North Dakota Information Technology Department

Security Assessment Report

[2024 Penetration Test Summary]

DOCUMENT REVISION HISTORY

VERSION	DATE	CHANGE DESCRIPTION
1.0	08/16/2024	Initial Draft
1.2	09/09/2024	Final Draft

SUBMITTED TO:

James Kary
Systems Auditor
North Dakota State Auditor's Office

(701) 328-2580
jkary@nd.gov

PREPARED BY:

Casey Bourbonnais
Lead Technical Tester
Secure Yeti, LLC

(918) 986-7060
casey.bourbonnais@secureyeti.com

TABLE OF CONTENTS

KEY PARTICIPANTS

NORTH DAKOTA INFORMATION TECHNOLOGY DEPARTMENT

James Kary
Systems Auditor
North Dakota State Auditor's Office
(701) 328-2580 (o)
jkary@nd.gov

Josh Kadrmas
Cyber Risk Analyst Team Lead
North Dakota Information Technology Department
(701) 328-1837 (o)
jkadrmas@nd.gov

Ryan Kramer
Enterprise Infrastructure Architect
North Dakota Information Technology Department
(701) 328-4655 (o)
rkramer@nd.gov

Charlie Tweet
IT Director
Bank of North Dakota
(701) 328-5842 (o)
ctweet@nd.gov

SECURE YETI

Brett Lessley
Project Manager
Secure Yeti
(918) 986-7060 (o)
brett.lessley@secureyeti.com

Casey Bourbonnais
Lead Technical Tester
Secure Yeti
(918) 986-7060 (o)
casey.bourbonnais@secureyeti.com

Joe Aguilar
Technical Tester
Secure Yeti
(918) 986-7060 (o)
joe.aguilar@secureyeti.com

Theresa Warnock
Technical Tester
Secure Yeti
(918) 986-7060 (o)
theresa.warnock@secureyeti.com

Christopher Carlis
Technical Tester
Secure Yeti
(918) 986-7060 (o)
christopher.carlis@secureyeti.com

1. EXECUTIVE SUMMARY

1.1. OVERVIEW

Under the direction of James Kary from the North Dakota State Auditor's Office on behalf of the North Dakota Information Technology Department (NDIT), Secure Yeti conducted a security assessment from June 17th, 2024, through July 26th, 2024. This assessment included the following activities:

- External Penetration Test
- Internal Penetration Test
- Internal Vulnerability Scanning
- On-Site Social Engineering

The objective of this assessment was to evaluate the overall security posture of the target network by subjecting network systems and resources to methods and techniques commonly used by criminals and malicious actors. This process enabled the proactive remediation of identified weaknesses and vulnerabilities before they could be exploited to gain unauthorized access to critical systems or sensitive data.

In collaboration with key IT and Information Security personnel, the assessment team discussed NDIT's current security posture, recent threat activity, and other scenarios the NDIT team felt could pose a potential risk to the State's network. From those discussions, compromised users were determined to be the threat actor of primary concern with a primary objective being to identify internal attack vectors that could be conducted through those user accounts to further compromise the NDIT system in its entirety, or pivot to/between different state offices. As a secondary objective, NDIT desired to test endpoint and network monitoring capabilities. Participating agencies included the North Dakota Office of Management and Budget (OMB), North Dakota Department of Transportation (DOT), North Dakota Department of Health & Human Services (DHHS), and the Bank of North Dakota (BND).

It is important to note that this report represents a "snapshot" of each environment at the point-in-time that it was assessed. The security posture observed during the test window may have improved, deteriorated, or remained the same since this completion of this assessment.

1.2. OVERALL FINDINGS

Over the course of testing, the assessment team noted five critical, ten high, five medium, and eight low findings. One informational finding was also observed.

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	10	5	8	1

1.3. CONCLUSION

A key goal of this engagement was to work in conjunction with the NDIT Security team to analyze their current ability to detect and identify malicious activity within their environment. To accomplish this goal, the assessment team maintained constant communication with NDIT's Security Operation Center (SOC) during the testing window. This collaboration allowed the SOC to effectively identify blind spots in current monitoring capabilities as the assessment team conducted the attacks. Using the MITRE ATT&CK framework as a guide, the teams worked together to identify and develop mitigation strategies for risks covering nearly all MITRE categories.

Secure Yeti understands the priority that NDIT has placed on cybersecurity and sincerely appreciates the opportunity to have worked with your organization. Secure Yeti would like to thank Josh Kadrmas, Ryan Kramer, and Charlie Tweet for their support in coordinating access and resources for this assessment. Their assistance was crucial to the success of this engagement. Should you have any questions regarding these findings or the content of this report, please feel free to contact us at any time.

