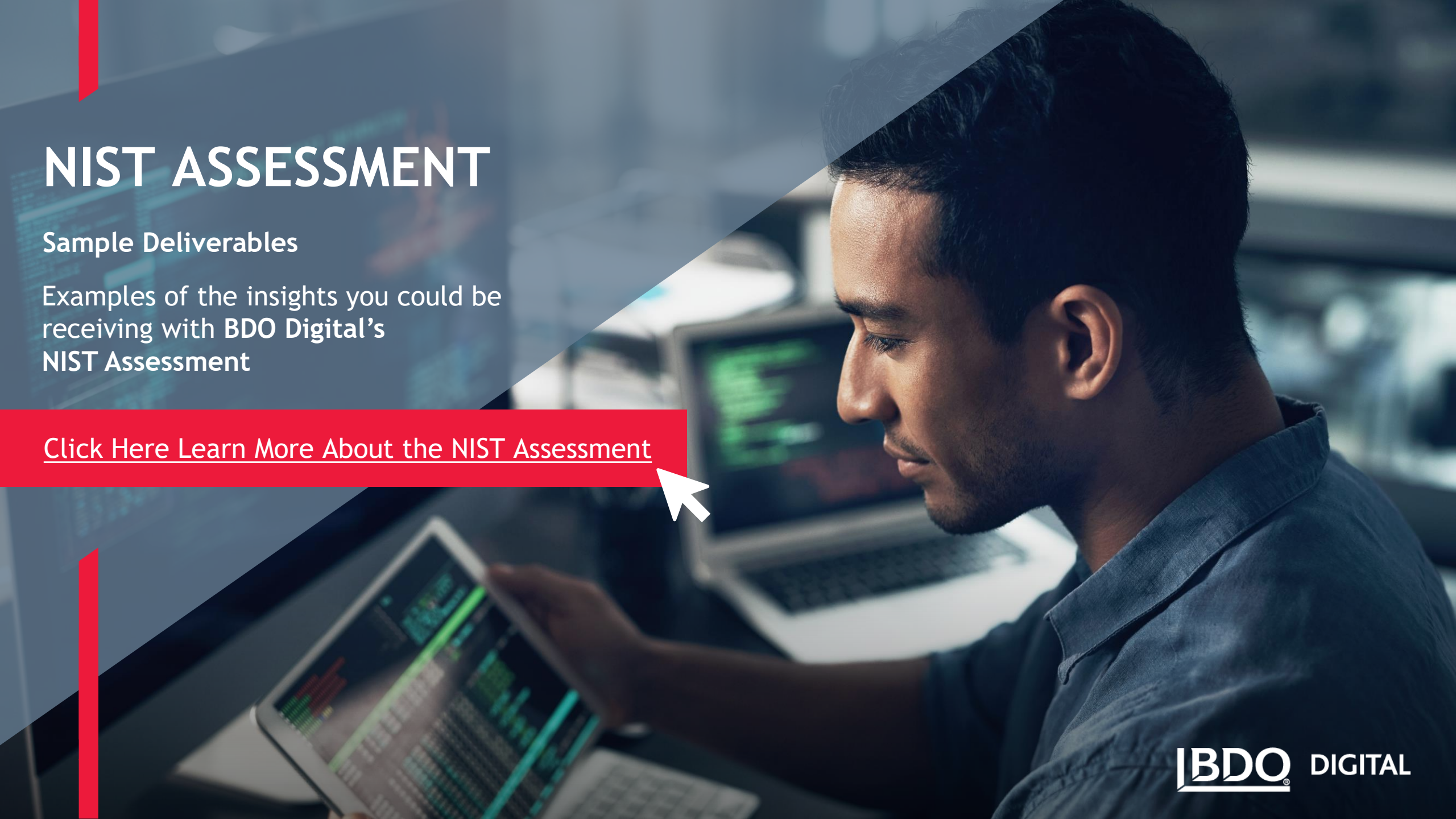
NIST ASSESSMENT

Sample Deliverables

Examples of the insights you could be receiving with **BDO Digital's NIST Assessment**

