VISTA INFOSEC®
TRUSTED ADVISORS, ASSURED COMPLIANCE™

3Di

3DI INC SOC2 ATTESTATION CASE STUDY

BACKGROUND

3Di Inc is a leading organization offering advanced technology solutions to government and corporate clients across the USA. The company has its headquarters in Brea, California, and offices in Mumbai, Pune in India. 3Di provides IT & Technology solutions to the government in sectors like Housing, Public Safety & Community Engagement. Their solutions facilitate easy communication, reporting and are known for increasing the operational efficiencies in the sectors. 3Di Inc. also works as a consultant for companies in need of Staff Augmentation, Website Development, Application Developments, & other specialized projects like integration of existing & new technology and services for their Corporate & Government clients across the USA.

OBJECTIVE OF SOC2 AUDIT & ASSESSMENT

The objective behind performing SOC2 Audit was intended to provide interested parties with information about the effectiveness of controls at 3Di System Inc. that may affect the processing of User Organization’s transactions and also to provide users with information about the operating effectiveness of the controls that were tested. The audit report describing the controls is intended to assist user auditors in (1) planning the audit of User Organization’s financial statements and in (2) assessing control risk for assertions in User Organization’s financial statements that may be affected by controls at 3Di Inc.

REQUIREMENTS

Highly experienced Cyber Security Consultants of VISTA InfoSec held an initial scoping call followed by a meeting with the 3Di Inc. to gather details for the SOC2 audit project initiation. The Auditing team of VISTA InfoSec performed an Audit Readiness Assessment to examine 3Di Inc's current level of compliance against the AICPA requirements and provided a detailed report with identified gaps, the effectiveness of controls, and recommendations to address the gaps prior to the SOC2 audit.

SOC2 ASSESSMENT WORKFLOW

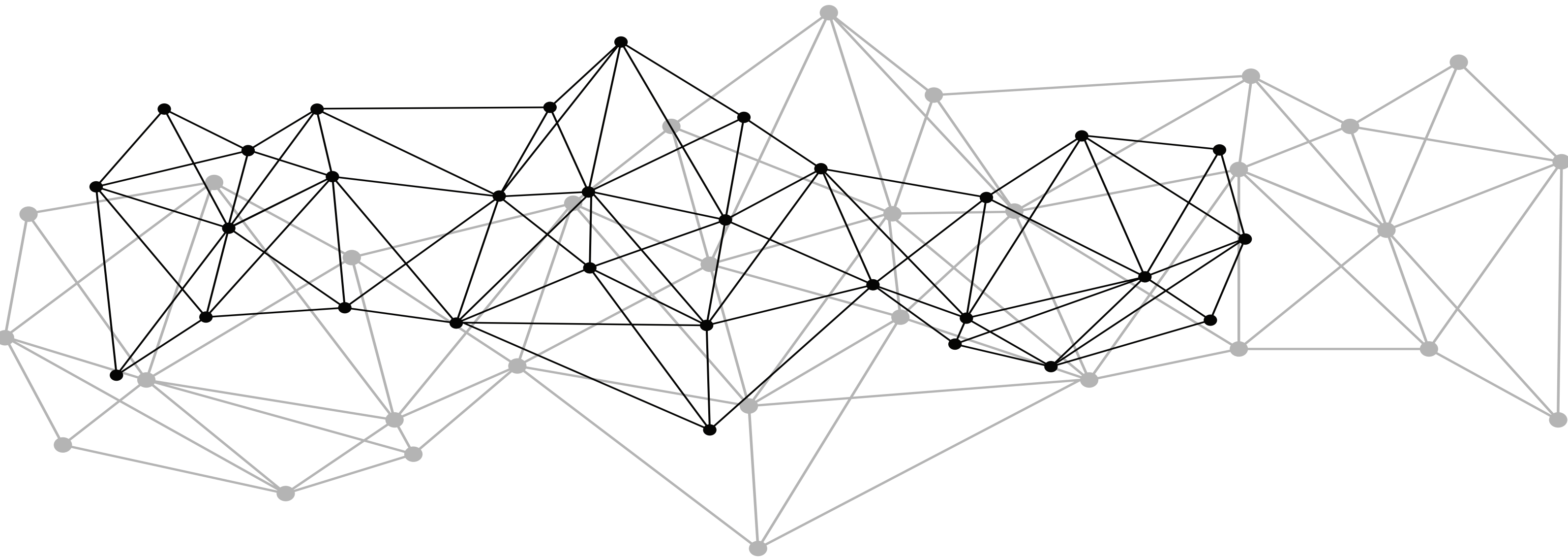
Once the statement of work was signed off with 3Di, VISTA InfoSec with its team of auditors conducted the assessment. The assessment was performed at 3Di Inc.'s office in Mumbai. The project initiation began with a detailed overview and understanding of 3Di Inc's Business, IT infrastructure, work process, and business operations. The assessment included interviews and inquiries conducted with the Management, Supervisory, Staff Personnel, Development Managers, and the Head of Operations and including other members from HR, IT, Networks and Development department to determine the critical areas to be assessed. The assessment also included inspection of documents and records, observation of activities and operations, and the effectiveness of controls surrounding and provided by 3Di Inc.