2. ASSESSMENT METHODOLOGY

2.1. EXPLANATION OF TESTING ACTIVITIES

IN SCOPE	ACTIVITY / DESCRIPTION
YES	External Penetration Testing: External penetration testing employs blended threat scenarios to assess the effectiveness of an organization's perimeter defense in preventing unauthorized access into internal resources. The primary objective of this assessment is to perform simulated attacks, using tactics and techniques identical to those used by current day threat adversaries. The assessment will include Open-Source Intelligence (OSINT) gathering, along with a variety of open source, commercial, and custom-built tools to conduct discovery scans and identify potential targets or vulnerabilities for additional testing. External testing specifically targets publicly accessible resources such as, but not limited to, firewalls, routers, VPN/remote access appliances, web applications, email servers, and DNS servers. This test gauges the effectiveness of the organization's perimeter security comprehensively.
YES	Internal Penetration Testing: Internal penetration tests provide organizations the opportunity to assess their internal defenses and procedures when faced with an attacker who has managed to obtain initial access to the internal network. Internal penetration testing is conducted from two separate perspectives: Testing during the first phase will be performed as an unauthenticated or anonymous guest who has managed to obtain physical access to the internal network. This approach simulates attack vectors that would be taken by a hacker that has managed to gain access to the internal network via alternate methods. A secondary round of testing will be performed using credentials and access given to a typical employee. This approach simulates actions and threats that could be performed by a malicious insider or a compromised employee. This phase commonly identifies privilege escalation vulnerabilities or excessive permissions. Internal penetration testing targets, and attempts to exploit, any device accessible on the internal network. The ability to maintain persistent access, elevate privileges, and move laterally are all tested in this activity.
YES	Internal Vulnerability Scanning: A controlled, authenticated vulnerability scan within an organization's internal network to discover assets across all available VLANs and network segments. The process involves identifying each asset within the network and subsequently probing them to determine service and/or software versions running on the identified host. This comprehensive approach aims to identify vulnerabilities present on the identified asset. The results provide insights into potential vulnerabilities within their environment so they can be proactively addressed to mitigate associated risks.

IN SCOPE	ACTIVITY / DESCRIPTION
YES	Onsite Social Engineering: Involves an in-person simulated attack by attempting to convince employees to give our team physical or logical access to network resources. These attacks scenarios could include gaining physical access to server rooms/closets, placing rogue devices on the network, or establishing outbound reverse-shells to the Secure Yeti attack network. Specific scenarios for each location will be determined in the Rules of Engagement (ROE).
NO	Wireless Penetration Testing: Wireless networks play a crucial role within most organizations, serving as a vital means to access systems and data. The objective of this activity is to thoroughly analyze the associated wireless protocols/technologies employed by an organization while attempting to identify and exploit vulnerabilities that could lead to unauthorized network access and data leakage. Wireless penetration testing involves the analysis, examination, and possible exploitation of advertised and non-advertised wireless networks. Wireless testing will be performed using access normally granted to a: 1) typical employee, 2) visitor, and 3) anonymous user. Testing will focus on the ability that an employee or visitor may have to access restricted areas of the network from their wireless device. The result is an understanding of the organization's wireless infrastructure, and the ability to enhance security by proactively addressing potential weaknesses. Please note that wireless penetration activities must be performed on site.
NO	Web Application Testing: Web application testing focuses on evaluating the security of the web application itself, in addition to attempting to gain access to underlying infrastructure supporting the website. The testing methodology is based on the Open Web Application Security Project (OWASP). This ensures a consistent method for testing all security aspects of an application. The process involves an active analysis of the web application for any weaknesses, technical flaws, or vulnerabilities.
NO	Phishing Campaign: Involves a designated user group undergoing a phishing campaign designed to assess the probability of users engaging with maliciously crafted emails. This will be a one-time campaign, and any optional follow-up tests are not included in the base scope.
NO	Vishing Campaign: Involves a designated user group undergoing direct dial contact via phone. The calls will simulate real-world attacks aimed at gaining access to restricted information or resources, without the risk of actual information compromise.
NO	Firewall Review: Management devices such as firewalls, routers, and switches are commonly misconfigured within an organization's internal environment. Secure Yeti offers automated configuration reviews to ensure organizations are following industry suggested best-practices
NO	Policy Review: Vulnerabilities don't always exist in hardware or software. Many low-hanging vulnerabilities can be quickly and cost-effectively remediated by a simple policy change. Secure Yeti will review the following, to ensure they are following industry suggested best-practices.