Click Here Learn More About the NIST Assessment



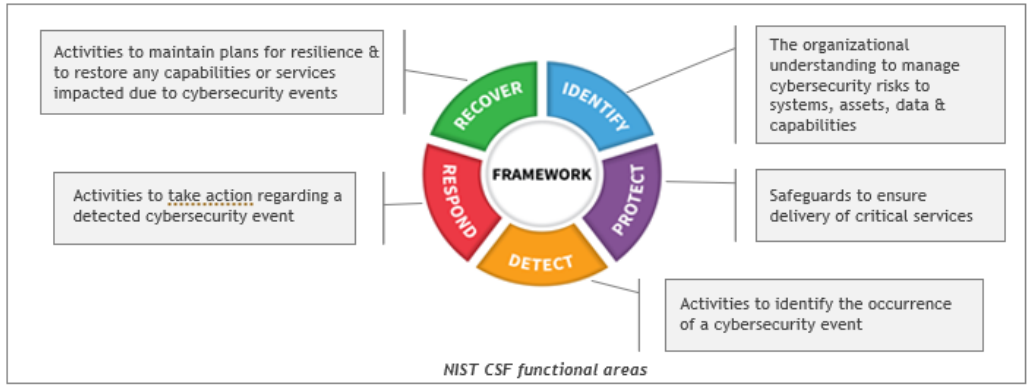
BDO DIGITAL

Overview

Project Overview

Project Background and Framework Overview

- BDO was engaged by [Client Name] to assess the current state of the company's cybersecurity maturity and posture, as well as to propose a future-state roadmap with prioritized improvement initiatives geared towards minimizing risks & their impacts.
- Evaluation was performed against the NIST Cybersecurity Framework (CSF) while using an evaluation system similar to the Capability Maturity Model Integration's (CMMI) approach to establish ratings. The NIST CSF consists of 108 security controls across five critical security functions: identify, protect, detect, respond & recover.



NIST CSF functional areas

Project scope, approach and objectives

1. Project initiation and planning

- Validate objectives, scope, and expectations
- Schedule domain interviews
- Request and review relevant documentation

2. Current state capability maturity assessment

- Conduct a series of interviews and follow-up discussions to understand current-state maturity
- Evaluate current state against NIST Cybersecurity Framework (CSF)
- Review policy documents as well as evidence relevant to each NIST CSF subcategories.

3. Sector relevant benchmark and leading practice recommendations

- Evaluate the maturity of NIST CSF categories based on data gathered.
- Develop observation themes and highlight key risks associated to gaps and framework categories.
- Provide benchmarking insights to understand how the current IS program compares with similar companies in the [Client Industry] industries.

4. Reporting, socialization, and wrap up

- Develop report of observations and recommendations for [Client Name] management consideration.
- Document key observations and high-level recommendations
- Develop a proposed future-state roadmap with prioritized improvement initiatives.

4

DRAFT

BDO DIGITAL

BDO DIGITAL

Maturity & Risk Summary

NIST CSF Maturity and Risk - Summary

NIST CSF function	Category	Risk Level	Maturity rating	Industry Average*	Proposed Goal
Identify	Asset Management (ID.AM)	Medium	Managed	Managed	Managed
	Business Environment (ID.BE)	Medium	Initial	Managed	Managed
	Governance (ID.GV)	Medium	Initial	Managed	Managed
	Risk assessment (ID.RA)	High	Managed	Managed	Defined
	Risk Management Strategy (ID.RM)	High	Initial	Managed	Managed
	Supply Chain Risk Management (ID.SC)	High	Initial	Initial	Managed
Protect	Access Control (PR.AC)	High	Managed	Defined	Defined
	Awareness & Training (PR.AT)	High	Initial	Defined	Defined
	Data Security (PR.DS)	High	Managed	Managed	Defined
	Information Protection Processes & procedures (PR.IP)	High	Initial	Managed	Managed
	Maintenance (PR.MA)	Medium	Initial	Managed	Managed
	Protective Technology (PR.PT)	High	Initial	Managed	Managed
Detect	Anomalies and Events (DE.AE)	Medium	Defined	Managed	Defined
	Security Continuous Monitoring (DE.CM)	Medium	Defined	Defined	Defined
	Detection processes (DE.DP)	Medium	Defined	Managed	Defined
Respond	Response Planning (RS.RP)	High	Defined	Managed	Defined
	Communications (RS.CO)	Medium	Managed	Managed	Managed
	Analysis (RS.AN)	Medium	Defined	Managed	Defined
	Mitigation (RS.MI)	High	Managed	Managed	Defined
	Improvements (RS.IM)	Low	Initial	Initial	Managed
Recover	Recovery Planning (RC.RP)	High	Managed	Defined	Defined
	Improvements (RC.IM)	Low	Initial	Managed	Managed
	Communications (RC.CO)	Low	Initial	Initial	Managed

