VENDOR MANAGEMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: 01/01/2021
Updated:

NextGen CGI, LLC Vendor Management Policy							
Effective Date:		01/01/2021		**Document Owner:**		NextGen CGI, LLC	
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Purpose

This policy and supporting procedures are designed to provide NextGen CGI, LLC with a documented and formalized Vendor Management policy that is always to be adhered to and utilized throughout the organization. Compliance with the stated policy and supporting procedures helps ensure the safety and security of NextGen CGI system resources.

Today's increased use of outsourcing to various third-parties has created a true need for monitoring such entities for baseline compliance measures with regards to NextGen CGI security standards. Specifically, all outsourced processes, procedures, and practices relevant to NextGen CGI are to be monitored on a regular basis, which includes undertaking various measures on all third-parties and providing critical services. This policy strives to ensure the overall confidentiality, integrity, and availability (CIA) of the organization's network.

2. Scope

This policy and supporting procedures encompass all system resources that are owned, operated, maintained, and controlled by NextGen CGI and all other system resources, both internally and externally, that interact with these systems.

- Internal Systems – resources owned, operated, maintained, and controlled by NextGen CGI and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External Systems – resources owned operated, maintained, and controlled by any entity other than NextGen CGI, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the internal system resources.

- When referencing the term “users”, this includes any individual that has been granted access rights by NextGen CGI to various system resources and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

- For the purposes of this policy, vendor management is defined as the following: The policies, procedures, and related processes undertaken for managing activities conducted through third-party relationships and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the organization.

- Additionally, the terms “vendors”, “third-party”, “third parties”, “outsourcers”, “organizations”, and the variant thereof are defined as entities providing outsourcing services to NextGen CGI.

3. Element of Risk

When using the services of various third-party outsourcing entities, a certain element of risk arises as responsibilities for critical initiatives are now in the hands of another organization. It’s important to understand these risks, what they are, and how NextGen CGI can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, legal issues, and public opinion misconceptions, ultimately damaging the organization. As such, the following risks are to be

thoroughly understood and assessed regarding business and contractual relationships entered into with third parties:

- Compliance Risk: These are risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of internal operational, business specific, and information security policies, procedures, and processes. A common example would be for an outsourced organization to violate compliance regarding the safety and security of Personally Identifiable Information (PII), such as having exposed such information to unauthorized parties, not having policies and procedures in place protecting PII, or not undergoing required annual compliance audits. Regulatory compliance is a large and critically important component for vendor management, requiring constant monitoring and oversight of third-parties for ultimately ensuring the safety and security of services being provided to NextGen CGI, LLC by such entities. Common compliance initiatives for which third-parties are to adhere to include numerous laws, legislative mandates, and industry specific requirements, including, but not limited to, the following: Sarbanes-Oxley, HIPAA, HITECH, SOC1 SSAE 16, SOC2, SOC3, GLBA, PCI DSS, and many others.

- Reputational Risk: These are risks arising from negative public perception and opinion of a third-party outsourcing entity for almost any imaginable reason, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information (i.e. Personally Identifiable Information), investigations from regulators into questionable business practices, etc. It's important to note that in today's world of transparency and close media scrutiny, any perceived negative public opinion on a third party being utilized by NextGen CGI ultimately affects the reputation of the organization.

- Strategic Risk: These are risks arising from third-parties failing to implement business initiatives that align with the overall goals and ideas of NextGen CGI, such as not offering services that provide an acceptable return on investment, both short and long term. Ultimately, when the long-term strategic vision of both NextGen CGI and the applicable third-party outsourcing entities do not align, relevant risks begin to surface which can significantly impact the business relationship.

- Operational Risk: These are risks arising from a failed system of operational internal controls relating to personal and the relevant policies, procedures, processes, and practices. This becomes a large issue since many organizations integrate their daily operational activities with outsourcing providers, thus a "breakdown" on the vendor side seriously impacts the organization, ultimately affecting productivity, workflow efficiency, and many other issues.

- Transaction Risk: These are risks arising from a third-party failing to deliver as promised, such as product delivery, operational efficiency, or unauthorized transactions and theft of information due to a weak system of operational and information security internal controls. An important component of mitigating such risk is having comprehensive, well-documented operational and information security policies, procedures, processes, and practices in place for guiding such third-parties daily.

- Credit Risk: These are risks arising from the financial condition of a third-party. Not being able to meet routine expenses can result in large risks for NextGen CGI as the organization is heavily dependent on various outsourcing entities for their services.

- Country Risk: These are risks arising from political, economic, and social landscape within a foreign country that can impact the services being provided by the third party, ultimately affecting operations for NextGen CGI. Managing such risks can be extremely challenging and complex, especially when one considers the diverse political landscape in various regions around the globe. Legal issues also can pose significant country risk, as laws and regulations differ greatly from region to region.

- Information Technology Risk: These are risks arising from any number of information technology and information security issues, such as inadequate IT resources (hardware and software) and lack of manpower. Additionally, risks can arise from abuse, misuse of information technology resources, while data breaches and security compromises can occur because of improperly designed networks, little to no information security policies, procedures, etc. Other serious information technology risks can include not correctly provisioning and hardening critical system resources, failing to implement “defense in depth”, using insecure security protocols, etc.

