

Verification of Declaration of Adherence

Declaring Company: ServiceNow Inc.



EU
CLOUD
COC

Verification-ID 2022LVL02SCOPE3113

Date of Approval July 2022

Valid until July 2023

Table of Contents

Verification of Declaration of Adherence	1
1 Verification against v2.11 of the EU Cloud CoC	5
2 List of declared services	5
2.1 IT Service Management: ITSM, ITSM Professional and ITSM Enterprise	5
2.1.1 ITSM	5
2.1.2 ITSM Professional	5
2.1.3 ITSM Enterprise	6
2.2 IT Operations Management: ITOM Standard, ITOM Professional and AIOps Enterprise	6
2.2.1 ITOM Standard	6
2.2.2 ITOM Professional	7
2.2.3 AIOps Enterprise	7
2.3 IT Asset Management: ITAM	7
2.4 Integrated Risk Management: IRM Standard, IRM Professional and IRM Enterprise	7
2.4.1 IRM Standard (GRC)	7
2.4.2 IRM Professional (GRC)	7
2.4.3 IRM Enterprise (GRC)	8
2.5 Legal Service Delivery: LSD	8
2.6 Safe Workplace Suite Pro, Workplace Service Delivery: WSD	8
2.6.1 Safe Workplace Suite Pro	8
2.6.2 Workplace Service Delivery	8
2.7 App Engine Starter, App Engine	8
2.6.3 App Engine Starter	8
2.6.4 App Engine	9
2.7 IntegrationHub Starter, IntegrationHub Professional and IntegrationHub Enterprise	9

2.7.1	Starter	9
2.7.2	Professional	10
2.7.3	Enterprise	11
2.8	Customer Service Management: CSM Standard, CSM Professional and CSM Enterprise	13
2.8.1	Customer Service Management Standard	13
2.8.2	Customer Service Management Professional	14
2.8.3	Customer Service Management Enterprise	14
2.9	HR Service Delivery: HRSD Professional and HRSD Enterprise	14
2.9.1	HR Service Delivery Professional	14
2.9.2	HR Service Delivery Enterprise	15
2.10	Security Operations	15
2.11	Field Service Management: FSM Standard and FSM Professional	15
2.11.1	Field Service Management Standard	15
2.11.2	Field Service Management Enterprise	15
2.12	Strategic Portfolio Management: SPM Standard, SPM Professional	16
2.12.1	SPM (Formerly ITBM) STANDARD	16
2.12.2	SPM (Formerly ITBM) PROFESSIONAL	16
2.13	Application Portfolio Management: APM V2	16
2.13.1	Application Portfolio Management V2	16
3	Verification Process - Background	17
3.1	Approval of the Code and Accreditation of the Monitoring Body	17
3.2	Principles of the Verification Process	17
3.3	Multiple Safeguards of Compliance	17
3.4	Process in Detail	18
3.4.1	Levels of Compliance	19
3.4.2	Final decision on the applicable Level of Compliance	20
3.5	Transparency about adherence	20
4	Assessment of declared services by ServiceNow (see 2.)	20

4.1	Fact Finding	20
4.2	Selection of Controls for in-depth assessment	21
4.3	Examined Controls and related findings by the Monitoring Body	21
4.3.1	Examined Controls	21
4.3.2	Findings by the Monitoring Body	22
5	Conclusion	24
6	Validity	24

1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)¹ in its version 2.11 (**'v2.11'**)² as of December 2020.

Originally being drafted by the Cloud Select Industry Group³ (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC⁴ incorporates feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code v2.11 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)⁵.

