GLBA From Auditors Perspective and Most Frequent Audit Findings

Cristian Ojeda Colón, CPA
Audit & Assurance Manager
Galíndez LLC

Galíndez LLC TRUSTworthy

Nexia

Relief and Legal Warning

- *This presentation is for educational purpose only and is not intended, nor should it be considered, as a contributor, legal or an accounting consultation.*

- *Any advise that this presentation contains has not been considered or written to be used, and can not be used, for the purpose of evading penalties that may be imposed under the Internal Revenue Code or any local, state or federal tax provision.*

Galíndez, LLC (December 7, 2023)

Terminology and Abbreviations

GLBA	Gramm-Leach-Bliley Act
ED	U.S. Department of Education
IHE	Institutions of Higher Education
QI	Qualified Individual
IT	Information Technology
FTC	Federal Trade Commission
TPS	Third-party servicer
PII	Personal Identifiable Information
GEN	Dear Colleague Letter
HEA	Higher Education Act
CFR	Code of Federal Regulations
PPA	Program Participation Agreement

AGENDA

Gramm-Leach-Bliley Act – Student Information Security Auditors' Perspective

Most frequent audit findings

Current financial outlook of universities

Gramm-Leach-Bliley Act– Student Information Security - (cont.)

- GLBA was enacted in 1999 (Pub. L. No. 106-102)
  - Provides a framework for regulating the privacy and data security practices of a broad range of financial institutions.
  - Requires financial institutions to provide customers with information about the institutions' privacy practices and about their opt-out rights, and to implement security safeguards.
- The Federal Trade Commission considers Title IV-eligible institutions that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act because they appear to be significantly engaged in wiring funds to consumers.
- Institutions (IHE/Colleges) agree to comply with GLBA in their Program Participation Agreement with ED.
- Institutions must protect student financial aid information, with particular attention to information provided to institutions by ED or otherwise obtained in support of the administration of the Federal student financial aid program.

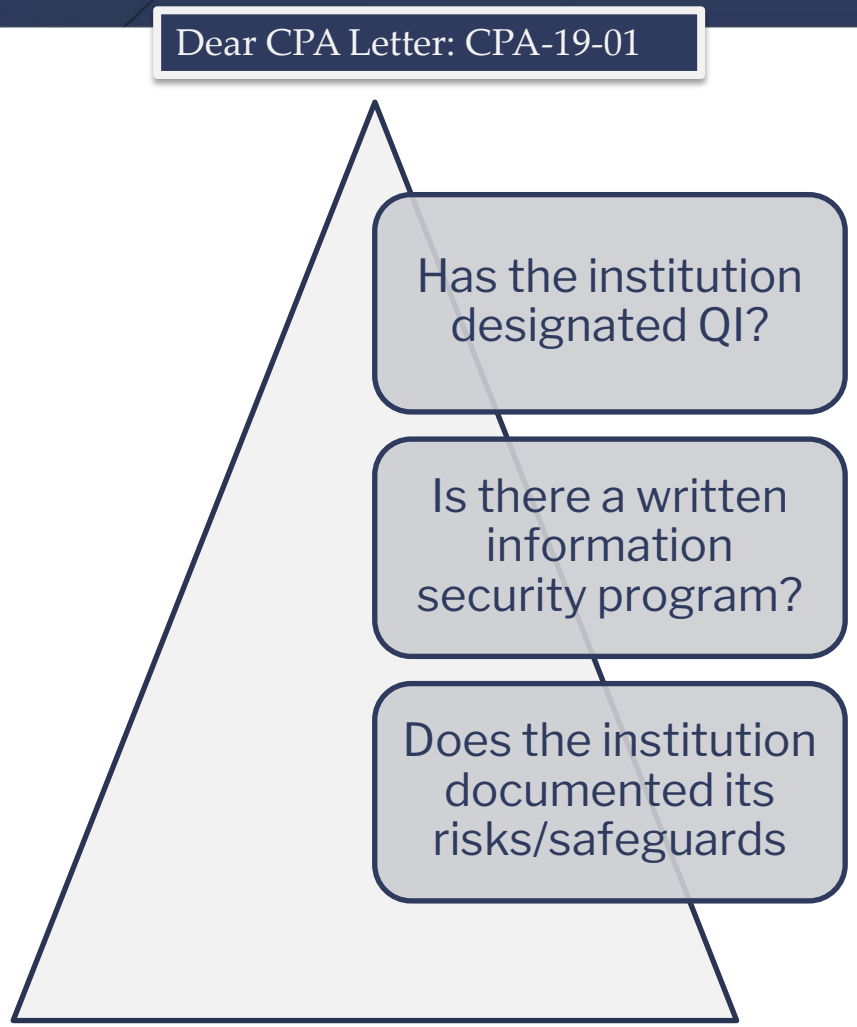
Gramm-Leach-Bliley Act– Student Information Security - (cont.)

"Auditors are expected to evaluate the information safeguard requirements of GLBA in audits of postsecondary institutions or third-party servicers under the regulations in 16 C.F.R. Part 314:"

1. Verify that the institution has designated an individual to coordinate the information security program and enforce its compliance.

2. Verify that the institution has a written information security program and that the written information security program addresses the remaining six required minimum elements.

When an auditor determines that an institution or servicer has **failed to comply with any of these GLBA requirements, the finding will be included in the institution's audit report.**



Gramm-Leach-Bliley Act– Student Information Security - (cont.)

The elements that an institution must address in its written information security program are at 16 CFR 314.4

1. Designates a qualified individual responsible for overseeing and implementing the institution's information security program and enforcing the information security program in compliance (16 CFR 314.4(a)).
   - In cases where an institution uses a service provider

     - Retain responsibility for compliance with GLBA;
     - Designate a senior member of its personnel responsible for direction and oversight of the Qualified Individual; and
     - Require the service provider or affiliate to maintain an information security program that protects the institution in accordance with the requirements of the regulations at 16 CFR Part 314(a)(1) through (3).