2.2. EXPLANATION OF SEVERITY RATINGS

Each finding identified during this assessment was analyzed by our assessment team to discuss and determine the potential impact it may have on your organization, the likelihood that it could be exploited, and the likelihood of success if it was. After this analysis, a severity rating was assigned that represents the overall risk each finding represents for your organization.

Critical	Critical severity ranking requires immediate action through mitigating controls, direct remediation, or a combination thereof. Exploitation of discovered critical severity vulnerabilities not only results in privileged access to the target system/application and/or sensitive data but also allows access to other hosts or data stores within the environment.
High	A finding denoted with a high severity ranking suggests that this observation requires immediate evaluation and subsequent resolution. Exploitation of high severity vulnerabilities discovered in the environment can lead directly to an attacker gaining to the system/application and/or sensitive data.
Medium	A finding denoted with a medium severity ranking requires review and resolution within a short period. From a technical perspective, vulnerabilities that warrant a medium severity ranking can lead directly to an attacker gaining non-privileged access to a portion system/application and/or sensitive data or cause a denial-of-service (DoS) condition on the host, service, or application.
Low	A finding denoted with a low severity ranking requires an evaluation for review and resolution once the remediation efforts for critical, high, and medium severity issues are complete. From a technical perspective, vulnerabilities that warrant a low severity ranking may leak information to unauthorized or anonymous users and potentially used to launch a more targeted attack against the environment.
Info	An informational notation presents no direct threat to the confidentiality, integrity or availability of the data or systems supporting the environment. These issues pose an inherently low threat, and any proposed resolution should be considered as an addition to the information security procedures already in place.

2.3. CONTROL FAMILIES / RISK CATEGORIES

CONTROL FAMILY / CLASS		DESCRIPTION
Access Control *(Technical)*	(AC)	The AC Control Family consists of security requirements detailing who has access to what assets and reporting capabilities like account management, system privileges, and remote access logging to determine when users have access to the system and their level of access.
Audit & Accountability *(Technical)*	(AU)	The AU control family consists of security controls related to an organization's audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information.
Awareness & Training *(Operational)*	(AT)	The control sets in the AT Control Family are specific to your security training and procedures, including security training records.
Configuration Management *(Technical)*	(CM)	CM controls are specific to an organization's configuration management policies. This includes a baseline configuration to operate as the basis for future builds or changes to information systems. Additionally, this includes information system component inventories and a security impact analysis control.
Contingency Planning *(Operational)*	(CP)	The CP control family includes controls specific to an organization's contingency plan if a cybersecurity event should occur. This includes controls like contingency plan testing, updating, training, and backups, and system reconstitution.
Identification & Authentication *(Technical)*	(IA)	IA controls are specific to the identification and authentication policies in an organization. This includes the identification and authentication of organizational and non-organizational users and how the management of those systems.
Incident Response *(Operational)*	(IR)	IR controls are specific to an organization's incident response policies and procedures. This includes incident response training, testing, monitoring, reporting, and response plan.
Maintenance *(Technical)*	(MA)	The MA controls in NIST 800-53 revision five detail requirements for maintaining organizational systems and the tools used.
Media Protection *(Operational)*	(MP)	The MP family includes controls that are specific to access, marking, storage, transport policies, sanitization, and defined organizational media use.

CONTROL FAMILY / CLASS		DESCRIPTION
Personally Identifiable Information Processing & Transparency *(Operational)*	(PT)	The PT control relates to an operation or set of operations performed upon personally identifiable information that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of personally identifiable information.
Personnel Security *(Operational)*	(PS)	PS controls relate to how an organization protects its personnel through position risk, personnel screening, termination, transfers, sanctions, and access agreements.
Physical & Environmental Protection *(Operational)*	(PE)	The PE control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.
Planning *(Management)*	(PL)	PL controls in NIST 800-53 are specific to an organization's security planning policies and must address the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
Program Management *(Management)*	(PM)	The PM control family is specific to who manages your cybersecurity program and how it operates. This includes, but is not limited to, a critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture.
Risk Assessment *(Management)*	(RA)	The RA control family relates to an organization's risk assessment policies and vulnerability scanning capabilities.
Security Assessment & Authorization *(Management)*	(CA)	The CA control family includes controls that supplement the execution of security assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections.
Supply Chain Risk Management *(Management)*	(SR)	The SR control refers to the systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain.
System & Communications Protection *(Technical)*	(SC)	The SC control family is responsible for systems and communications protection procedures. This includes boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.