SOC2 ASSESSMENT PROCESS

	Check List Process of Validation	Description of the Process
SOC2 Compliance Validation Services	**Initial Kick-off**	The initial kick-off for SOC2 Readiness assessment included conducting a meeting with the management and the respective team heads to understand the business operations and work process of 3Di Inc. As a part of this process, VISTA InfoSec sent a set of questionnaires to 3Di to get details about the company.
	Scope Definition	At this stage, VISTA InfoSec along with the team of 3Di Inc. defined and established the scope of work and audit boundaries. This included defining the responsibilities of employees and third parties, and establishing processes.
	Data Gathering	Based on the initial kick-off and scope definition relevant data was gathered from 3Di. The data collected included documents concerning the policies, procedures, processes, agreements, contracts, and documents explaining services, systems, and products provided and information on the infrastructure, software, and people that support business processes and services.
	GAP Analysis	VISTA InfoSec team assessed the organization and evaluated the applicability and scope against the Trust Service Criteria in line with Security, Availability, Process Integrity, Privacy, and Confidentiality of the data. This assessment helped identify gaps that were required to be addressed.

	Check List Process of Validation	Description of the Process
SOC2 Advisory Services	**Awareness Program**	The team of VISTA InfoSec conducted a brief Awareness Training program on SOC2 for the 3Di Inc. This included highlighting the gaps identified against AICPA TSC.
	Asset Identification & Classification	The team of VISTA InfoSec along with 3Di Identified the critical information assets and accordingly classified them into a separate Asset Inventory for further assessment against various risks.
	Risk Analysis	The audit team of VISTA InfoSec conducted a comprehensive risk assessment and analysis to identify the gaps that could impact the business-critical assets of the organization.
	Risk Treatment	The risks identified were then prioritized based on the severity and necessary recommendations were given to strategize appropriate Risk Treatment measures.
	Develop Documentation	The team gathered documents and verified the same pertinent to system controls & infrastructure, policies & procedures including the hiring process, employee separation process, IT policies, help desk process, performance management reviews, documents related to risk assessments & mitigation, physical, environmental security measures & policies, access management, incident management change management, business continuity, disaster management policies, and process, vulnerability scans data restoration and backup processes to name a few.
	User Training Program	The team of VISTA InfoSec offered an end-to-end User Training program for all personnel covered in scope on their specific responsibilities. This was also backed by a set of training documents provided to 3Di Inc for future use and reference.

	Check List Process of Validation	Description of the Process
SOC2 Advisory Services	**Policy Rollout Support**	The team of VISTA InfoSec assisted 3Di Inc in rolling out relevant policies and procedures to support the implemented security measures in alignment with the SOC2 requirements. The document set was created in collaboration with the 3Di team with inputs and validation acquired from the 3Di team.
	Internal Compliance Assessment	After a reasonable gestation period, the team of VISTA InfoSec conducted a pre-assessment of measures implemented and policies, processes and procedures rolled out to fix the gap against the SOC2 Compliance requirements.
	SOC2 Type II Compliance Audit	VISTA InfoSec conducted a comprehensive SOC2 Type II compliance audit. This was to verify and confirm whether all the relevant policies, procedures, and processes recommended were in place to meet the SOC2 requirements.
	Documentation & Reporting	Once all controls were confirmed to be in place, VISTA InfoSec's US-based CPA Auditor documented and drafted a detailed report confirming 3Di Inc's adherence to the SOC2 requirements. A detailed assessment report was produced and an attestation confirming 3Di's commitment to SOC2 Compliance was provided.