GLBA- elements that an institution must address in its written information security program (cont.)

2. Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (16 CFR 314.4(b).

3. Provides for the design and implementation of safeguards to control the risks the institution identifies through its risk assessment (16 CFR 314.4(c)).

4. Provides for the institution to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 CFR 314.4(d)).

5. Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 CFR 314.4(e)(1)).

6. Addresses how the institution will oversee its information system service providers (16 CFR 314.4(f)).

7. Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring;

Gramm-Leach-Bliley Act– Student Information Security - (cont.)

Minimum safeguards that the written information security program must address:

1. Implement and periodically review access controls.
2. Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted.
3. Encrypt customer information on the institution's system and when it's in transit.
4. Assess apps developed by the institution.
5. Implement multi-factor authentication for anyone accessing customer information on the institution's system.
6. Dispose of customer information securely.
7. Anticipate and evaluate changes to the information system or network.
8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access.

GLBA– Documents requested by auditors-

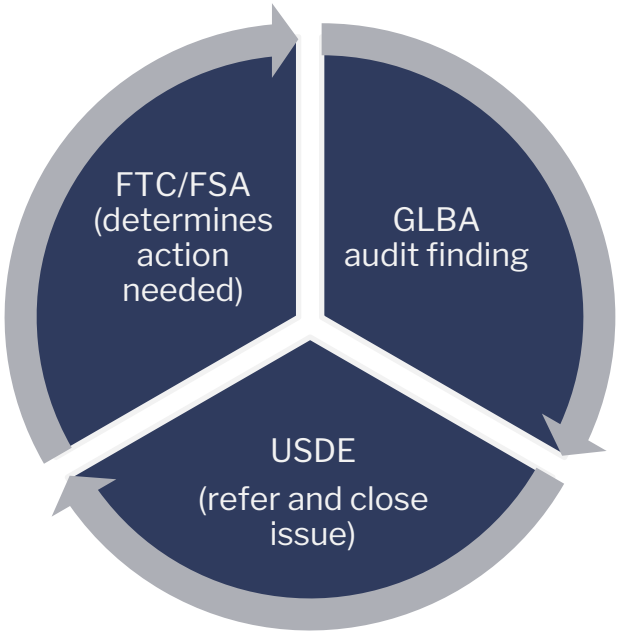
GLBA Security and Compliance Plan
Business Continuity Plan (BCP)
IT Security Policy
IT Network Monitoring Procedure
Antivirus/Endpoint Monitoring Procedure
Pentest Report
Risk Assessment Report
Users Security Awareness Procedure
User Awareness Training Evidence – performed each year
Business Continuity Test Report
IT Office Organizational Chart
Network Diagram (including security perimeters controls)
Financial and Academic Applications Inventory

Gramm-Leach-Bliley Act– Student Information Security

Dear CPA Letter: CPA-19-01

Federal Trade Commission

1. When an audit report that includes a GLBA audit finding is received by the Department, we will refer the audit to the FTC.
2. Once the finding is referred to the FTC, that finding will be considered closed for the Department's audit tracking purposes.
3. The FTC will determine what action may be needed as a result of the GLBA audit finding.



Gramm-Leach-Bliley Act– Student Information Security

Dear CPA Letter: CPA-19-01

FSA Cybersecurity Team

1. Federal Student Aid's Postsecondary Institution Cybersecurity Team (Cybersecurity Team) will also be informed of findings related to GLBA, and may request additional documentation from the institution in order to assess the level of risk to student data presented by the institution or servicer's information security system.

2. If the Cybersecurity Team determines that the institution or servicer poses substantial risk to the security of student information, the Cybersecurity Team may temporarily or permanently disable the institution or servicer's access to the Department's information systems.

3. Additionally, if the Cybersecurity Team determines that as a result of very serious internal control weaknesses of the general controls over technology that the institution's or servicer's administrative capability is impaired or it has a history of non-compliance, it may refer the institution to the Department's Administrative Actions and Appeals Service Group for consideration of a fine or other appropriate administrative action by the Department.

Request additional information

Disable access to the Department's information systems

Fine or administrative action

Fines & Penalties

FAILURE TO COMPLY WITH GLBA

- Organizations are fined up to $100,000 for each violation of this law, and the officers and directors of the organization may be fined up to $10,000 personally. Individual may also face up to 5 years in prison.

GLBA– GEN 23-03 & 08 (update)

Issued on February 15, 2023 and updated on May 16, 2023

Update list of functions and activities that fall within the scope of the third-party servicer (TPS) (§ 668.2) requirements.

*An institution may **not contract** with a TPS to perform any aspect of the institution's participation in a Title IV program if the servicer is located outside U.S. or operated by a non citizen.

An institution must report any individual or entity with which it contracts that meets the TPS criteria listed above using the Department's E-App process.

GLBA– GEN 23-03 & 08 (update) – cont.

Third-party servicer

(1) An individual or a State, or a private, profit or nonprofit organization that enters into a contract with an eligible institution to administer, through either manual or automated processing, any aspect of the institution's participation in any Title IV, HEA program. The Secretary considers administration of participation in a Title IV, HEA program to—

GLBA– GEN 23-03 & 08 (update) – (cont.)