CONTROL FAMILY / CLASS		DESCRIPTION
System & Information Integrity *(Technical)*	(SI)	The SI control family covers controls that protect system and information integrity. These include flaw remediation, malicious code protection, information system monitoring, security alerts, software and firmware integrity, and spam protection.
System and Services Acquisition *(Management)*	(SA)	The SA control family relates to controls that protect allocated resources and an organization's system development life cycle. This includes information system documentation controls, development configuration management controls, and developer security testing and evaluation controls.

2.4. RISK ASSIGNMENT

Just as one cannot make assumptions based solely on outward appearances, one cannot judge a vulnerability without the context in which that vulnerability exists. Vulnerabilities are inherently neutral. Their significance depends on factors that can either mitigate or elevate their potential risk. It is impossible to gauge the potential harm or determine effective mitigation measures without ascertaining the risk a vulnerability represents. In determining overall risk, our team analyzes two key factors for each finding:

1. IMPACT: defined as "the magnitude of harm that can be expected." When calculating impact, the following possibilities are considered:
    - degradation of mission capabilities
    - damage / loss of organizational assets or data (& sensitivity of that data)
    - financial loss
    - reputational loss
    - loss of life or physical harm

2. LIKELIHOOD: defined as "the probability of an event occurring." When calculating likelihood, we consider:
    - the likelihood of the event occurring or being initiated
    - the likelihood of the event being successful
    - factors that mitigate risk (i.e. – small user-base, located on an isolated network, rarely used)
    - factors that magnify risk (i.e. – publicly accessible, weak password policies, misconfigurations)

LIKELIHOOD \ IMPACT	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

OVERALL RISK

OVERALL RISK DETERMINATION CHART – BASED ON IMPACT-LIKELIHOOD ANALYSIS.

3. ASSESSMENT SCOPE

3.1. SCOPE SUMMARY

Secure Yeti and the NDIT team worked together to coordinate logistics and define the scope of testing for this engagement. These details were finalized and recorded within the Rules of Engagement (RoE) document, which served as the assessment team's roadmap for testing. Both parties approved the RoE before any testing began. The tables below identify networks and hosts determined to be in scope for this engagement.

The scope of this assessment consisted of:

TOTAL IP ADDRESSES	EXTERNAL IP ADDRESSES	INTERNAL IP ADDRESSES	EXCLUDED IP ADDRESSES
40,462	32,246	8,216	199,765**

CIDR BLOCK	BLOCK SIZE	EXTERNAL BLOCKS	EXTERNAL COUNT	INTERNAL BLOCKS	INTERNAL COUNT	EXCLUDED BLOCKS	EXCLUDED COUNT
/8	16,777,216	-	0	-	0	-	0
/9	8,388,608	-	0	-	0	-	0
/10	4,194,304	-	0	-	0	-	0
/11	2,097,152	-	0	-	0	-	0
/12	1,048,576	-	0	-	0	-	0
/13	524,288	-	0	-	0	-	0
/14	262,144	-	0	-	0	-	0
/15	131,072	-	0	-	0	-	0
/16	65,536	-	0	-	0	3	196.605
/17	32,768	-	0	-	0	-	0
/18	16,384	-	0	-	0	-	0
/19	8,192	-	0	-	0	-	0
/20	4,096	3	12,288	-	0	-	0
/21	2,048	1	2,048	-	0	-	0
/22	1,024	9	9,216	1	1024	-	0
/23	512	5	2,560	9	4,608	-	0
/24	256	17	4,352	8	2,048	12	3,072
/25	128	7	896	2	256	-	0
/26	64	6	384	2	128	-	0
/27	32	8	256	1	32	-	0
/28	16	8	128	1	16	-	0
/29	8	12	96	13	104	-	0
/30	4	5	20	-	0	-	0
/31	2	-	0	-	0	-	0
/32	1	2	2	-	0	88	88

SUMMARY OF THE IP SPACE AND UNIQUE CIDR BLOCKS TESTED. DOES NOT INCLUDE IPV6 BLOCKS.

** please note that these exclusions were not included in the in-scope IP count provided in the Rules of Engagement document (RoE) and are not reflected in the total IP count above.

3.2. CHANGES TO APPROVED SCOPE

- No changes to the approved scope were made or requested.

3.3. ON-SITE SOCIAL ENGINEERING SCOPE

#	NAME / LOCATION / ROOM	ADDRESS
1	Bank of North Dakota	1200 Memorial Highway Bismarck, ND. 58506 07/09/2024 – 07/12/2024 from 8AM – 5PM Authorizing Officials: Charlie Tweet – Director of IT Allison Anderson – Chief Banking & Innovation Officer Christy Steffenhagen – Chief Risk Officer

4. FINDINGS SUMMARY - CHARTS & GRAPHS

4.1. NIST CONTROL FAMILY SUMMARY

In addition to the assessment of risk, each finding is also sorted into functional categories, known as “control families.” If the observed deficicency for a particular find applies to multiple families, a secondary classification is assigned.