2 List of declared services

2.1 IT Service Management: ITSM, ITSM Professional and ITSM Enterprise

2.1.1 ITSM

- | | |
|-----------------------------|------------------------------------|
| ■ Incident Management | ■ Benchmarks |
| ■ Problem Management | ■ Surveys and Assessments |
| ■ Change Management | ■ Virtual Agent |
| ■ Request Management | ■ Digital Portfolio Management |
| ■ Asset and Cost Management | ■ DevOps |
| ■ Walk-Up Experience | ■ Predictive Intelligence |
| ■ Agent Workspace | ■ Dynamic Translation |
| ■ Now Mobile | ■ Performance Analytics |
| ■ Mobile Agent | ■ Continual Improvement Management |
| ■ Knowledge Management | ■ Service Owner Workspace |
| ■ Configuration Management | ■ Vendor Manager Workspace |
| ■ Reporting | ■ Workforce Optimization |
| ■ Service Level Management | ■ Process Optimization |

2.1.2 ITSM Professional

- | | |
|-----------------------|----------------------|
| ■ Incident Management | ■ Problem Management |
|-----------------------|----------------------|

¹ <https://eucoc.cloud>

² <https://eucoc.cloud/get-the-code>

³ <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct>

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>

⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

- Change Management
- Request Management
- Asset and Cost Management
- Walk-Up Experience
- Agent Workspace
- Now Mobile
- Mobile Agent
- Knowledge Management
- Configuration Management
- Reporting
- Service Level Management
- Benchmarks
- Surveys and Assessments
- Virtual Agent
- Digital Portfolio Management
- DevOps
- Predictive Intelligence
- Dynamic Translation
- Performance Analytics
- Continual Improvement Management
- Service Owner Workspace
- Vendor Manager Workspace
- Workforce Optimization
- Process Optimization

2.1.3 ITSM Enterprise

- Incident Management
- Problem Management
- Change Management
- Request Management
- Asset and Cost Management
- Walk-Up Experience
- Agent Workspace
- Now Mobile
- Mobile Agent
- Knowledge Management
- Configuration Management
- Reporting
- Service Level Management
- Benchmarks
- Surveys and Assessments
- Virtual Agent
- Digital Portfolio Management
- DevOps
- Predictive Intelligence
- Dynamic Translation
- Performance Analytics
- Continual Improvement Management
- Service Owner Workspace
- Vendor Manager Workspace
- Workforce Optimization
- Process Optimization

2.2 IT Operations Management: ITOM Standard, ITOM Professional and AIOps Enterprise

2.2.1 ITOM Standard

- Discovery
- Service Mapping
- Certificate Management
- Firewall Audit
- Service Graph Connectors
- Configuration Management Database
- Agent Client Collector
- Event Management
- Metric Intelligence
- Site Reliability Operations
- Health Log Analytics

2.2.2 ITOM Professional

- Discovery
- Service Mapping
- Certificate Management
- Firewall Audit
- Service Graph Connectors
- Configuration Management Database
- Agent Client Collector
- Event Management
- Metric Intelligence
- Site Reliability Operations
- Health Log Analytics

2.2.3 AIOps Enterprise

- Discovery
- Service Mapping
- Certificate Management
- Firewall Audit
- Service Graph Connectors
- Configuration Management Database
- Agent Client Collector
- Event Management
- Metric Intelligence
- Site Reliability Operations
- Health Log Analytics

2.3 IT Asset Management: ITAM

- Hardware Asset Management
- Software Asset Management
- Cloud Insights
- IT Asset Offboarding
- SaaS License Management

2.4 Integrated Risk Management: IRM Standard, IRM Professional and IRM Enterprise

2.4.1 IRM Standard (GRC)

- Policy and Compliance Management
- Risk Management
- Performance Analytics
- Audit Management
- Use Case Accelerators
- Virtual Agent (chatbot)
- Predictive Intelligence
- Continuous Authorization and Monitoring
- Regulatory Change
- Operational Resilience
- Operational Risk Management

2.4.2 IRM Professional (GRC)

- Policy and Compliance Management
- Risk Management
- Performance Analytics
- Audit Management
- Use Case Accelerators
- Virtual Agent (chatbot)
- Predictive Intelligence
- Continuous Authorization and Monitoring

- Regulatory Change
- Operational Resilience

2.4.3 IRM Enterprise (GRC)

- Policy and Compliance Management
- Risk Management
- Performance Analytics
- Audit Management
- Use Case Accelerators
- Virtual Agent (chatbot)

- Operational Risk Management

- Predictive Intelligence
- Continuous Authorization and Monitoring
- Regulatory Change
- Operational Resilience
- Operational Risk Management