- Recruitment
- Student & institutional
- Consumer information
- Default prevention
- Delivery of Title IV funds
- Computer services
- Retention of students
- Instructional content
- Consulting and auditing

Third-Party Servicer	Not a Third-Party Servicer
The activities, functions, services, or roles in this column **ARE** considered an aspect of an institution's participation in a Title IV program, whether performed from a remote location or on-site at an institution, and thus are subject to TPS requirements if performed on behalf of a Title IV-eligible institution. The institution and TPS are jointly and severally liable to the Department for any violation by a TPS.	The activities, functions, services, or roles in this column **ARE NOT** considered an aspect of an institution's participation in a Title IV program and thus are not subject to TPS requirements if performed on behalf of a Title IV-eligible institution. The institution is solely responsible for any Title IV liability incurred as a result of a non-TPS contractor violation.

GLBA– GEN 23-03 & 08 (update) – (cont.)

Effective date

May 1, 2023

September 1, 2023

September 1, 2023 no longer in effect

ED plan to issue a final revised DCL with an effective date **at least six months after its publication** to allow institutions and third-party servicers covered by the final guidance to meet any reporting requirements.

Common GLBA Compliance Findings

- Missing Information Technology Point of Contact.
- Risk Assessment has not been performed.
- Use of accounts that are not password protected.
- Account passwords shared with staff members and student interns.
- Scanning and storage of PII to a network that can be easily accessed through any of the common administrator accounts.
- Discovered malicious programs, such as ones capable of capturing keystrokes typed on the keyboard (keylogger).

Finding Examples

Part III - Findings and Questioned Costs Relating to Federal Awards – (continued)

Finding No. 2019-03

Special Tests and Provisions – Gramm-Leach-Bliley Act –Student Information Security

Federal Program

Students Financial Assistance Programs Cluster
CFDA 84.007 Federal Supplemental Educational Opportunity Grants
CFDA 84.033 Federal Work-Study Program
CFDA 84.063 Federal Pell Grant Program
CFDA 84.268 Federal Direct Student Loan Program

Name of Federal Agency

U.S. Department of Education

Pass-through Entity

N/A

Category

Compliance/Internal Control – Significant deficiency

Compliance Requirements

Special Tests and Provisions – Gramm-Leach-Bliley Act –Student Information Security

Criteria

Development, implementation and maintenance of a formal Information Security Program is a new requirement set forth in the 2019 OMB Compliance Supplement following The Federal Trade Commission's consideration that Title IV - eligible institutions that participate in Title IV Educational Assistance Programs are designated as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 CFR 313.4).

Part III - Findings and Questioned Costs Relating to Federal Awards – (continued)

Finding No. 2019-03

Special Tests and Provisions – Gramm-Leach-Bliley Act –Student Information Security (continued)

Condition

Under an institution's Program Participation Agreement with the U.S. Department of Education and the Gramm-Leach-Bliley Act, schools must protect student financial aid information, with particular attention to information provided to the University by the USDE or otherwise obtained in support of the administration of the federal student financial aid programs. Review and inquiry procedures disclosed that the University has not developed, implemented or maintained a formal Information Security Program as required by the newly released Compliance Supplement (2019), since no formal Information Security Risk Assessment has been performed to sustain actual control environment.

Cause

As part of the development, implementation and maintenance of an information security program, the University must have designated an employee to coordinate the program. However, the key project personnel in charge resigned and the University could not replace this position in a short time.

Effect

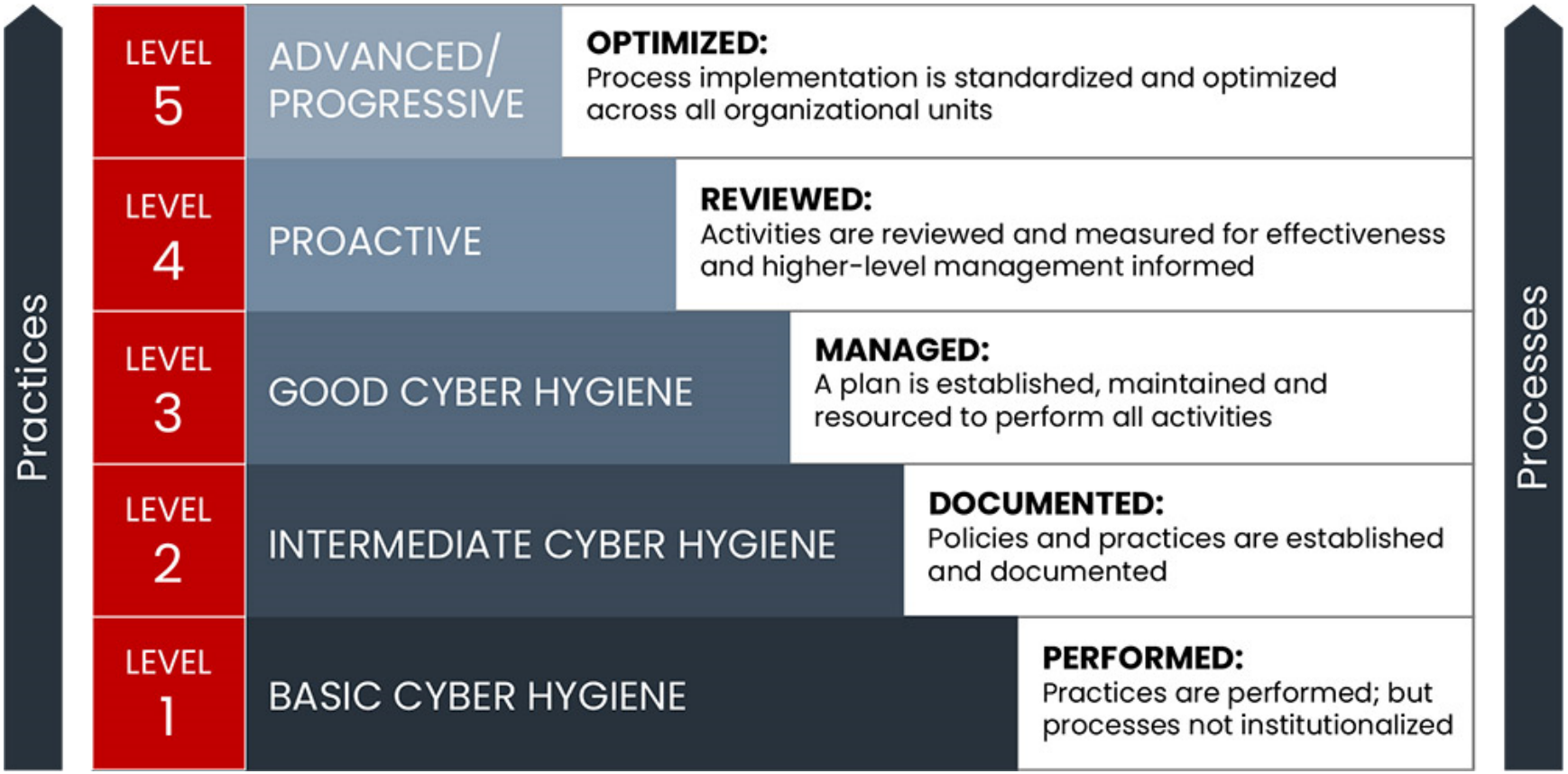
Information security is the process by which institutions protects the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware and infrastructure used to store and transmit such information. Information security promotes the commonly accepted objectives of confidentiality, integrity, and availability of information and is essential to the overall safety and soundness of an institution. Information security exists to provide protection from malicious and non-malicious actions that increase the risk of adverse effects on earnings, capital, or enterprise value.