The table below shows the breakdown of findings based on control families:

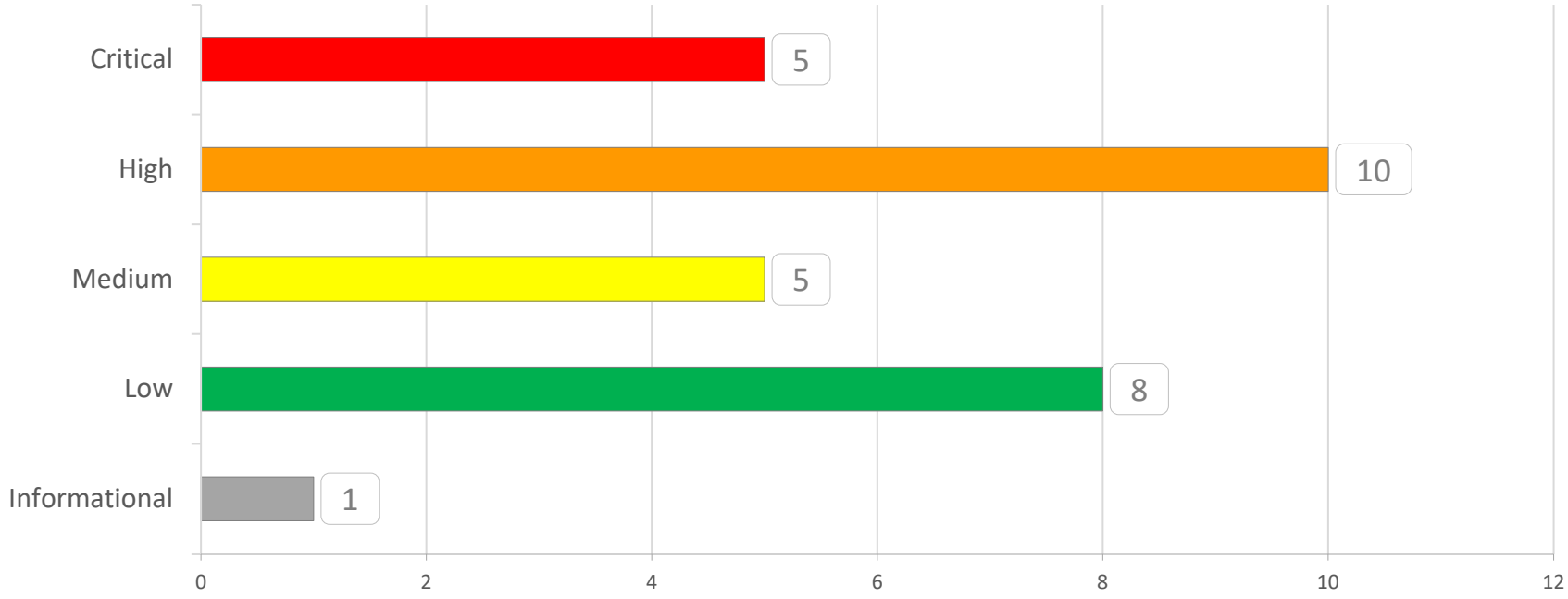
Control Families:	PRIMARY	SECONDARY	COUNT
Access Control	2	2	4
Access, Authorization, & Monitoring	0	0	0
Audit & Accountability	1	0	1
Awareness & Training	2	1	3
Configuration Management	7	7	14
Contingency Planning	0	0	0
Identification & Authentication	5	1	6
Incident Response	0	1	1
Maintenance	0	0	0
Media Protection	0	0	0
Personnel Security	0	0	0
Physical & Environmental Protection	0	1	1
Planning	0	0	0
Program Management	0	0	0
Risk Assessment	0	0	0
Security Assessment & Authorization	0	0	0
Supply Chain Risk Management	0	0	0
System & Communications Protection	5	3	8
System & Information Integrity	7	1	8
System & Services Acquisition	0	0	0
TOTAL:	29	17	46