2.5 Legal Service Delivery: LSD

- Request management
- Legal Counsel Centre
- Legal Matter Management
- Legal Practice Applications
- Knowledge Management

- Employee Centre
- NOW Mobile
- Mobile Agent
- Virtual Agent
- Reporting

2.6 Safe Workplace Suite Pro, Workplace Service Delivery: WSD

2.6.1 Safe Workplace Suite Pro

- Safe Workplace Suite
- Workplace Reservation Management
- Workplace Visitor Management
- Workplace Indoor Mapping
- Reporting

- Virtual Agent
- Now Mobile
- Employee Center
- Performance Analytics

2.6.2 Workplace Service Delivery

- Safe Workplace Suite
- Workplace Reservation Management
- Workplace Visitor Management
- Workplace Indoor Mapping
- Reporting
- Virtual Agent

- Now Mobile
- Employee Center
- Performance Analytics
- Workplace Case Management
- Workplace Space Management
- Workplace Move Management

2.7 App Engine Starter, App Engine

2.6.3 App Engine Starter

- Custom Table Limits
- UI Builder

- Automated Test Framework
- Delegated Development

- Flow Designer
- Service Creator
- Service Portal
- Studio IDE
- Guided App Creator
- Now Mobile
- Mobile Studio
- Agent Workspace
- Process Automation Designer
- App Engine Management Center

2.6.4 App Engine

- Unlimited Apps
- UI Builder
- Automated Test Framework
- Delegated Development
- Flow Designer
- Service Creator
- Service Portal
- Studio IDE
- Guided App Creator
- Now Mobile
- Mobile Studio
- Agent Workspace
- Process Automation Designer
- App Engine Management Center
- App Engine Studio
- Prebuilt Templates
- Performance Analytics
- Predictive Intelligence
- Virtual Agent

2.7 IntegrationHub Starter, IntegrationHub Professional and IntegrationHub Enterprise⁶

Subject to the Code is the connectivity feature, i.e., the integration subject to appropriate technical and organisational measures. Not in scope of this declaration of adherence is any of the services that might be integrated by the Customer respectively the processing activities of such services. The listing in this report shall only reflect the capabilities at the time of assessment.

2.7.1 Starter

Spokes

- AI Search
- Cisco WebEx Teams
- Cisco WebEx Meetings
- Continuous Integration and Continuous Delivery (CICD) Spoke
- Google Hangouts

⁶ **Provided by the CSP:** Definitions: A Spoke is a predefined action, flow, and/or integration for connecting or automating third party systems or processes within Flow Designer. A Protocol is the communication format of mechanism used when interacting with a third-party system. A Utility is a common, reusable, solution to facilitate integration development.

*Each package includes entitlement to all spokes, protocols, and utilities in lower tier packages.

** Remote Instance Spoke Transactions are not counted against Transaction entitlement.

- Goto
- Looker
- Microsoft Teams
- Microsoft Teams Graph API
- Microsoft Teams Communications
- Miro
- PagerDuty
- Plivo
- Rally
- Roadmunk

Protocols

- REST

Utilities

- Zip

Features

- Payload Builder step
- Retry policies

- ServiceNow Remote Instance (formerly eBonding)
- Slack
- Slack WebHooks
- Smartrecruiters
- Utility Actions
- Vonage
- Workfront
- Workplace from Facebook
- Zoom

- SOAP

- Remote Tables

2.7.2 Professional

Spokes

- Agent Client Collector
- Ansible
- Docker
- F5 BIG-IP
- GitHub
- GitLab
- Gremlin
- Infoblox
- Jenkins
- Jenkins V2
- JIRA
- Kubernetes
- Twitter
- Microsoft Azure Artifacts
- Azure DevOps Boards
- Aha!
- Amazon Alexa
- Amazon Elastic Container Service
- Azure Automation
- BMC Remedy
- Box
- Calendly
- Confluence Cloud
- Dropbox Business
- Google Calendar
- Google Directory