The potential adverse effects that can arise from not having a proper Information Security Program include disclosure of information to unauthorized individuals, unavailability or degradation of services, modification or destruction of systems or information as well as possible critical data losses which can lead to fines, sanctions, and reputational damage.

Questioned Cost

None

Cyber Hygiene



Audit risk and most frequent audit findings

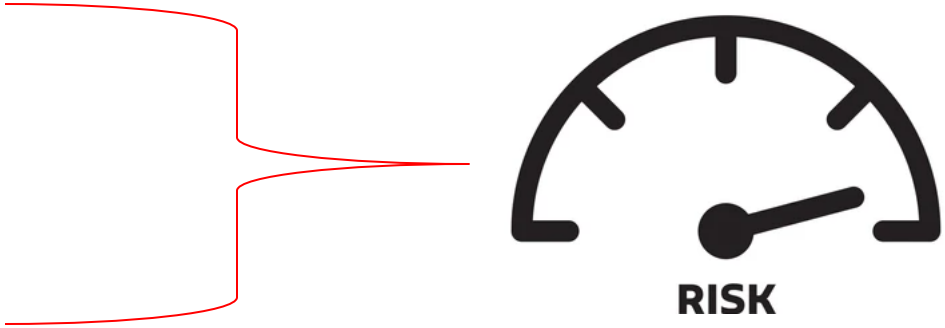
Audit risk

Programs designated by ED as susceptible to significant improper payments

- Pell Grant
- Direct Loans

Test that may identify improper payments

- Eligibility
- Cash Management
- Verification
- Disbursements
- Return of IV funds



Audit risk - cont.

Factors that contribute to an increase audit risk in SFA cluster

Changes in payment methods

Significant increase in enrollment

New bachelor's and master's programs

Technology and IT controls

Expiration of agreements and contracts (PPA, Ecar, etc.)