4.2. HEAT MAP (RISK / NIST CONTROL FAMILY

CONTROL FAMILY / RISK LEVEL:	CRITICAL (16 PTS)	HIGH (8 PTS)	MEDIUM (4 PTS)	LOW (2 PTS)	INFO (1 PT)	TOTAL POINTS
Configuration Management:	1	6	2	4	1	81
System & Communications Protection:	2	3	0	3	0	62
Identification & Authentication:	1	3	1	1	0	46
System & Information Integrity:	1	1	3	3	0	42
Access Control:	1	2	0	1	0	34
Awareness & Training:	0	2	0	1	0	18
Physical & Environmental Protection:	1	0	0	0	0	16
Audit & Accountability:	1	0	0	0	0	16
Incident Response:	1	0	0	0	0	16
Assessment, Authorization, & Monitoring:	0	0	0	0	0	0
PII Processing & Transparency:	0	0	0	0	0	0
Contingency Planning:	0	0	0	0	0	0
Maintenance:	0	0	0	0	0	0
Media Protection:	0	0	0	0	0	0
Personnel Security:	0	0	0	0	0	0
Planning:	0	0	0	0	0	0
Program Management:	0	0	0	0	0	0
Risk Assessment:	0	0	0	0	0	0
Supply Chain Risk Management:	0	0	0	0	0	0
System & Services Acquisition:	0	0	0	0	0	0
TOTAL POINTS:	144	136	24	26	1	331

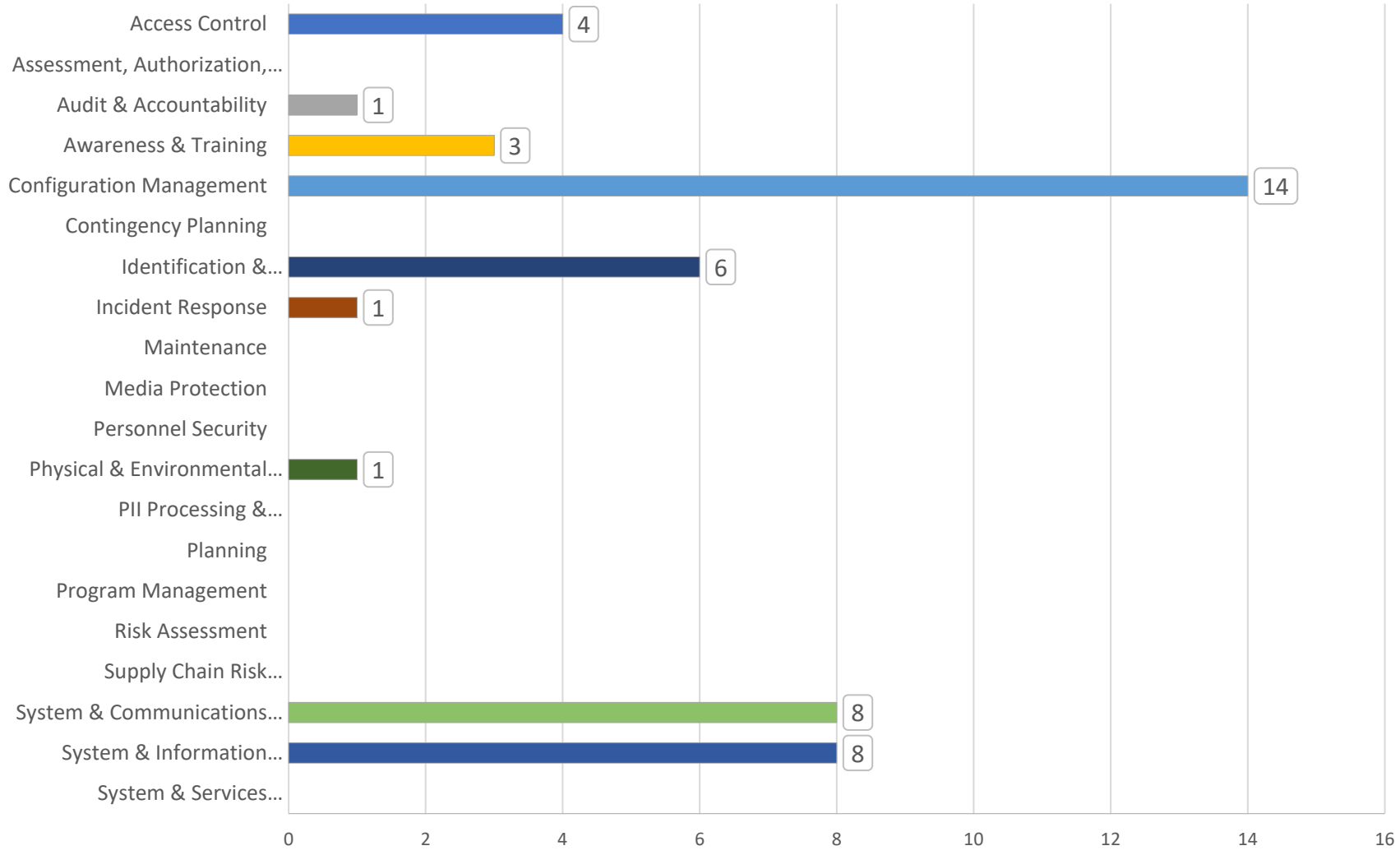
DISTRIBUTION & RISK-LEVEL OF FINDINGS PER CONTROL FAMILY. PLEASE NOTE THAT THIS CHART DOES NOT NECESSARILY INDICATE PRIORITY