- Google Docs
- Google Drive
- Google Cloud DNS
- Gmail
- Google Sheets
- Google Tasks
- Go Notify
- Microsoft AD
- Microsoft AD v2
- Microsoft Azure AD
- Microsoft Azure Application Insights
- Microsoft Azure Resource Management
- Microsoft Exchange Online
- Microsoft Exchange Server
- Microsoft 365 Excel
- Microsoft Intune
- Microsoft OneDrive
- Microsoft OneDrive Document Services
- Microsoft SharePoint
- Monday.com
- Okta
- Oracle Autonomous DB
- Oracle Block Storage
- Oracle Boot Volume
- Oracle Cloud IAM
- Oracle Compute Engine
- Oracle Object Storage Management
- Oracle Virtual Cloud Network
- Qualtrics
- SABA
- Secureworks CTP
- Shodan
- Smartsheet
- Survey Monkey
- Trello
- Wrike

Apps

- Orchestration

Protocols

- Powershell
- SSH
- JDBC

Features

- JSON Parser
- XML Parser

2.7.3 Enterprise

Spokes

- Adobe Experience Platform
- Adobe Sign
- Amazon Connect
- Amazon CloudWatch
- Amazon DynamoDB
- Amazon EC2
- AWS Elastic BeanStalk
- Amazon EBS
- AWS IAM
- Amazon RDS
- Amazon Route53
- Amazon S3

- Amazon SNS
- Amazon VPC
- Automation Anywhere
- AWS Certificate Manager
- AWS CloudFormation
- AWS Elastic Load Balancing
- AWS Lambda
- AWS OpsWorks
- Azure Blob Storage
- Azure Traffic Manager
- BigFix Inventory
- Blue Prism
- Confluent Kafka REST Proxy
- Cornerstone
- Coupa
- CrowdStrike
- DocuSign
- First Advantage
- Google Identity and Access
- Google Cloud Datastore
- Google Cloud Functions
- Google Cloud Load Balancer
- Google Cloud Pub Sub
- Google Cloud SQL
- Google Cloud Storage
- Google Cloud Virtual Network
- Google Cloud VPC Access
- Google Compute Engine
- Google Persistent Disk
- Jamf
- Jira Service Management
- Microsoft 365
- Microsoft Azure Cosmos DB
- Microsoft Azure Managed Storage
- Microsoft Azure SQL Database
- Microsoft Azure Notification Hub
- Microsoft Azure Virtual Machines
- Microsoft Azure Virtual Network
- Microsoft Dynamics CRM
- Microsoft Endpoint Configuration Manager
- Microsoft Dynamics 365 for Finance and Operations
- Microsoft SCCM Usage Metering
- Microsoft Security Response Center
- Oracle EBS spoke
- Oracle Financial Cloud spoke
- Oracle HCM Cloud
- Oracle Peoplesoft Financial
- Pluralsight
- Salesforce
- Salesforce Marketing Cloud
- SAP Ariba
- SAP Concur
- SAP Commerce Cloud
- SAP ECC IDoc
- SAP ECC RFC
- SAP Fieldglass
- SAP S4 HANA IDOC
- SAP S4 HANA RFC
- ServiceNow Kafka Consumer
- SuccessFactors
- SumTotal
- Udemy
- UIPath
- UKG
- UCF
- Workday Financials
- Workday HR
- YouTube
- Zendesk

Apps

- Access
- Management

Automation

- Flow Templates for Access management
- Flow Templates for Notifications
- Flow Templates for Documents Management
- Flow Templates for IntegrationHub Enterprise
- Flow templates for HR Management
- Flow templates for Cloud services
- Remote Process Synchronisation
- Password Reset integration with Okta
- Password Reset integration with Google Directory
- Client software Distribution
- Client Software Distribution 2.0
- Password Reset Integration with AD
- Password Reset Integration with Azure AD
- ServiceNow Kafka Consumer
- Virtual Agent for Citrix ITSM Connector

Features

- Data Stream actions
- Introspection (dynamic inputs and dynamic outputs)
- REST API trigger