Program reviews

Control environment

Most frequent audit findings

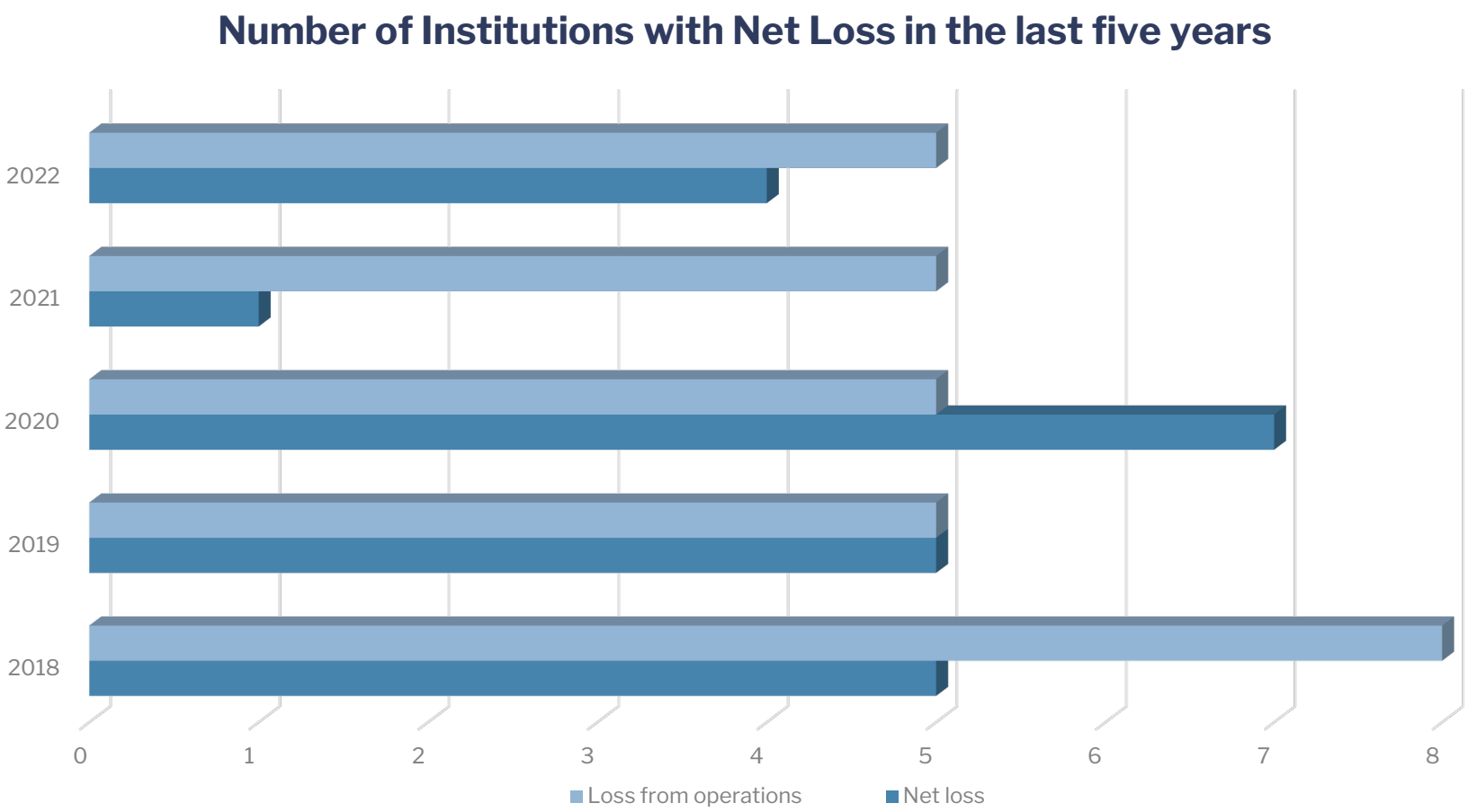
Number	Findings	Compliance Requirement
1	Time Elapsing Between Transfer of Funds and Disbursements exceeding reasonable time	Cash Management
2	The University, specifically the Institute division, does not have an internal control system designed to provide for the segregation of duties to ensure cash draw downs and indirect cost allocations prepared are reviewed by separate individuals.	Cash Management – Drawdowns of funds
3	Advanced funds remained idle at the University's operational account for an extended amount of time	Cash Management – Drawdowns of funds
4	The University inadvertently failed to report the correct Pell disbursement date in the Pell disbursement records.	Reporting - Pell Disbursement and Origination Records
5	University incorrectly calculated the credit balance.	Special Test and Provisions – Disbursement to or on Behalf of Students under the Federal Direct Student Loan Program – Credit Balances
6	University failed to properly allocate the Direct Loans funds in the required order.	Special Test and Provisions – Return of Title IV Funds – Allocation of Funds
7	Disbursements To or On Behalf of Students: The University failed to issue the required loan notifications to students within the required timeframe.	Special Tests and Provisions
8	Monthly reconciliations of the SAS data files with the University's financial records were not prepared on a timely basis.	Special Tests and Provisions – Borrower Data and Reconciliation (Direct Loan)

Most frequent audit findings – cont.

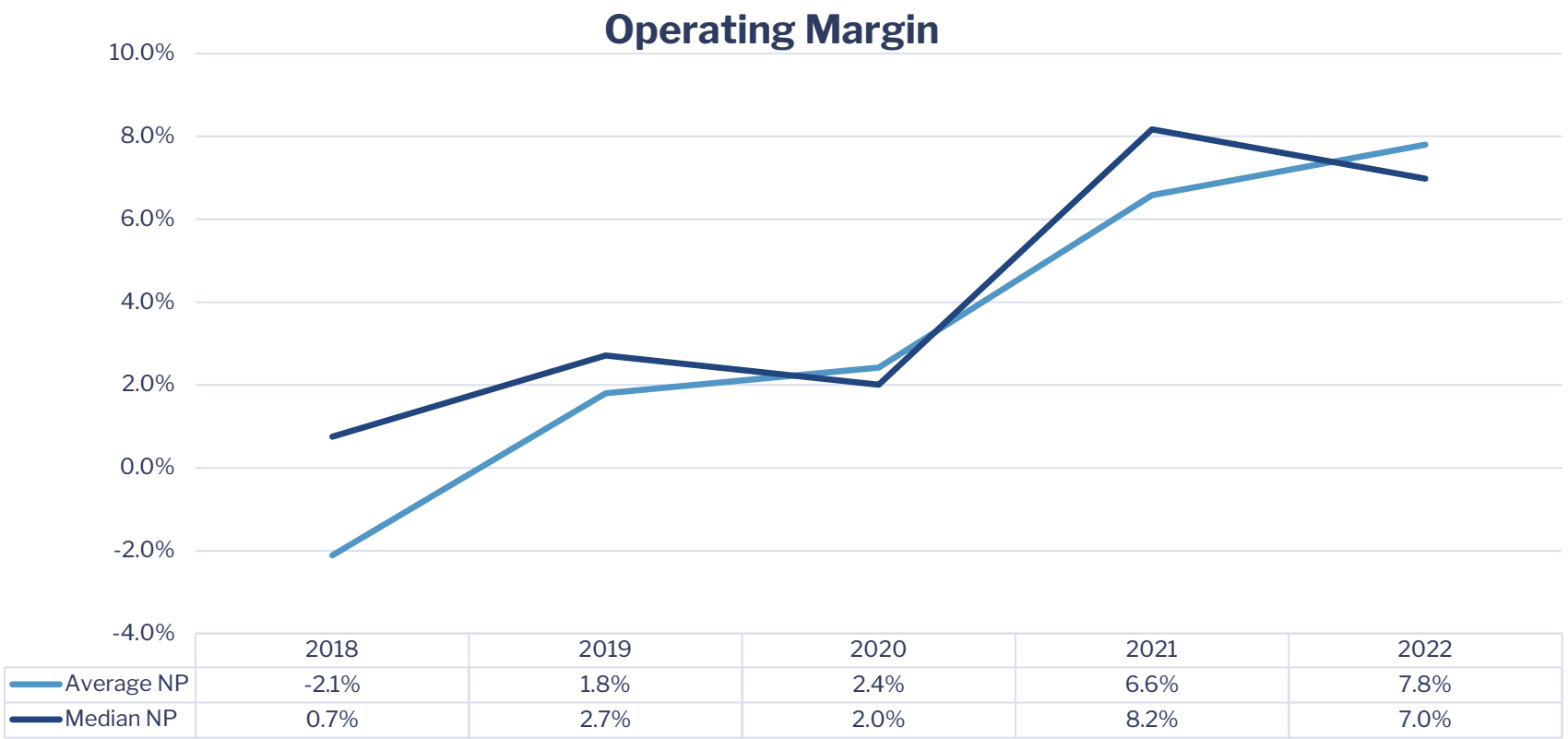
Number	Findings	Compliance Requirement