*Industry average maturity derived from assessments of [Client's Industry] companies and similar organizations across North America.

- This table compares [Client Name]' current levels of maturity for the 23 NIST cybersecurity categories, with the industry average as well as the proposed future state for [Client Name].
- It is important to note that the industry averages are inherently less mature than some other industries, and therefore future maturity goals should aim to exceed industry averages for certain categories.

Maturity Level Description	
Initial	Basic, undocumented and changing capability; limited technology and tools
Managed	Partial capability with some technology and tools; some local processes are repeatable, but may not be good practice or maintained
Defined	Defined capability with significant technology and tools; many repeatable processes; organizational guidance is in place
Quantitatively Managed	Maturity capability with advanced technology and tools; consistent processes exist; some governance exists
Optimized	Advanced capability using leading-edge technology and tools; Enterprise processes with formal policy exception process; effective governance throughout

7

DRAFT

BDO DIGITAL

BDO DIGITAL

Observations Summary

Key current state areas of strength

[Service Provider Name] SOC and NOC as a service

- [Client Name] has contracted [Service Provider Name] to handle its Security Operations and Network Operations Center as a managed service.
- [Service Provider Name] ensures that [Client Name] has a dedicated and trained team to continuously monitor its information systems and logical environment for events and incidents.
- [Service Provider Name] provides monthly vulnerability scanning reports and NOC/SOC metrics.

Authentication and Remote Access

- [Client Name] has implemented Duo 2FA for Office apps and remote access.
- Site-to-Site VPN within North America and from France office.
- Password changes are required every 90 days.

Cybersecurity Initiative and Appetite

- ELT Members are aware of the importance of and current lack in cybersecurity.
- [Client Name] has completed a Vulnerability Assessment and Pen Test (VAPT) and is focusing on remediation.
- [Client Name] has imposed stricter reporting metrics on [Service Provider Name].

Key current state areas of gaps

Data Security and Protective Technologies

- Few to no Data Loss Prevention Controls: i.e. USB access, cloud backup services, endpoint device encryption (BitLocker), email DLP, secure file cabinets, etc.
- No Data Classification, Data Retention, or Data Handling processes.
- No software management solution or approved list of applications for endpoint installation.

Identity Access Management

- No least privilege access and least functionality strategy as identities and permissions for new hires are copy/pasted from similar positions.
- Service Accounts credentials and Sysadmin passwords are not securely managed and shared across IT.

Key current state areas of gaps

Security Awareness, Training and Education (SATE)

- [Client Name] does not provide cyber training or role-based trainings (specific to responsibilities) to its employees.
- [Client Name] does not manage a phishing program and campaign.

Risk Management and Risk Awareness

- Lack of Cyber Risk Management team or program that supports business initiatives, develop prioritized projects and allocate budget.
- Most cybersecurity processes are handed to [Service Provider Name], which is not sufficient, as [Client Name] needs to be more proactive in the process.
- Lack of threat modeling, risk tolerance, Business Impact Analysis.
- Lack of cybersecurity policies, procedures and documentation across all cyber processes.