2.8 Customer Service Management: CSM Standard, CSM Professional and CSM Enterprise

2.8.1 Customer Service Management Standard

- Agent Workspace
- Case Management
- Omni-Channel
- Self-Service
- Knowledge Management
- Communities
- Walk-Up Experience for Customer Service
- Service Management for Issue Resolution
- Advanced Work Assignment
- Engagement Messenger
- Digital Portfolio Management
- Proactive Customer Service Operations
- Predictive Intelligence
- Performance Analytics
- Virtual Agent
- Playbooks for Customer Service
- Guided Decisions
- Industry Data Models
- Outsourced Customer Service
- Customer Project Management
- Continual Improvement Management
- Vendor Management Workspace
- DevOps Change Velocity
- Workforce Optimization
- Process Optimization

2.8.2 Customer Service Management Professional

- Agent Workspace
- Case Management
- Omni-Channel
- Self-Service
- Knowledge Management
- Communities
- Walk-Up Experience for Customer Service
- Service Management for Issue Resolution
- Advanced Work Assignment
- Engagement Messenger
- Digital Portfolio Management
- Proactive Customer Service Operations
- Predictive Intelligence
- Performance Analytics
- Virtual Agent
- Playbooks for Customer Service
- Guided Decisions
- Industry Data Models
- Outsourced Customer Service
- Customer Project Management
- Continual Improvement Management
- Vendor Management Workspace
- DevOps Change Velocity
- Workforce Optimization
- Process Optimization

2.8.3 Customer Service Management Enterprise

- Agent Workspace
- Case Management
- Omni-Channel
- Self-Service
- Knowledge Management
- Communities
- Walk-Up Experience for Customer Service
- Service Management for Issue Resolution
- Advanced Work Assignment
- Engagement Messenger
- Digital Portfolio Management
- Proactive Customer Service Operations
- Predictive Intelligence
- Performance Analytics
- Virtual Agent
- Playbooks for Customer Service
- Guided Decisions
- Industry Data Models
- Outsourced Customer Service
- Customer Project Management
- Continual Improvement Management
- Vendor Management Workspace
- DevOps Change Velocity
- Workforce Optimization
- Process Optimization

2.9 HR Service Delivery: HRSD Professional and HRSD Enterprise

2.9.1 HR Service Delivery Professional

- Case and Knowledge Management
- Now Mobile
- Agent Workspace
- Mobile Agent
- Universal Request
- Employee Relations

- Employee Center
- Performance Analytics
- Virtual Agent
- Predictive Intelligence

2.9.2 HR Service Delivery Enterprise

- Case and Knowledge Management
- Now Mobile
- Agent Workspace
- Mobile Agent
- Universal Request
- Employee Relations
- Employee Center

2.10 Security Operations

- Security Incident Response
- Vulnerability Response
- Configuration Compliance
- Threat Intelligence

2.11 Field Service Management: FSM Standard and FSM Professional

2.11.1 Field Service Management Standard

- Dynamic Scheduling
- Mobile Agent
- Planned Maintenance
- Asset Management
- Cost Management
- Field Service Contractor Management
- Dispatcher Workspace

2.11.2 Field Service Management Enterprise

- Dynamic Scheduling
- Mobile Agent
- Planned Maintenance
- Asset Management
- Cost Management
- Field Service Contractor Management
- Dispatcher Workspace

- Employee Journey Management
- Enterprise Onboarding and Transitions
- Alumni Service Center
- Employee Document Management

- Performance Analytics
- Virtual Agent
- Predictive Intelligence
- Employee Journey Management
- Enterprise Onboarding and Transitions
- Alumni Service Center
- Employee Document Management

- Performance Analytics for Security Operations
- Event Management
- DLP Incident Response

- Field Service Crew Operations
- Capacity and Reservations Management
- Continual Improvement Management
- Predictive Intelligence
- Virtual Agent
- Performance Analytics
- Field Service Multi-Day Task Scheduling

- Field Service Crew Operations
- Capacity and Reservations Management
- Continual Improvement Management
- Predictive Intelligence
- Virtual Agent
- Performance Analytics
- Field Service Multi-Day Task Scheduling

2.12 Strategic Portfolio Management: SPM Standard, SPM Professional

2.12.1 SPM (Formerly ITBM) STANDARD

- Project Portfolio Management
- Financial Planning -PPM
- Resource Management
- Release Management
- Time Card
- Digital Portfolio Management
- Innovation Management
- Alignment Planner Workspace

