



JANUCAT Data Privacy Governance

Aug 2023, ©JANUSEC

Contents

- ❑ Three Core Questions of Data Privacy & the Solution
- ❑ Introduction of JANUCAT
- ❑ Compliance Method of JANUCAT
- ❑ Data Privacy Governance Framework Demo

Three Core Questions of Data Privacy & the Solution

- What data are we processing?
 - To maintain data inventories (processing activities, assets and recipients)
 - JANUCAT provides data inventories module that includes all the elements required by GDPR
- Are these processing compliant?
 - To perform assessments (DPIA/PIA, TIA, LIA etc.)
 - JANUCAT provides assessments module
- How to demonstrate compliance?
 - Compliance records of all processing activities
 - Technical and organizational measures for regulating processing activities
 - JANUCAT provides an accountability framework to guide compliance practices

Introduction of JANUCAT

JANUCAT is a data privacy governance solutions aimed at building Compliance, Accountability and Transparency.

The main functions of JANUCAT include:

- Records of processing activities
- Data protection impact assessments, asset security assessments
- Records of control measures
- etc.,

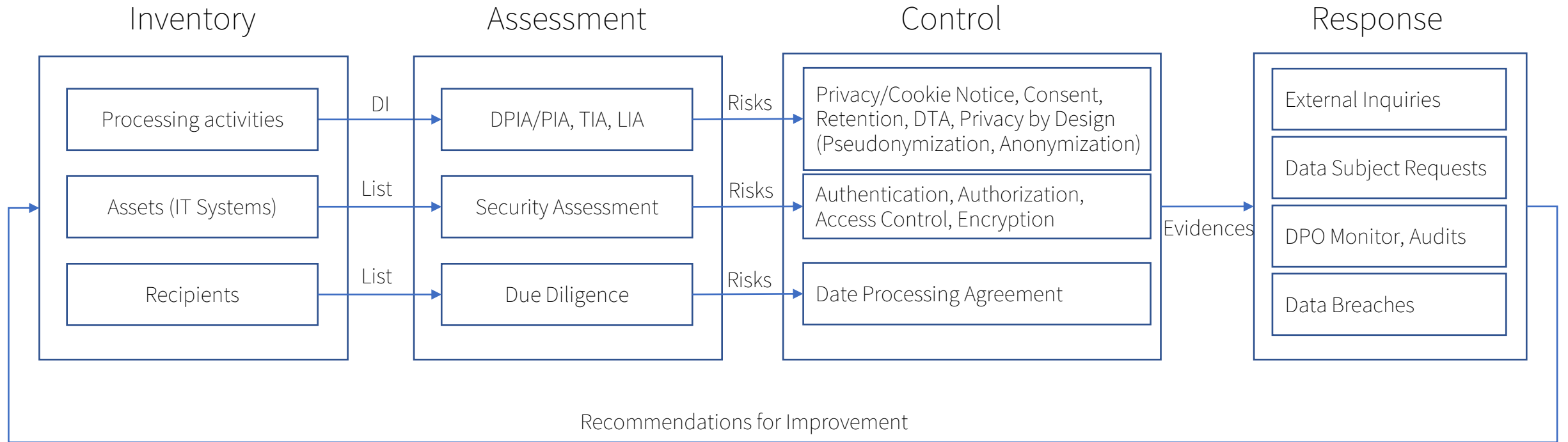
to help enterprises demonstrate privacy compliance with accountability (GDPR etc.).

Two modes available:

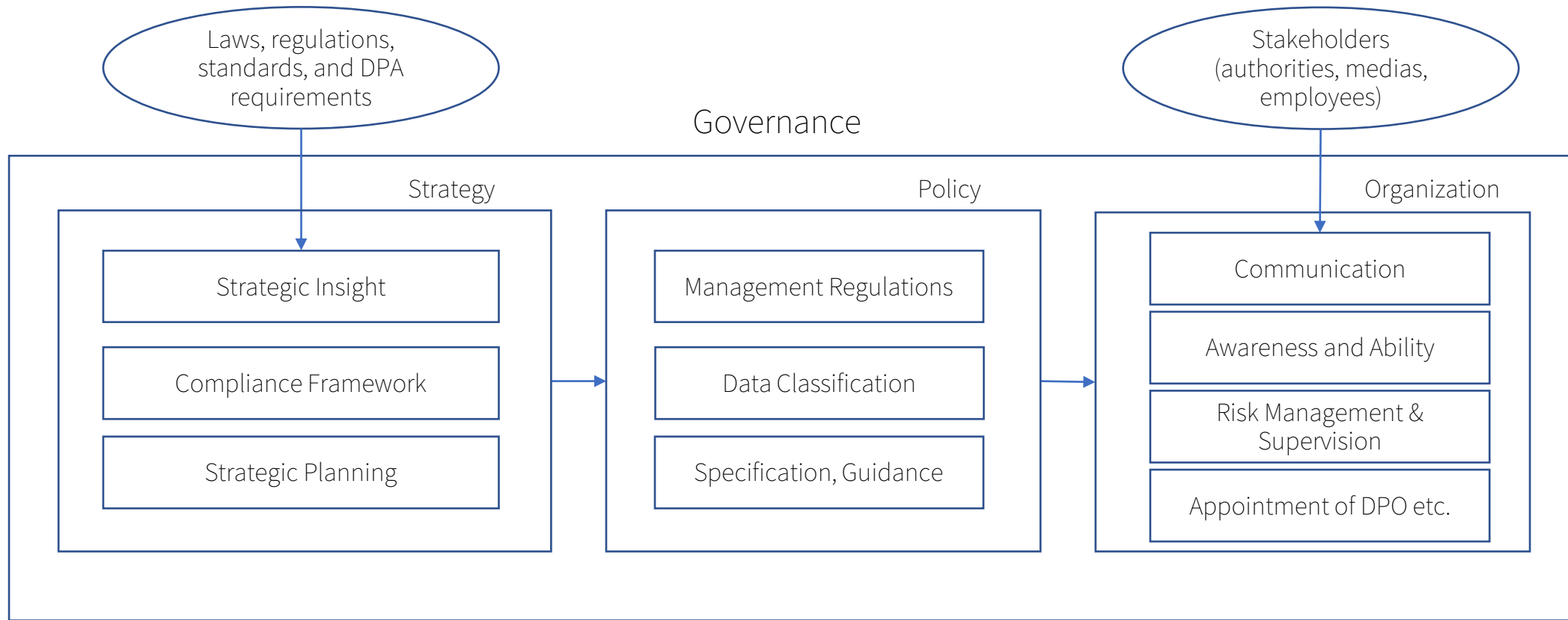
- SaaS Cloud Service Mode
- On-Premise/Private Deployment Mode (Debian and PostgreSQL maintenance experience is required)

