Gate Way Solutions, LLC
1728 Corporate Crossing, Suite 5
O'Fallon, IL 62269
www.gatewaysolutions.com

AISIC Task Force 1.3 – Gen AI Risks and Associated Controls
NIST 600-1 Compliance Checklist (VRT)

Third-Party Vendors and Tools

Risk Assessment and Management:

ID #	Questions	References	Yes	No	NA	Remarks
	1. Risk Assessment Framework: Have you implemented a specific risk assessment framework for evaluating the potential risks associated with third-party generative AI tools?	NIST SP 800-37 Rev. 2				
	2. Periodic Risk Reviews: Do you conduct periodic reviews of the risks associated with third-party generative AI tools?	ISO/IEC 27001:2013				
	3. Risk Categorization: Have you categorized risks related to third-party generative AI tools based on severity and impact on your organization?	NIST SP 800-30 Rev. 1				
	4. Threat Modeling: Does your company perform threat modeling exercises specific to third-party generative AI tools?	NIST SP 800-53 Rev. 5				

Contracts and Agreements:

ID #	Questions	References	Yes	No	NA	Remarks
	5. Contractual Obligations: Do your contracts with third-party generative AI vendors specify obligations for data privacy, security, and intellectual property protection?	GDPR, Article 28				

	6. Liability Clauses: Do your contracts include clear liability clauses related to potential breaches or misuse of generative AI tools by third parties?	CIS Controls v8, Control 16.6				
	7. Termination Rights: Do you have contractual rights to terminate agreements with third-party generative AI vendors in the event of non-compliance or security breaches?	ISO/IEC 27018:2019				
	8. IP Rights Clauses: Are there specific clauses in your contracts that address the protection of intellectual property rights when using third-party generative AI tools?	WIPO Model IP Clauses				

Supplier and Vendor Management:

ID #	Questions	References	Yes	No	NA	Remarks
	9. Supplier Vetting Process: Do you have a formal vetting process for evaluating third-party generative AI vendors before integration?	NIST SP 800-161 Rev. 1				
	10. Ongoing Vendor Monitoring: Is there a process for ongoing monitoring of third-party generative AI vendors' compliance with NIST 600-1 standards?	ISO/IEC 27002:2022				
	11. Vendor Performance Metrics: Do you measure the performance of third-party generative AI vendors against predefined metrics related to security, privacy, and compliance?	NIST SP 800-55 Rev. 1				
	12. Supplier Audits: Do you conduct regular audits of third-party generative AI suppliers to ensure they adhere to your security and compliance requirements?	ISO 9001:2015				

Data Privacy and Content Provenance:

ID #	Questions	References	Yes	No	NA	Remarks

	13. Data Privacy Impact Assessments: Have you conducted data privacy impact assessments (DPIAs) for all third-party generative AI tools used?	GDPR, Article 35				
	14. Data Anonymization: Do the third-party generative AI tools you use ensure data anonymization where applicable?	NIST SP 800-122				
	15. Data Ownership: Is data ownership clearly defined and agreed upon with third-party generative AI vendors?	ISO/IEC 27018:2019				
	16. Provenance Tracking Tools: Do you use specific tools or methods to track the provenance of data processed by third-party generative AI systems?	NIST SP 800-53 Rev. 5				

Security and Compliance:

ID #	Questions	References	Yes	No	NA	Remarks
	17. Security Protocols: Are there documented security protocols in place for the integration and operation of third-party generative AI tools?	NIST SP 800-53 Rev. 5				
	18. Encryption Standards: Do you require third-party generative AI tools to adhere to encryption standards for data at rest and in transit?	FIPS 140-3				
	19. Access Control: Are there strict access control measures for third-party generative AI tools, ensuring only authorized personnel can access sensitive data?	NIST SP 800-63B				
	20. Compliance Verification: Do you verify that third-party generative AI tools comply with all relevant legal and regulatory standards, including NIST 600-1?	ISO/IEC 27001:2013				