CONTROLS EVALUATED

All the relevant aspects of Control Environment, Risk Assessment Process, Information and Communication, and Monitoring at 3Di were evaluated against all the 5 TSC including the Security, Availability, Privacy, Confidentiality, and Process Integrity. In places where there were gaps identified in terms of not having controls in place, the shortfalls were discussed with the 3Di management team. Accordingly, the issues were addressed by developing relevant strategies and implementing necessary measures of internal controls. Tests were performed to validate and verify the operational effectiveness of the controls listed below. The control evaluated at 3Di against Security, Availability, Privacy, Confidentiality, and Process Integrity included –

SR. NO.	CONTROLS EVALUATED
1.	Organization and Management □ Performance Management
2.	Information & Communications □ Information System □ Workstation □ Email Security □ Patch Management □ Antivirus □ Perimeter Defense Firewall □ VPN Access □ Password Controls
3.	Risk management & Risk Mitigation □ Design and implementation of controls

SR. NO.	CONTROLS EVALUATED
4.	Incident Management
5.	Access controls □ Logical access and Application access
6.	Physical and Environmental Security □ Server Room Access □ Confidential, Restricted / Privileged, Internal, Public Access Controls □ Data Restoration & Backups
7.	Change Management
8.	Application Development
9.	Business continuity plan (BCP)
10.	Disaster Recovery Plan & Management
11.	Monitoring Internal Controls □ Vulnerability Scanning and Monitoring □ Availability Monitoring
12.	Subsurface Organization

CHALLENGES FACED

One of the major challenges faced during the SOC2 Audit Preparation was for 3Di to have in place all the documentation evidence of the past year. Since this was 3Di Inc's first SOC2 Audit, gathering evidence was a huge challenge. However, with all the department heads and management stepping in the process, 3Di Inc managed to submit evidence as required for validation and audit.

The on-site assessment was another major challenge due to the COVID-19 scenario. But with the proactive team of 3Di, the audits were successfully performed remotely through online video calls.

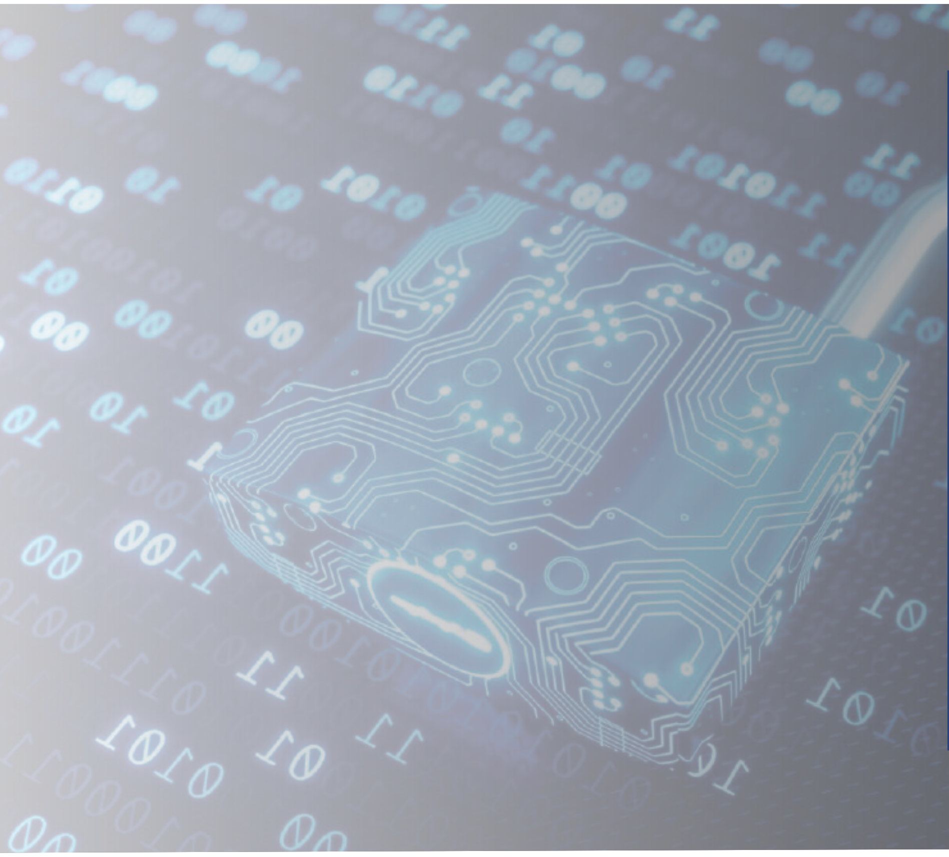
SOC2 Audit is a long-driven process that requires constant engagement from both the auditor and the company's side. This is often a huge challenge especially when the process spans over 6-8 months. Moreover, when the audits and assessments are performed remotely it is difficult to maintain the continuity and involvement required to get measures in place. However, the team of 3Di Inc was proactive in the process and maintained constant communication with the team of VISTA InfoSec. While the team of VISTA InfoSec shared a weekly track record of the task and status of the audit to ensure efficiency and continuity in the audit process.