Supply Chain Risk Management

- As one of the critical areas to [Client Name]' business, there are no SCRM initiatives, such as policies, SLA checklists, inventory of vendors and suppliers' information, third-party risk assessments.
- Lack of a templated or streamlined process to assess new vendors/suppliers as part of onboarding and ongoing third-party risk management.
- No Physical security processes for supply chain integrity and availability.

Vulnerability and Patch Management

- Although [Service Provider Name] provides vulnerability reporting, it does not provide any remediation and patch management, which is [Client Name]' responsibility.
- [Client Name] does not have a Vulnerability and Patch Management program or a defined process to manage reported vulnerabilities and to remediate them.

Contingency Planning

- DR plans for [Facility], [Facility] and IS exist but are outdated, not well maintained or tested, and missing sections. Data Centers and Backup strategy do not account for geographical redundancy as they are within proximity.
- [Service Provider Name] has an IR plan, but [Client Name] does not have an internal IRP or Business Continuity Plan to handle incidents, as [Service Provider Name] is not contracted to perform containment, mitigation, eradication and recovery on behalf of [Client Name].

9

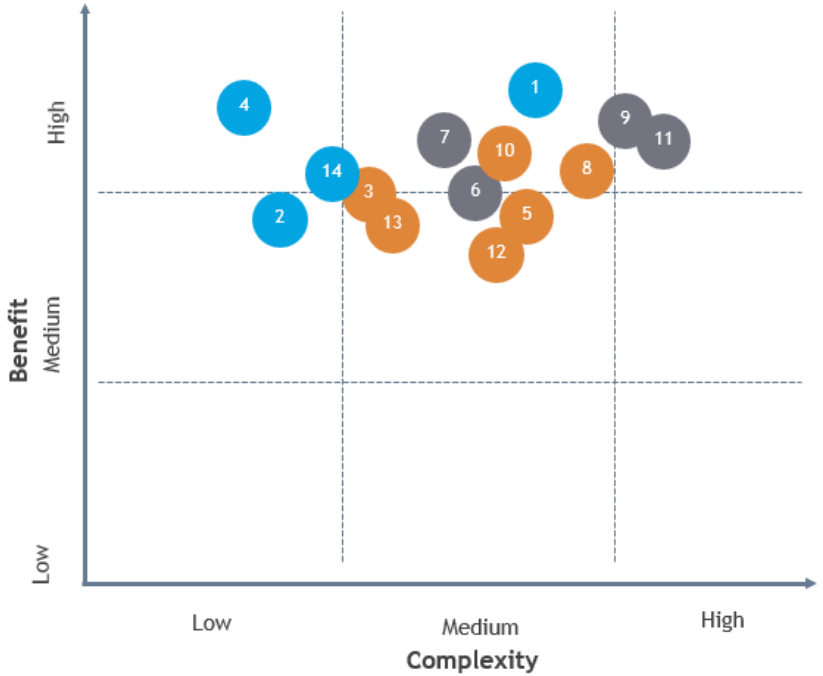
DRAFT

BDO DIGITAL

BDO DIGITAL

Cyber Roadmap

Recommended Cybersecurity Initiatives



ID	Description
	Quick wins, initiative to quickly improve cybersecurity posture
	Improvement of an existing function or capability within [Client Name]' environment today
	Significant improvement to or creation of new functions or capabilities that do not exist today

#	Cyber Initiatives	ID
1	Vulnerability and Patch Management Program	
2	Information Security Policies and Procedures	
3	IT Asset Inventorying and Management	
4	Security Awareness and Training	
5	Incident Response Planning	
6	Risk Management Program	
7	Business Impact Analysis	
8	Access Management	
9	Info Systems Redundancy and Data Backups	
10	Disaster Recovery and Business Continuity	
11	Data Governance Program	
12	Environment Hardening Assessment	
13	Reassess Program Maturity	
14	Cybersecurity Personnel	

- **Complexity:** The level of effort required to pursue the cyber initiative.
- **Benefit:** The level of mitigation towards identified gaps, threats and risks, and improving relevant NIST categories.