2.12.2 SPM (Formerly ITBM) PROFESSIONAL

- Project Portfolio Management
- Financial Planning -PPM
- Resource Management
- Release Management
- Time Card
- Digital Portfolio Management
- Innovation Management
- Alignment Planner Workspace
- Agile Development
- Test Management
- Scrum Programs for Agile 2.0
- Scaled Agile Framework (SAFe)
- Investment Funding
- Predictive Intelligence
- Virtual Agent
- Performance Analytics
- App Engine Starter

2.13 Application Portfolio Management: APM V2

2.13.1 Application Portfolio Management V2

- Application Portfolio Management
- Digital Portfolio Management
- Predictive Intelligence
- Performance Analytics
- App Engine Starter

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR⁷.

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba⁸.

The Code has been officially approved May 2021⁹. SCOPE Europe has been officially accredited as Monitoring Body May 2021¹⁰. The robust and complex procedures and mechanisms can be reviewed by any third party in detail at the website of the EU Cloud CoC alongside a short summary thereof.¹¹

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e., continuous, rigorous, and independent monitoring, an independent complaints' handling and finally any

⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

⁸ <https://scope-europe.eu>

⁹ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

¹⁰ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

¹¹ <https://eucoc.cloud/en/public-register/assessment-procedure/>

CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Control's Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g., by media reports, publications and actions of supervisory authorities are covered.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon make them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.11 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is however no difference in terms of which parts of the Code are covered since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the “First Level of Compliance”, Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body’s report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the “Second Level of Compliance” but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is up to the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark¹² and refer to the Public Register of the EU Cloud CoC¹³ to enable Customers to verify the validity of adherence.

4 Assessment of declared services by ServiceNow (see 2.)

4.1 Fact Finding

Following the declaration of adherence of ServiceNow Inc. (**ServiceNow**), the Monitoring Body provided ServiceNow with a template, requesting ServiceNow to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a “service family”. A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

¹² <https://euococ.cloud/en/public-register/levels-of-compliance/>

¹³ <https://euococ.cloud/en/public-register/>

ServiceNow promptly responded within the template. The provided information consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. ServiceNow provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework.

The Monitoring Body explicitly strived for a common understanding of Cloud Services in the sense of the Code and Cloud Services from a perception of Customers. In this context, the Monitoring Body took into consideration not only the information as provided by ServiceNow in their responses, but also the publicly facing representation of services and products.

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC¹⁴, the Monitoring Body analysed the responses and information provided by ServiceNow.

ServiceNow declared cloud services subject to this declaration of adherence¹⁵ have been externally certified and audited, e.g., ServiceNow holds current ISO 27001 certificates. Notwithstanding other certifications¹⁶, the declaration of adherence referred to the respective ISO 27001 certification within the responses to Section 6 of the Code (IT-Security). As provided by the Code, the Monitoring Body may consider third party certifications and audits. Accordingly, the Monitoring Body did verify the certification and references. Further in-depth checks were not performed, as provided third party certifications adequately indicate compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from ServiceNow which outlined how all the requirements of the Code were met by ServiceNow implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information.

¹⁴ <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

¹⁵ As listed above in section 2

¹⁶ <https://www.servicenow.de/company/trust.html>

The controls selected for this level of review were: 5.1.C, 5.1.D, 5.1.H, 5.2.A, 5.2.E, 5.3.B, 5.3.D, 5.3.G, 5.5.C, 5.5.D, 5.5.E, 5.6.A, 5.7.E, 5.7.F, 5.8.B, 5.10.A, 5.11.A, 5.11.C, 5.13.B, 5.14.A, 5.14.E, 6.1.A, 6.2.P.

4.3.2 Findings by the Monitoring Body

The Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as a Cloud Service Family. In this respect, the Monitoring Body aligned closely with ServiceNow to understand both their internal and external references, as well as their listed Cloud Service under this declaration of adherence. The Monitoring Body concluded that the listed items reflect both Cloud Services and a Cloud Service Family under the Code.