Establishing new policies and procedures can be challenging but the team 3Di Inc together with the team of VISTA InfoSec drafted relevant policies and p¬rocedures to meet the SOC2 requirements. Compliance expert of VISTA InfoSec ensured end-to-end hand-holding in the process of drafting and implementing new polices procedures and processes.

Adhering to the requirements of SOC2 required implementation of relevant technology controls. Experienced Infrastructure Advisors of VISTA InfoSec provided the necessary guidance to the team of 3Di Inc on those lines. While the 3Di management was forthcoming in the decision making and invested in the required technology to ensure compliance.

SOC2
AUDIT OUTCOME

VISTA InfoSec successfully planned, strategized, and performed the SOC 2 audit for 3Di Inc, and helped the organization meet the AICPA's SOC2 requirements in alignment with their client requirements and objectives. With constant guidance and end-to-end support from the experienced compliance team through the SOC2 Audit, 3Di Inc implemented the industry best practices to meet the compliance requirements. Successfully completing the SOC2 audit, 3Di demonstrated its commitment and proactive attitude towards building a comprehensive information security program. The cyber security program established is related to technology trends that may impact the products and services offered to user entities. This includes high regard for the value of controls and the emphasis given to the controls that are reflected in the company's policies, procedures, methods, and organizational structure.



VISTA INFOSEC SOC2 AUDIT READINESS SOLUTION

SOC 2 audit report enables 3Di to demonstrate to their clients and other stakeholders that they have implemented relevant and appropriate controls concerning the AICPA 5 TSP which includes Security, Availability, Processing Integrity, Confidentiality, and Privacy. VISTA InfoSec's SOC2 Audit Readiness Solution included offering 3Di Inc. an end-to-end compliance service that ensured they received complete guidance handholding through the compliance process. Highly experienced and qualified compliance and audit team worked in collaboration with the 3Di team to build a road map for the organizations to implement industry best practices and achieve their compliance goals.

WHY IS VISTA INFOSEC YOUR BEST AUDITOR & CONSULTANT?

US Based – Our attestation is provided by our office in the US to ensure maximum accountability and market acceptability of our reports.

Trusted Independent Auditors – Our auditors are a separate team based in the US (with good standing with the AICPA) with no relation with our Advisory team. Additionally, our Audit team has licensed CPA accreditation. The audit team is also supported by personnel having other relevant certifications such as CISA / CISSP, etc. with at least 12-15 years experience.

Industry Expertise – With more than 100 assignments on SOC2, you have the assurance that you will get the best industry experts.

Years of Experience – Your organization will benefit from our decade-long years of Industry experience and knowledge.

End - to - end support – Our team will hand-hold you at every stage of the Compliance process.

Robust security & risk management solution – We will provide you with a comprehensive solution, designed to meet your requirements.

WHY IS VISTA INFOSEC YOUR BEST AUDITOR & CONSULTANT?

Reports detailing the analysis finding – We will provide you with documents detailing the findings of the analysis and provide relevant recommendations for the same.

Bridge letter – As a part of our SOC2 Attestation services, we provide a bridge letter that details the internal control environment of your organization during the “gap period”, for your clients.

Training videos and materials – We will provide you with valuable training videos and materials for the ongoing training of your personnel.