9	University failed to properly submit the disbursement records to the Common Origination and Disbursement (COD) center within 15 days of the disbursement date. (Direct Loans program and PELL)	Special Tests and Provisions – Borrower Data Transmission and Reconciliation - Reporting
10	No monthly reconciliations of the SAS data files with the University's financial records were available for test.	Special Tests and Provisions – Borrower Data Transmission and Reconciliation - Reporting
11	University failed to return the corresponding refund within 14 days' time frame from the date the University determined that the student had a Federal Student Aid (FSA) credit balance.	Special Tests and Provisions – Disbursements to or on Behalf of Students
12	University failed to properly include all the required information on the loan disbursement notifications.	Special Tests and Provisions – Disbursements to or on Behalf of Students under the Federal Direct Student Loan Program - Notifications
13	University failed to provide evidence of the written notification sent to the participating students or their parents.	Special Tests and Provisions – Disbursements to or on Behalf of Students under the Federal Direct Student Loan Program - Notifications
14	The status change was never reported to National Student Loan Data System (NSLDS) which is the Department of Education central database for student aid.	Special Tests and Provisions – Enrollment Reporting
15	The status change reported to the National Student Loan Data System (NSLDS) was past the 60 days established threshold.	Special Tests and Provisions – Enrollment Reporting
16	Return of Title IV funds was computed using an incorrect date	Special Tests and Provisions - Return of Title IV Funds and Disbursements to or on behalf of students