Free trial: <https://www.janusec.com/free-trial>

Compliance Method by JANUCAT (Part 1: Business Unit)



Compliance Method by JANUCAT (Part 2: Governance Unit)



Through strategic planning, policy formulation, optimization of organizational and decision-making mechanisms, systematic direction and supervision of business processing activities are carried out to achieve the goals of data privacy compliance, accountability, and transparency.

Summary of JANUCAT Data Privacy Governance Framework (GIACR)



JANUCAT GIACR Framework

Function	Responsible Organization	Key Measures
Governance	Governance or Risk Control Unit	Provide systematic direction and supervision for business units through: <ul style="list-style-type: none"> • Strategy • Policy • Organization
Inventory	Business Unit	Maintain inventories of: <ul style="list-style-type: none"> • Processing activities • Assets • Recipients
Assessment	Business Unit	Perform assessments such as: <ul style="list-style-type: none"> • DPIA/PIA, TIA, LIA • Security • Due diligence
Control	Business Unit	Implement technical and organizational measures: <ul style="list-style-type: none"> • Privacy/Cookie notice • Consent • Retention • DTA, DPA • Anonymization, pseudonymization • Encryption
Response	Business Unit	Continuous improvement by responding to breaches, requests, audit findings and external inquiries

JANUCAT Data Privacy Governance Framework Demo (Part 1)

Function	Measure Grouping	Control Measure	Must	Special Instructions	Reference
1 Governance (治理)	1.1 Strategy (战略)	1.1.1 Routinely gain insight into external laws and regulations, enforcement cases, standards and best practices, and perform summaries and gap analyses (例行洞察外部法律法规、执法案例、标准和最佳实践、总结与差距分析)			
		1.1.2 Based on the summary and gap analysis, determine the development plan and project approval, including but not limited to continuously converting external requirements into internal policy documents, improving the process of building data security and privacy protection by design and by default, etc. (基于总结与差距分析, 确定发展规划与项目立项, 包括但不限于持续将外部要求转换为内部政策文件、完善从设计开始构建默认的数据安全与隐私保护的流程等)			
		1.1.3 Establish the vision of data security and privacy protection, and use the internal and external speeches of the management to set the tone for all employees to achieve compliance (确立数据安全与隐私保护的愿景, 并借助管理层的内外部发言, 奠定全员努力达成合规的基调)			
	1.2 Policies (政策)	1.2.1 Develop a general policy that clearly defines the principles to ensure privacy compliance and data security (建立总体政策, 明确保障隐私合规与数据安全的原则)			
		1.2.2 Clarify the responsibilities and operating mechanisms of internal departments (明确内部各部门的职责与运作机制)			
		1.2.3 Improve protection policies in various sub-sectors, covering minors, employees, specific business areas, etc. (完善各细分领域的保护政策, 覆盖未成年人、雇员、特定业务领域等)			
		1.2.4 Publish management regulations for privacy statement, entrusted processing, cross border transfer and Data subject rights etc., as needed (根据需要, 发布管理规定, 包括隐私声明、委托处理、跨境转移、数据主体权利保障等)			
	1.3 Organization (组织)	1.3.1 Establish a privacy protection and data security governance team to provide guidance, training for business, and monitor business compliance (建立隐私保护和数据安全治理团队, 为业务提供指导, 培训, 并监督业务合规)			
		1.3.2 Designation of DPO (任命DPO)	Y	The corresponding role in China is PIPD (中国对应角色为个人信息保护负责人)	GDPR Article 37, PIPL Article 52
		1.3.3 Designation of representative for offshore business (为离岸业务任命代表)	Y		GDPR Article 27, PIPL Article 53
		1.3.4 Awareness and capacity enhancement (意识和能力提升)			
		1.3.5 Perform inspections, monitoring and metrics (执行稽查, 监控和度量)			
		1.3.6 Establish a decision-making mechanism for risk management, such as tracking and managing risks through routine meetings (建立风险管理的决策机制, 如通过例行会议跟踪和管理风险)			

JANUCAT Data Privacy Governance Suite



Usage scenarios

- Scenario 1: External or Internal Audit
 - Check the records of processing activities and export them as pdf files
 - Check DPIA/PIA or other assessments reports and export them as pdf files
 - Present these PDF files to the auditor as evidences
- Scenario 2: Privacy Protection Operations, Metrics and Reports
 - Track issues with internal privacy protection implementation
 - Metrics and reports
 - As a platform for daily privacy protection, used for internal management improvement and ensuring compliance

Thank you!

<https://www.janusec.com/>