11

DRAFT

BDO DIGITAL

BDO DIGITAL

Recommended Plan of Action

#	Cyber Initiatives	Recommended Plan of Action
1	Vulnerability and Patch Management Program	• Gather a complete inventory of IT systems (hardware and software) that provides full endpoint visibility, and that showcases criticality and cost. • Evaluate the scope of current vulnerability scans performed by [Service Provider Name] to ensure that all systems (especially critical ones) are covered by scans. • Develop a formal process to evaluate vulnerability severity and risk ranking, as well as cadence and prioritization for remediation. • Ensure that [Service Provider Name] is scanning vulnerabilities for the same devices (since the Rapid7 agent is running on endpoints) to ensure a continuous flow of reporting and metrics for each month. [Service Provider Name] should accurately track the vulnerabilities that were remediated by [Client Name], to support accurate reporting. • Develop remediation, mitigation and acceptance strategies and processes in order to handle reported vulnerabilities and ensure a continuous process flow. • Execute vulnerability and patch management strategies and processes.
2	Information Security Policies and Procedures	• Develop a company cybersecurity policy that includes: Acceptable Use Policy, Roles and Responsibilities, Risk Management, Data Security (Classification, Retention, Destruction, Encryption, DLP, Backup), IT Asset Management, Cybersecurity Training, Cyber Incident Management, Physical and Environmental Security, Account Management and Access Control, password management and Vulnerability and Patch Management. • Develop cybersecurity procedures that expand on the previously mentioned cybersecurity policies (e.g. Risk Management procedures should include Third-Party and Supply Chain Risk Management). • Create an annual review process to update policies and procedures.
3	Risk Management	• Designate Risk Management roles and identify a Risk Management team. • Develop a Risk Management program and processes for each of the following areas: Information Systems, Third-Party Vendors and Supply Chain. • Identify and document the Threat Landscape for [Client Name], its Risk Profile (inherent and residual risks, as well as Key Risk Indicators to help business leaders track how [Client Name]' risk profile is evolving) as well as its Risk Tolerance (to include accepted risks). • Identify and document key regulatory and compliance requirements based on [Client Name]' industry, as well as the information that it stores (EU GDPR and HIPAA)
4	Incident Response Planning	• Designate Incident Response roles and responsibilities. • Develop Containment, Eradication and Recovery procedures, that rely on [Service Provider Name]'s detection and analysis of incidents to account for a continuous flow for [Service Provider Name]'s process and to handle reported incidents. • Develop post-incident processes to account for lessons learned and improvements. • Test the Incident Response plan annually by performing cyber fire drills, that account for specific scenarios (e.g. phishing, ransomware, etc.). Identify and document lessons learned and key takeaways.
5	Info Systems Redundancy and Data Backups	• Perform a Business Impact Analysis to understand critical processes and to identify critical IT systems in order to inform redundancy and backup strategies with prioritization. • Formalize and document a backup strategy to account for geo-redundancy, and recovery bottlenecks. • Evaluate backup tools/services to match strategy (recommended to use cloud backup services). • Implement and test backup tool/service to ensure recovery objectives and requirements identified in the Business Impact Analysis are met. • Ensure that critical infrastructure is deployed with redundancy strategies to ensure availability of critical services. • Test server failover and network load-balancing and failover capabilities.

BDO DIGITAL

Risk Assessment

Risk Assessment [ID.RA]

Risk Level: High

Initial	Managed	Defined	Quantitatively Managed	Optimized

Category Objectives

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, including asset vulnerabilities, internal and external threats, likelihood and impact of attacks.

Gaps and Observations

- Asset vulnerabilities are identified and reported by [Service Provider Name] (SOC as a service) that scans internally facing environment once a month using Rapid7 InsightVM.
- Asset vulnerabilities are identified and reported by third parties for externally facing systems on a yearly basis.
- BDO completed a Vulnerability Assessment and Penetration Test (VAPT) for [Client Name].
- [Service Provider Name] uses various sources for Cyber Threat Intelligence (CTI) and ingests Indicators of Compromise (IoCs) and malicious actors Tactics, Techniques, and Procedures (TTPs).
- [Client Name] does not have a process in place to identify and document threats (both internal and external) to its organization's information systems.
- [Client Name] does not have a process to determine cyber risk and risk levels using threats, vulnerabilities, likelihoods and impacts.
- [Client Name] does not calculate risk using vulnerabilities but understands that critical vulnerabilities pose a risk and attempts to manage vulnerabilities that have a CVSS score of 9 and above.