Current financial outlook of universities

Number of Institutions with Net Loss in the last five years

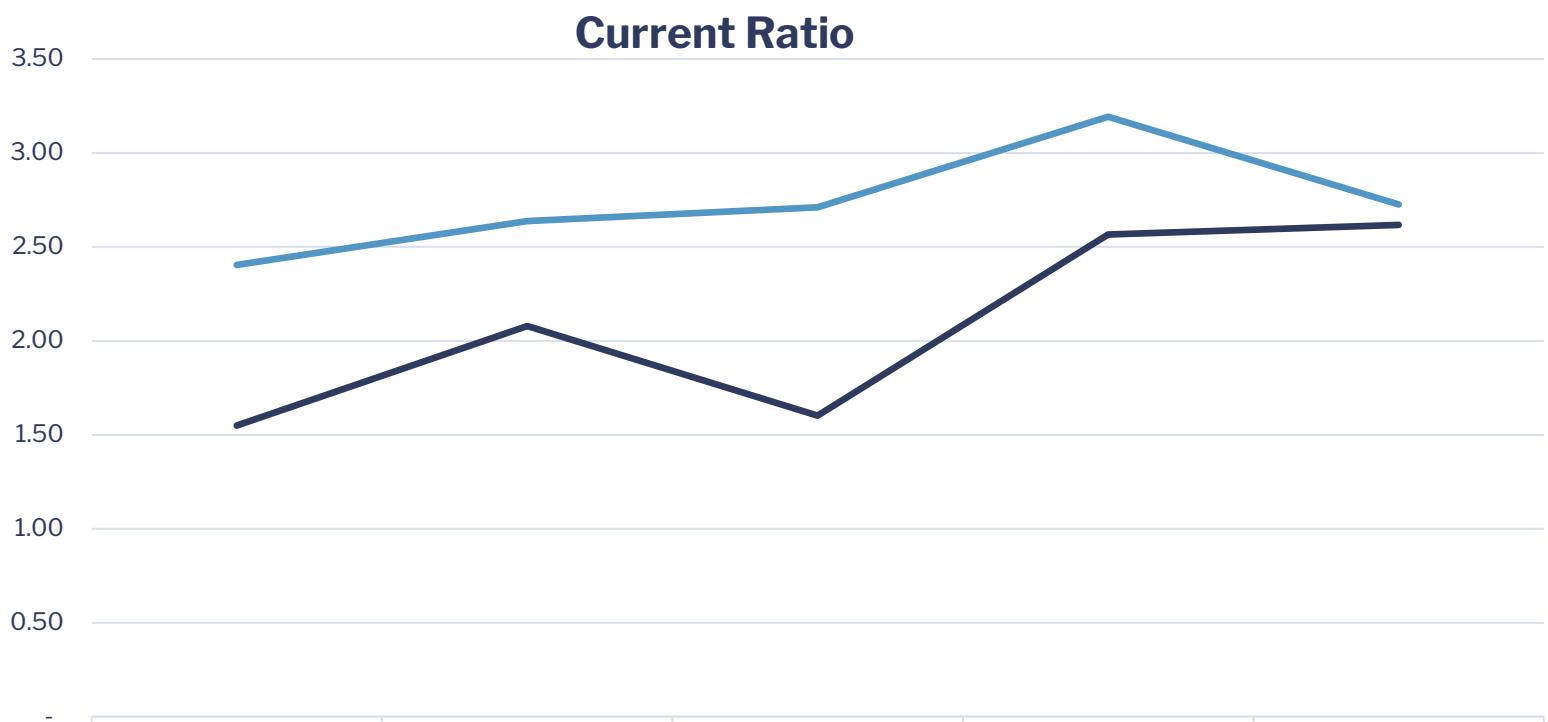


Operating Margin



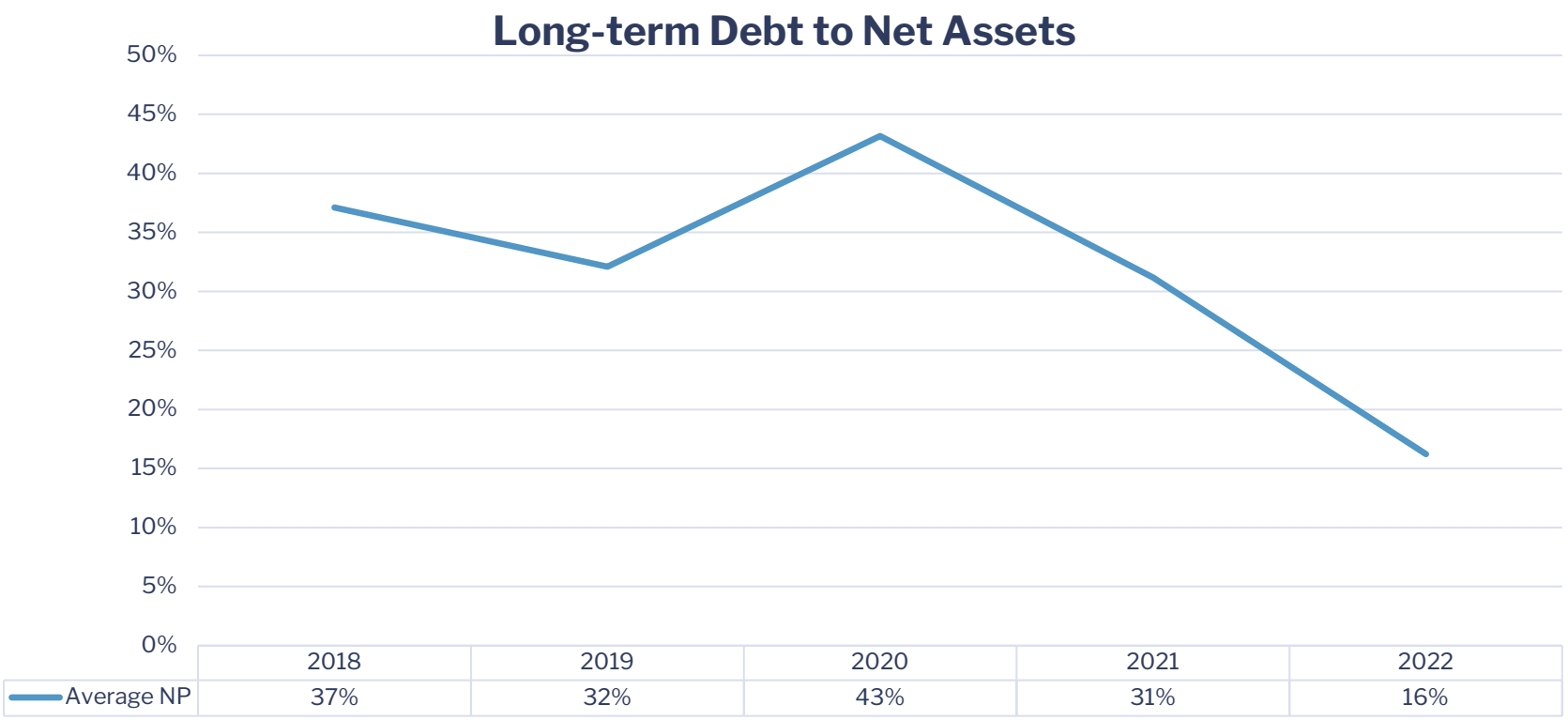
	2018	2019	2020	2021	2022
Average NP	-2.1%	1.8%	2.4%	6.6%	7.8%
Median NP	0.7%	2.7%	2.0%	8.2%	7.0%