4.3. LINE GRAPHS (FINDINGS PER RISK LEVEL)



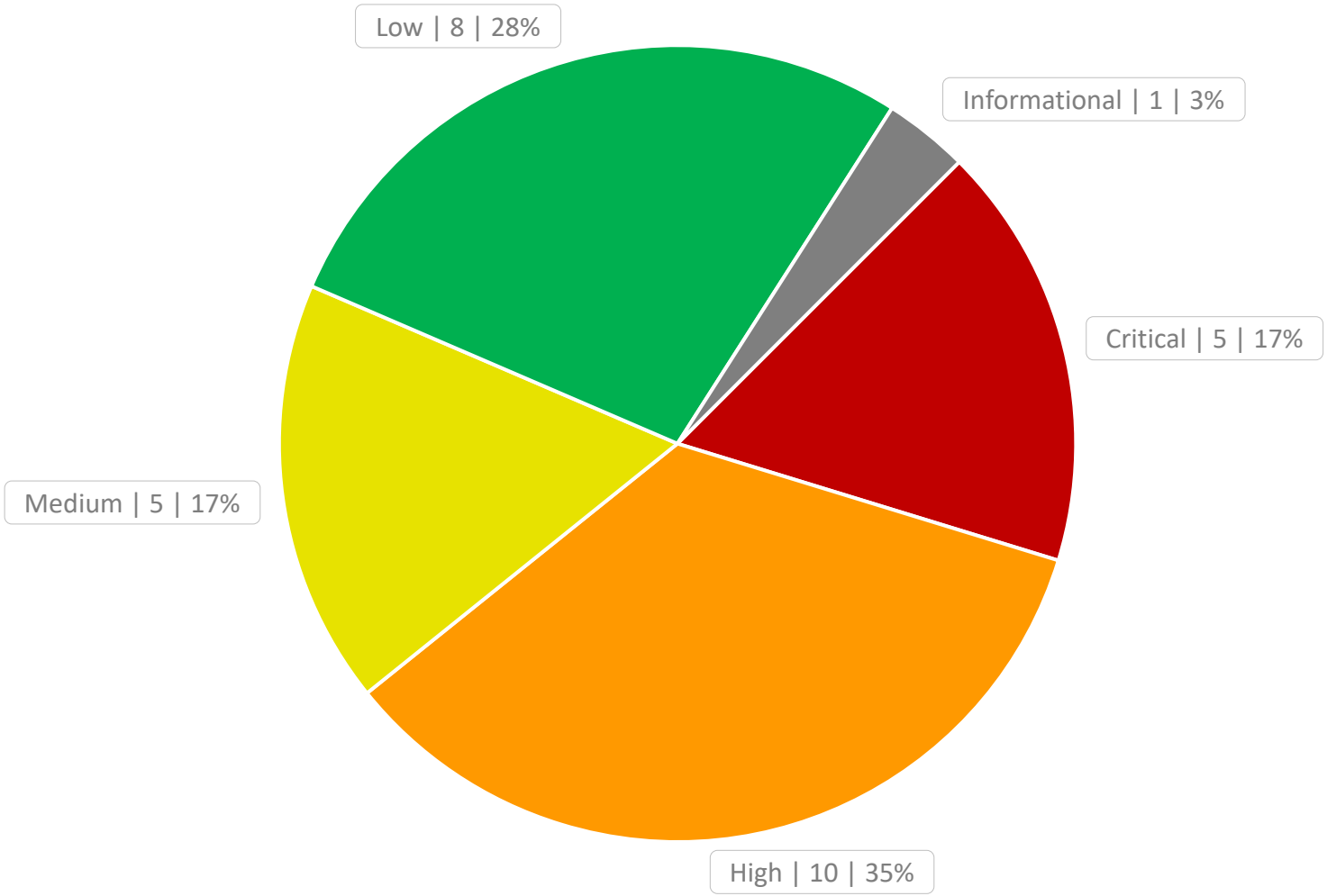
DISTRIBUTION OF FINDINGS PER RISK LEVEL

4.4. LINE GRAPH (FINDINGS PER NIST CONTROL FAMILY)



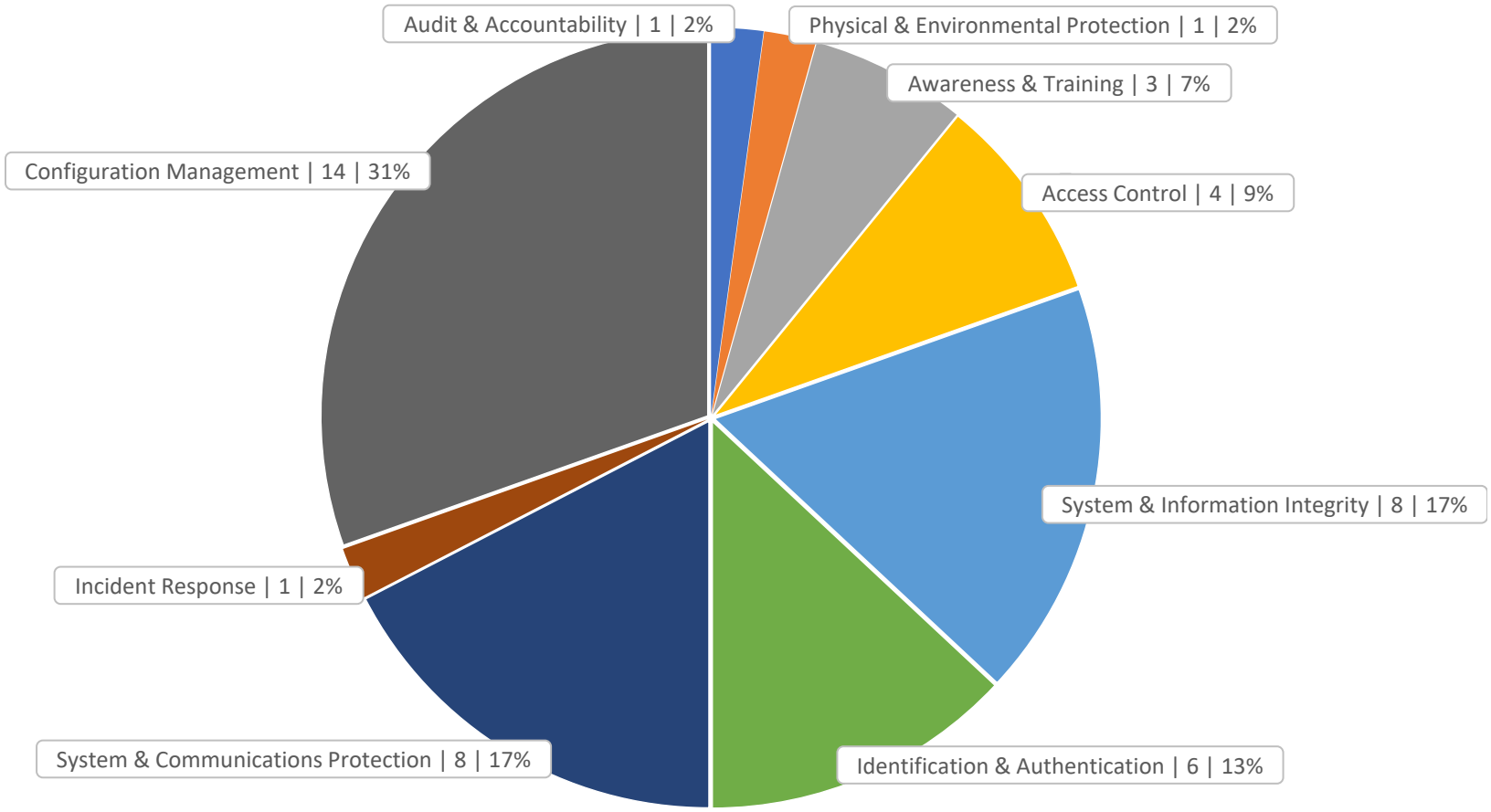
DISTRIBUTION OF FINDINGS PER NIST CONTROL FAMILY

4.5. PIE CHART (FINDING PER RISK LEVEL)



PIE CHART SHOWING PERCENTAGE OF FINDINGS PER LEVEL OF RISK

4.6. PIE CHART (FINDINGS PER NIST CONTROL FAMILY)



PIE CHART SHOWING PERCENTAGE OF FINDINGS PER CONTROL FAMILY

[PAGE INTENTIONALLY LEFT BLANK]