Key Risks Identified

- Without risk assessments, the company cannot determine which systems are vulnerable, how likely they are to be compromised and exploited by malicious actors, as well as the impact that the compromise will have on the company from a financial, operational and reputation standpoint.
- Cybersecurity Risk Assessments are designed to give business leaders the data and resources they need to navigate potential risks and identify areas that may have been missed.
- A critical component to managing cyber risks is understanding the different threat vectors relevant to the company, such as Phishing, Supply Chain, Ransomware and IoT attacks, as well as Intellectual Property theft and Insider Threats.
- Unpatched and unidentified security vulnerabilities are one of the leading causes for attackers to compromise information systems and gaining initial unauthorized access, which in turn has a high likelihood to lead to more damaging attacks.

21

DRAFT

BDO DIGITAL

BDO DIGITAL

Deep Dive

Response Planning [RS.RP]

Risk Level: High

Initial	Managed	Defined	Quantitatively Managed	Optimized

Category Objectives

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Gaps and Observations

- [Service Provider Name] is contracted to handle incident response with the assistance of [Client Name] staff.
- [Service Provider Name] employs a runbook that contains a communication plan, escalation plan, and SOPs specific to the execution of response steps for supported event types.
- [Service Provider Name] also has an Incident Response Plan for [Client Name] covering different scenarios such as Malware workflows, DDoS, Phishing, Sensitive Data Disclosure, Third-Party Data Breach, Zero Day Vulnerabilities.
- [Client Name] has no documentation or solid understanding as to how it should assist [Service Provider Name] in the event of an incident or how it should process and handle incident reports internally.
- [Client Name] does not perform any IRP testing.

Key Risks Identified

- Not having an efficient IRP in place poses very high risk, as the organization will not have a process ready to prepare for, to identify, to contain, to eradicate, to recover from and to learn from incidents, which will lead to longer periods of downtime, increased loss of revenue, and potential lawsuits for data theft or discontinuity of services.
- Although [Service Provider Name] provides incident response as a service, it is important that [Client Name] has an Incident Response plan for internal use that accounts for the services that [Service Provider Name] provides, and that integrates [Service Provider Name]'s current IRP. Additionally, it is important to scope into [Client Name]' IRP areas that [Service Provider Name] may not cover.
- Lack of testing an IRP may lead to unexpected behaviors and a lack of plan optimization, which may slow down the response process, which in turn may have adverse effects.

36

DRAFT

BDO DIGITAL

BDO DIGITAL

Recovery

Recovery Planning [RC.RP]

Risk Level: High

Initial	Managed	Defined	Quantitatively Managed	Optimized

Category Objectives

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Gaps and Observations

- [Service Provider Name] offers recovery planning services, but they are out of scope for [Client Name]' current contract. [Service Provider Name] usually leverages clients' Disaster Recovery and Business Continuity plans.
- [Client Name] has DR plans for [Facility] and [Facility] facilities, as well as for its Information Systems. However, these plans are not up to date, not effectively tested and lack in content.
- [Client Name] does not have an IRP that details recovery processes for affected systems.

Key Risks Identified

- Not having a defined, maintained and tested Incident Recovery process will disrupt business continuity and [Client Name]' supply chain if an incident occurs, and lead to extended system downtimes, which will have significant financial, operational and reputational impact on the company.

DRAFT

BDO DIGITAL

BDO DIGITAL

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 65 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 91,000 people working out of more than 1,600 offices across 167 countries and territories.

BDO Digital, LLC, a Delaware limited liability company, is a wholly-owned subsidiary of BDO USA, LLP. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for Each of the BDO Member Firms. For more information on BDO Digital, LLC please visit:

www.bdodigital.com

BDO DIGITAL