4. Benefits of Vendor Management

True vendor management is much more than just meeting regulatory compliance purposes. Specifically, vendor management initiatives for NextGen CGI should seek to help reduce costs, improve operations, strengthen security, while also improving relationships with all applicable third-party outsourcing entities. Vendors for NextGen CGI are looked upon as instrumental organizations providing critical services, and as such, are to be taken seriously in every manner, which means assessing all risk areas while also striving for the following:

- Reduction of Costs
- Improvement of Operations

- Strengthening of Security
- Improvement of Relations

5. Vendor Assessment Analysis

True vendor management entails assessing the current list of third-party outsourcing organizations while also putting in place initiatives for evaluating new vendors – and finally – implementing continuous monitoring practices. Specifically, NextGen CGI current vendor assessment analysis is to comprehensively assess each organization in regards to the aforementioned risk areas, which include, but are not limited to, the following:

- Identify all third-party outsourcing organizations
- Obtain all contractual documents and other supporting documentation for helping assess current third-party services. This may also include legal correspondence, audited financial statements, various expenses and revenues directly tied to such providers, etc.
- Obtain all regulatory compliance reports. This may include assessment such as SOC2, PCI DSS, FISMA, ISO, and many other compliance mandates and reports.
- Identify, review, and assess any consumer complaints, unethical business practices, etc.
- Identify, review, and assess any data security breaches, cyber security attacks, etc.
- Identify if any third-parties are storing, processing, and/or transmitting any sensitive and confidential information, commonly known as Personally Identifiable Information (PII), payment card information (Cardholder Data), or Patient Health Information (PHI).
- Identify, review, and assess all operational, business specific, and information security policies, procedures, and practices relevant to services being provided to NextGen CGI, particularly documentation pertaining to incident response, security awareness, business continuity, and disaster recovery (BCDRP).
- Identify, review, and assess all information technology platforms (hardware and software) and IT personnel relevant to services being provided to NextGen CGI, particularly what systems are being used, and the skill sets and experience of these individuals.
- All other measures deemed necessary by NextGen CGI.

6. Due Diligence in Vendor Selection

The selection process for new vendors is to consist of exhaustive measures for ensuring relevant risk areas have been thoroughly assessed by NextGen CGI, which is to include, but not limited to, the following measures:

- Review of all applicable financial documentation, such as financial statements
- Review of all regulatory compliance and operational audits and assessments

- Experience and overall business knowledge
- Operational capacity and scalability
- Use of other third-parties by the actual vendor themselves (i.e. sub-contractors)
- Reputation within the industry and from the general public
- Inquiry into any past, present, or expected legal issues, constraints, or concerns
- Experience and business aptitude, strength, and knowledge of senior management and all other relevant personnel
- Alignment of vision, strategies, and overall goals with each organization
- Assessment of operational, business specific, and information security policies, procedures, and practices, particularly documentation pertaining to incident response, security awareness, business continuity, and disaster recover planning (BCDRP)
- Assessment of organizational-wide system of internal controls
- Underwriting criteria
- Insurance coverage

7. Contractual Documentation

Once vendors have been selected for providing critical outsourcing services to NextGen CGI, comprehensive procedures are to be undertaken regarding all contractual documentation – specifically – the following:

- A formalized and written contract has been produced, one that dutifully identifies roles, responsibilities, obligations, and expectations from all relevant parties.
- The contract has been approved by senior management throughout NextGen CGI, which includes all major stakeholders, such as board of directors, audit committee personnel, equity owners, officers, and all other relevant personnel. This also requires addressing the following issues regarding stakeholders:
    - Are they aware of the risks when entering contractual agreements with such vendors?
    - Are there any financial relationships or associations with such vendors?
    - Were all due diligence findings and documentation presented clearly and in a timely manner to such individuals?
- Comprehensive and appropriate review undertaken by legal-council, with all issues, constraints, and concerns addressed as necessary.
- Defined operational, performance, and other necessary baseline standards for services to be performed, along with reporting metrics on such issues, such as daily, weekly, and monthly reports.
- Fees paid for stated services along with other financial considerations.
- Regulatory compliance audits and mandates, such as annual financial statement audits, annual operational and security assessments (I.e. PCI DSS).

- Information security protection measures regarding the safety and security of sensitive and confidential information, such as PII, and any other variant thereof.
- Numerous other legal issues, including, but not limited to, the following: resolution measures, indemnification, continuation of services, default, intellectual property, etc.

8. Management Oversight and Continuous Monitoring

Upon successfully approving all business agreements with vendors, management of NextGen CGI is to continuously monitor the various aspects of the outsourcing entity as it relates to compliance risk, reputation risk, strategic risk, operational risk, transaction risk, credit risk, country risk, and information technology risk. A large part of continuous monitoring involves significant input from senior management – personnel directly responsible for the long-term strategic vision of NextGen CGI - thus policies, procedures, and practices are to be reviewed and approved by such individuals for ensuring a strong working relationship with all vendors providing outsourcing services. One of the largest areas for risk involves information security – specifically – ensuring that all vendors have well-documented, formalized policies and procedures in place along with adhering to IT best practices. The subsequent checklists include comprehensive due diligence and continuous monitoring practices to be undertaken by NextGen CGI when working with new, current, or prospective vendors seeking to provide outsourcing services.

9. Breach Notification

The vendor is responsible for notifying all persons whose sensitive data may have been compromised as a result of the breach as required by law.

10. Related Standards, Policies, and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

11. Vendor Management Checklists

Procedure	Responsible Party	General Notes / Comments
Identify all third-party outsourcing organizations.		
Obtain all contractual documents and other supporting documentation for helping assess current third-party services.		

Obtain all regulatory compliance reports. This may include assessments such as SOC1, SOC2, PCI DSS, FISMA, ISO, and many other compliance mandates and reports.		
Identify, review, and assess any consumer complaints, unethical business practices, etc.		
Identify and document data transmitted to or stored by the third-party that belongs to the organization.		
Monitor third-party activity and ensure breaches or security incidents are communicated to the organization.		