Incident Management:

ID #	Questions	References	Yes	No	NA	Remarks
	21. Incident Response Plans: Have you established incident response plans specifically tailored for breaches or issues related to third-party generative AI tools?	NIST SP 800-61 Rev. 2				

	22. Breach Notification Requirements: Do your contracts with third-party vendors include breach notification requirements within a specified timeframe?	GDPR, Article 33				
	23. Post-Incident Review: After an incident involving third-party generative AI tools, do you conduct a post-incident review to identify and mitigate future risks?	NIST SP 800-184				
	24. Incident Reporting Channels: Are there clear channels for reporting and addressing incidents related to third-party generative AI tools?	ISO/IEC 27035-1:2016				

Intellectual Property and Licensing:

ID #	Questions	References	Yes	No	NA	Remarks
	25. Licensing Compliance: Do you verify that third-party generative AI tools are properly licensed and comply with all intellectual property laws?	WIPO Copyright Treaty				
	26. Content Ownership: Is the ownership of content generated by third-party AI tools clearly established and documented (Terms of Service or End User License Agreements)	NIST 600-1 GV-6.1-004				
	27. IP Infringement Monitoring: Do you have mechanisms in place to monitor and address potential IP infringements by third-party generative AI tools?	DMCA, Section 512				

Training and Awareness:

ID #	Questions	References	Yes	No	NA	Remarks
	28. Employee Training: Have your employees received training on the risks and compliance requirements related to third-party generative AI tools?	NIST SP 800-50				
	29. Third-Party Risk Awareness: Are your employees aware of the specific risks associated with the use of third-party generative AI tools in your organization?	ISO/IEC 27002:2022				

	30. Policy Communication: Have you communicated policies regarding the use of third-party generative AI tools to all relevant stakeholders within your organization?	NIST SP 800-100				

Governance and Oversight:

ID #	Questions	References	Yes	No	NA	Remarks
	31. Governance Framework: Is there a governance framework in place for managing the use of third-party generative AI tools within your organization?					
	32. Oversight Committees: Do you have oversight committees or roles specifically responsible for monitoring compliance with NIST 600-1 in the context of third-party AI tools?	ISO/IEC 38500:2015				
	33. Periodic Reviews: Do you conduct periodic reviews of governance practices related to third-party generative AI tools?	NIST SP 800-53 Rev. 5				

Technology and Integration:

ID #	Questions	References	Yes	No	NA	Remarks
	34. Technology Assessments: Do you perform technology assessments before integrating third-party generative AI tools into your systems?	ISO/IEC 27001:2013				
	35. System Compatibility: Is the compatibility of third-party generative AI tools with your existing systems thoroughly evaluated before integration?	NIST SP 800-53 Rev. 5				
	36. Fallback Mechanisms: Have you implemented fallback mechanisms in case of failure or malfunction of third-party generative AI tools?	ITIL 4				

Data Security and Confidentiality:

ID #	Questions	References	Yes	No	NA	Remarks

	37. Data Segmentation: Do you segment sensitive data when using third-party generative AI tools to minimize potential exposure?	NIST SP 800-125				
	38. Confidentiality Agreements: Are confidentiality agreements in place with third-party vendors to protect sensitive information?	ISO/IEC 27018:2019				
	39. Data Retention Policies: Do your data retention policies include specific guidelines for data processed by third-party generative AI tools?	NIST SP 800-88 Rev. 1				

Ethical Considerations:

ID #	Questions	References	Yes	No	NA	Remarks
	40. Bias Detection: Do you evaluate third-party generative AI tools for potential biases in their outputs?	IEEE 7003-2021				
	41. Ethical Use Policies: Are there ethical use policies in place for the deployment of third-party generative AI tools?	ISO/IEC 23894				
	42. Human Oversight: Is there a requirement for human oversight of critical decisions made by or involving third-party generative AI tools?					