During the process of verification, ServiceNow gave the impression of having prepared the Declaration of Adherence well and thoroughly. Responses being provided were detailed and never created any impression of intentional non-transparency. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

The Monitoring Body did not focus on Section 6, as a current and applicable ISO certification was provided. The Monitoring Body may rely on such external reports and certifications, if those meet the criteria as set out in the Code, which is indicated where such international audit or certification is already being mapped within the Control's Catalogue. Referenced audits and certifications are those international standards, that have been appropriately mapped to Section 6, so that the Monitoring Body has strong indications allowing the Monitoring Body to rely on those. The Monitoring Body analysed the certifications and assessed whether the scope of applicability covered all Controls as provided by the Code. Upon request ServiceNow confirmed that all Cloud Services being declared in this declaration of adherence are covered by the respective certificates.

One area of focus was the understanding of the contractual framework, i.e., the applicable Data Processing Addendum (DPA). ServiceNow updated the Data Processing Addendum during the process, which required the Monitoring Body to ensure assessing the current and applicable version. Additionally, ServiceNow offers different versions of the DPA, depending on Customer needs and requests; e.g., with or without Standard Data Protection Clauses – also referred to as Standard Contractual Clauses – attached as Annex to the DPA.

An area of assessment has also been the possibility for Customers for perform their right to audit. In accordance with the Code, ServiceNow implemented a staggered approach, i.e., Customers may first

seek for relevant information either by Customer Support, existing third-party attestation, and document review. As provided by the contractual framework, Customers may – ultimately and where needed – seek for additional assistance. The Monitoring Body assessed the procedures involved, as well as the expected costs for Customers. The procedures balance the interests of the involved parties, including the confidentiality and security of the data processing of other Customers. To the extent costs are involved, the Monitoring Body concludes that those are not designed to prohibit Customers from performing their due rights, but representing the expected complexities involved.

Regarding third country transfers, ServiceNow relies on Standard Data Protection Clauses, also referred to as Standard Contractual Clauses, as published by the European Commission. ServiceNow stays within the deadlines of implementing the updated version.

Customers are principally enabled to retrieve their data, where needed, as well as respond to data subject requests autonomously. However, in case of need, ServiceNow provides assistance upon request, ensuring GDPR requirements will be met; in this context, the Monitoring Body also analysed whether ServiceNow implemented procedures to adequately respond to requests by Data Protection Supervisory Authorities.

In regards of assistance of Customers in general, ServiceNow assists Customers where needed. Principally, Customers are provided with documentation and third-party attestations. Where the provided information may not suffice, Customers may reach out to ServiceNow and request additional assistance. Likewise, Customers may instruct ServiceNow. ServiceNow has implemented procedures to ensure that instructions are being followed, including mechanisms to ensure that instruction are duly authorized.

In the context of instructions, the Monitoring Body analysed the management of subprocessors and related transparency. ServiceNow has implemented due notification of Customers in case of any changes. Customers can object and take effective measures prior changes are implemented. ServiceNow applies due diligence regarding its subprocessors, safeguarding subprocessors apply no less protective measures as provided by ServiceNow. ServiceNow indicated that the latter is explicitly safeguarded by using internal ServiceNow entities, currently. ServiceNow will extend its procedures, where necessary, once it may use external entities.

Deletion at the end of term and during the term also falls in the scope of instructions, and thus has been subject to evaluation. ServiceNow indicated with its procedures to follow state-of-the-art approaches in ensuring that to be deleted data and end-of-life assets are treated adequately.

5 Conclusion

Given answers by ServiceNow were consistent. Where necessary ServiceNow gave additional information or clarified their given information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service(s) will be listed in the Public Register of the EU Cloud CoC¹⁷ alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by ServiceNow to support the compliance of its service, the Monitoring Body grants ServiceNow with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 24 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify, that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC¹⁸.

Verification-date: July 2022

Valid until: July 2023

Verification-ID: 2022LVL02SCOPE3113

¹⁷ <https://eucooc.cloud/en/public-register/>

¹⁸ <https://eucooc.cloud/en/public-register/>