GOVS

Auditing Services

Audit Plan Proposal

A3N Technology

October 15, 2016

October 15, 2016

GOVS

To the A3N Audit Committee

Dear Committee Members,

We appreciate the opportunity to discuss the A3N's business issues and your expectations of GOVS Professional Services as your independent auditors. We are pleased to present our audit plan, which includes an analysis of key risks, audit strategy and reporting timetable.

As A3N is a government contractor we understand the critical significance of securing this contracted data to maintain these government relationships. We recognize the importance of your Acceptable Memory Drive Usage Policy in driving appropriate employee awareness, behavior, and compliance to mitigate potential security risks.

Through an initial review of this policy and discussions with A3N managment, we have identified the primary risks that this policy should be mitigating to include:

- Overall policy awareness and employee compliance is insufficient
- The inappropriate safeguarding of and access to government contracted data.
- The unsuitable disposal and destruction of "Red Labeled" drives.
- The failure to report policy violations such as misuse of or inappropriate actions that affect A3N or client data.

Further discussion of our plan with you ensures our GOVS Professional Services engagement team members understand your concerns and that we agree on mutual needs and expectations to provide the highest level of service quality. Our approach is responsive to the many changes affecting A3N goals and objectives. If you have any questions regarding this plan please contact engagement partner, at 555-555-5555.

Professionally,

GOVS Auditing Services

Objectives

Our audit plan goal is to perform a comprehensive evaluation of A3N's Acceptable Media Drive Usage Policy (AMDUP). The scope is to evaluate and measure the sufficiency of A3N's safeguarding of sensitive government contracted data. This audit will also identify varying risks and gaps to determine the effectiveness of A3N employee and vendor AMDUP compliance. The intended result of the audit is to provide potential findings, and recommendations to enhance the AMDUP in alignment with A3N strategic goals and objectives.

Audit Timetable

Your GOVS team works on the audit engagement to provide A3N with timely and responsive service. We envision our audit process to encompass four weeks.

Audit Fieldwork (November 2016)

- Management Interview for Acceptable Use of AMDUP
- Management Interview for Disposal and Deconstruction of AMDUP
- Management Interview for Incident Management of AMDUP

Audit Reporting (November 2016)

- Acceptable Use of AMDUP
- Disposal and Deconstruction of AMDUP
- Incident Management of AMDUP

Final Audit Report and Summary (December 2016)

- Executive Summary
- Final Audit Opinion
- Findings & Recommendations

Terms of Engagement

Our engagement letter sets out the terms of our appointment as auditors of A3N.

The engagement letter covers the following

- Scope of the audit
- Our responsibilities and limitations (engagement letter)
- Management's responsibilities

Audit Strategy

Our audit strategy is only successful with an encompassing understanding of your strategies and objectives. Engaging in detailed discussions with management, GOVS develops a deep understanding A3N organizational objectives and risks. We then focus our efforts towards these risks and its potential impact on company integrity and financial loss.

Once business objectives and risks are identified, we concentrate on the key controls in place to manage those risks. We test those management controls and determine the level of effectiveness and compliance amongst employees.

Findings will be delivered at the completion of the evaluation and will be based on the outcomes of the audit. These results will identify any existing AMDUP risk exposures and gaps in compliance that are not aligned with A3N business goals as defined by governing leadership. Additionally, any corresponding audit recommendations will be appropriately aligned to the A3N risk appetite and remain within A3N risk tolerance.

Audit Plan (Risk Analysis)

Our assessment and identification of risk is performed throughout the audit process in coordination with A3N management.

- Through pre-planning measures, we have listed the AMDUP policy goals, controls and evidence as provide by A3N.
- Our fieldwork observations will focus on listed policy goals, controls and evidence to identify risks that potentially result in unsecure data and non-compliance.
- See Appendix I

Conclusions

GOVS is looking forward to providing its full auditing services to assist A3N with its continued dedication to mitigating security risks and enhancing employee awareness, training and compliance.

Engagement Team

Name	Title
Galarza, Andres	CEO
Olubajo, Alex	Audit Account Director
Van Cleave, Nathan	Audit Engagement Lead
Sardaro, Andrew	Audit Engagement Director

Appendix I

Policy Goals	Controls	Risk	Evidence	Actions
Acceptable Use	A3N employees may only use INFOSEC approved and encrypted RMDs	▪ Policy awareness and employee compliance is insufficient. ▪ Unauthorized person obtaining a red labeled media drive. ▪ Employee using non-red labeled media drive ▪ Sensitive data can be copied to a non-red labeled media drive. ▪ Process and/or technology to detect unapproved and unencrypted media drives is insufficient.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Acceptable Use	A3N approved RMDs may not be connected to or used in Non-A3N computers	▪ Policy awareness and employee compliance is insufficient. ▪ Red labeled media drive is used on an unapproved device. ▪ An unapproved device is brought into classified A3N areas. ▪ Process and/or technology to prevent red labeled media drive use on non-A3N device.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Acceptable Use	Sensitive information should be stored on RMDs only when required in the performance of your assigned duties	▪ Policy awareness and employee compliance is insufficient ▪ Employee roles are not appropriately defined and incorrect security clearance allows access to sensitive information.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Acceptable Use	Sensitive information should be stored on RMDs only when providing required information from other state or federal agencies	▪ Policy awareness and employee compliance is insufficient ▪ An unauthorized state or federal employee requesting sensitive information. ▪ Transfer and acceptance of red labeled drive is not properly logged and approved. ▪ Sensitive information stored on red labeled drive is not properly validated prior to transfer.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Acceptable Use	Sensitive information stored on RMDs must be encrypted in accordance with the A3N/DoD encryption policies	▪ Policy awareness and employee compliance is insufficient ▪ Incorrect encryption standard is used to secure the red labeled drives. ▪ Red labeled drives are not appropriately and routinely inspected for latest security patches and updates.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Disposal and Destruction	Red coded removable RMDs that have reached EOL or have become damaged must be relinquished to INFOSEC for	▪ Policy awareness and employee compliance is insufficient ▪ Information stored on red labeled drives are not sufficiently destroyed. ▪ Red labeled drives are not appropriately cataloged and tracked to end of life.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD

	proper decommission, disposal and destruction			
Disposal and Destruction	The INFOSEC team will abide by DoD Data wiping standards	▪ Policy awareness and employee compliance is insufficient ▪ Information stored on red labeled drives are not sufficiently wiped using most current DoD standard. ▪ Unauthorized person performing red labeled drive data wiping procedure.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Incident Management	In the event that a red coded RMD has been lost or suspected to be lost, it is the responsibility of the employee to notify his or her immediate manager and INFOSEC	▪ Policy awareness and employee compliance is insufficient ▪ Employee is not aware of the appropriate process to report an incident. ▪ Employee is non-compliant with incident reporting process. ▪ Incident management system or process is inadequate and/or ineffective.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD
Incident Management	Any misuse or irresponsible actions that affect A3N or client data must be reported as a security incident to the INFOSEC department	▪ Policy awareness and employee compliance is insufficient ▪ Misuse or irresponsible actions are not clearly defined and appropriately communicated. ▪ Employee is not aware of the appropriate process to report an incident. ▪ Employee is non-compliant with incident reporting process. ▪ Incident management system or process is inadequate and/or ineffective.	▪ Policy Training class and video ▪ INFOSEC team posters	TBD