5	Network Security
SE-6	Physical Security
RS-1	Human Oversight and Intervention
RS-2	Safety
RS-3	Robustness
RS-4	Explainability and Interpretability
RS-5	Fairness and Bias Management
PR-1	Privacy by Design and Governance
PR-2	Personal Data Management
PR-3	Privacy Compliance and Monitoring
PR-4	Privacy-Enhancing Technologies and Mechanisms
AA-1	Internal Assessment & Audit
AA-2	Independent Assessment and Certification
AA-3	Safety and Security Validation
OM-1	System Performance Monitoring
OM-2	Event Logging
OM-3	Continuous Improvement
TP-1	Third-Party Provider Responsibilities
TP-2	Supplier Risk Management
CO-1	Al System Transparency
CO-2	Stakeholder Engagement and Feedback
IM-1	Incident Detection and Response
IM-2	Incident Reporting and Notification
IM-3	Incident Analysis and Improvement



If you're doing AI Governance for real, subscribe at ethos-ai.org for free, practical guidance and resources