Current ratio

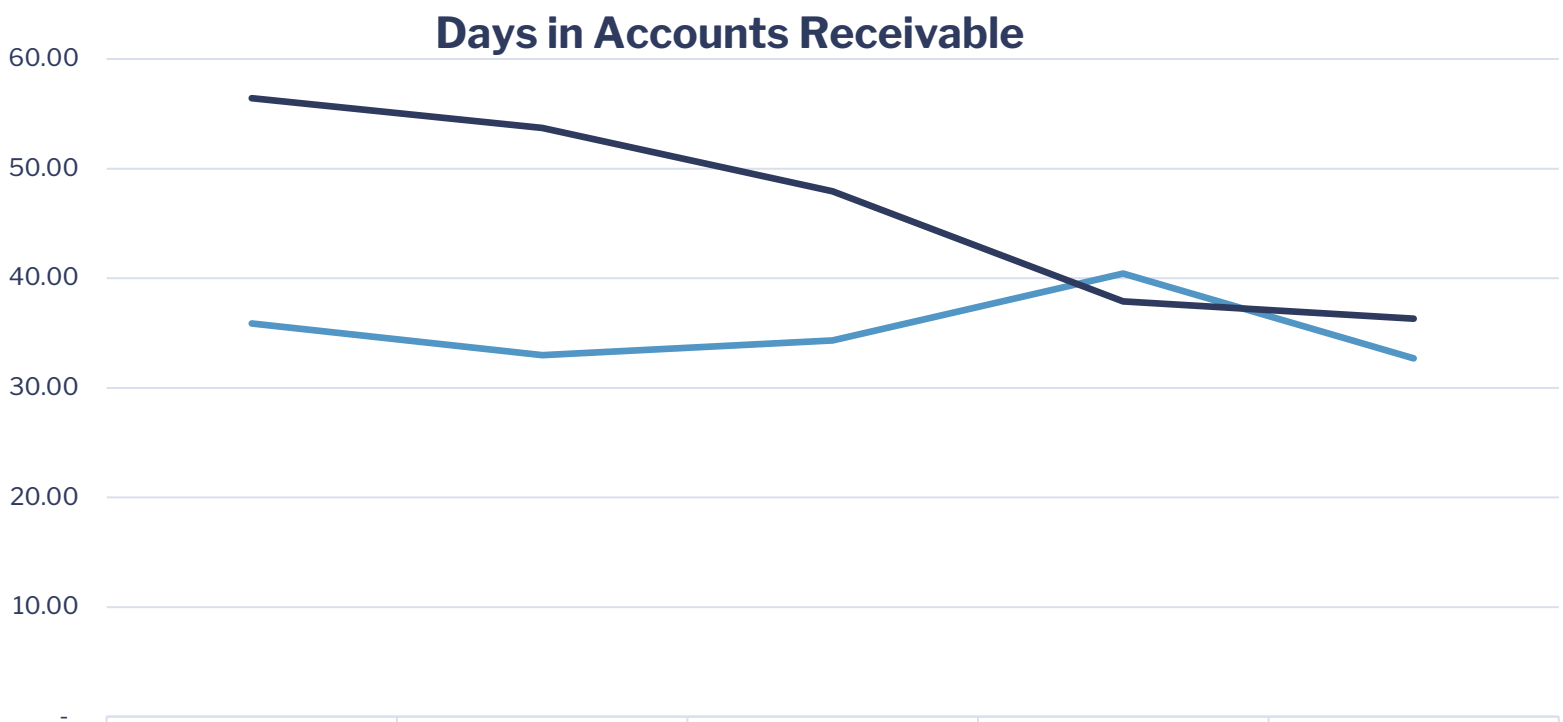


	2018	2019	2020	2021	2022
Average NP	2.40	2.64	2.71	3.19	2.73
Average GO	1.55	2.08	1.60	2.57	2.62

Long-term Debt to Net Assets

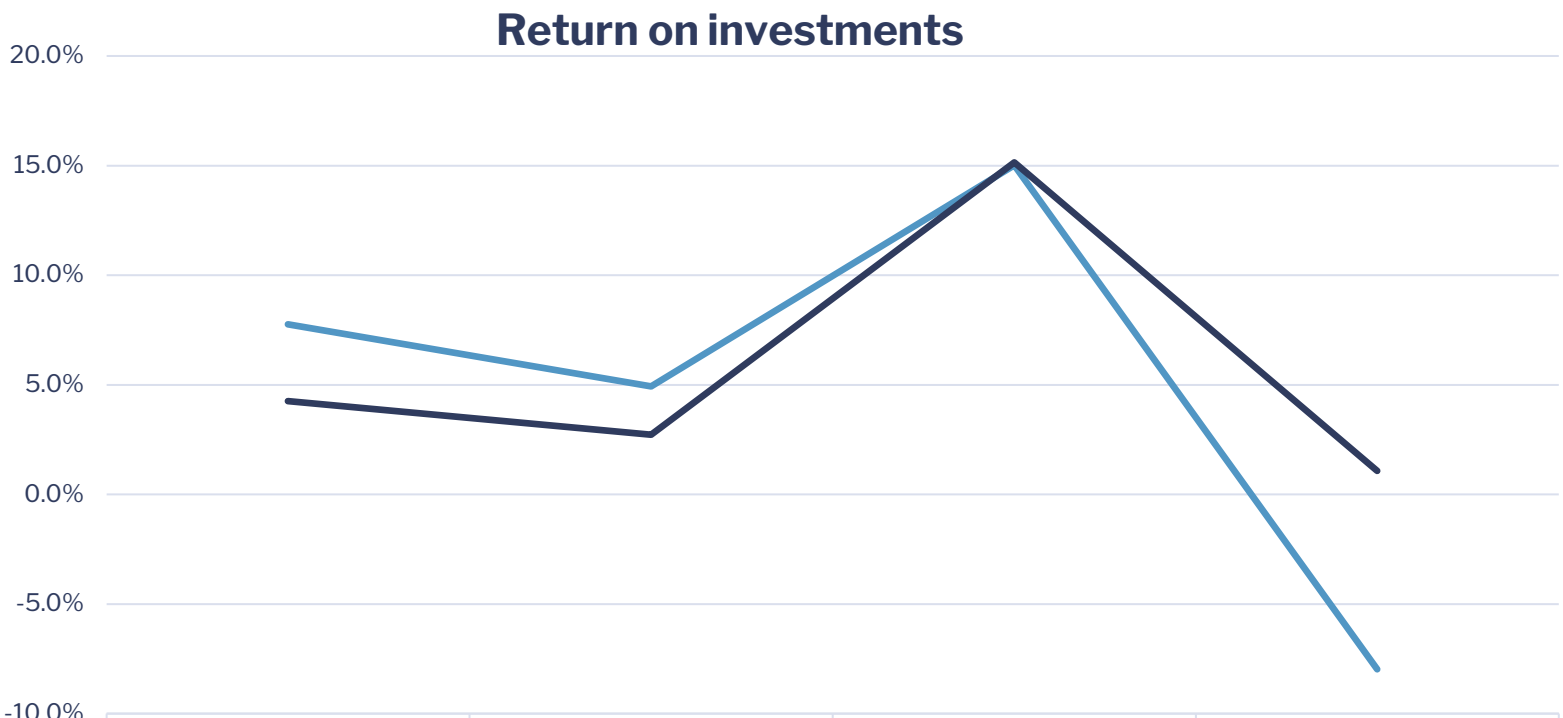


Days in Accounts Receivable



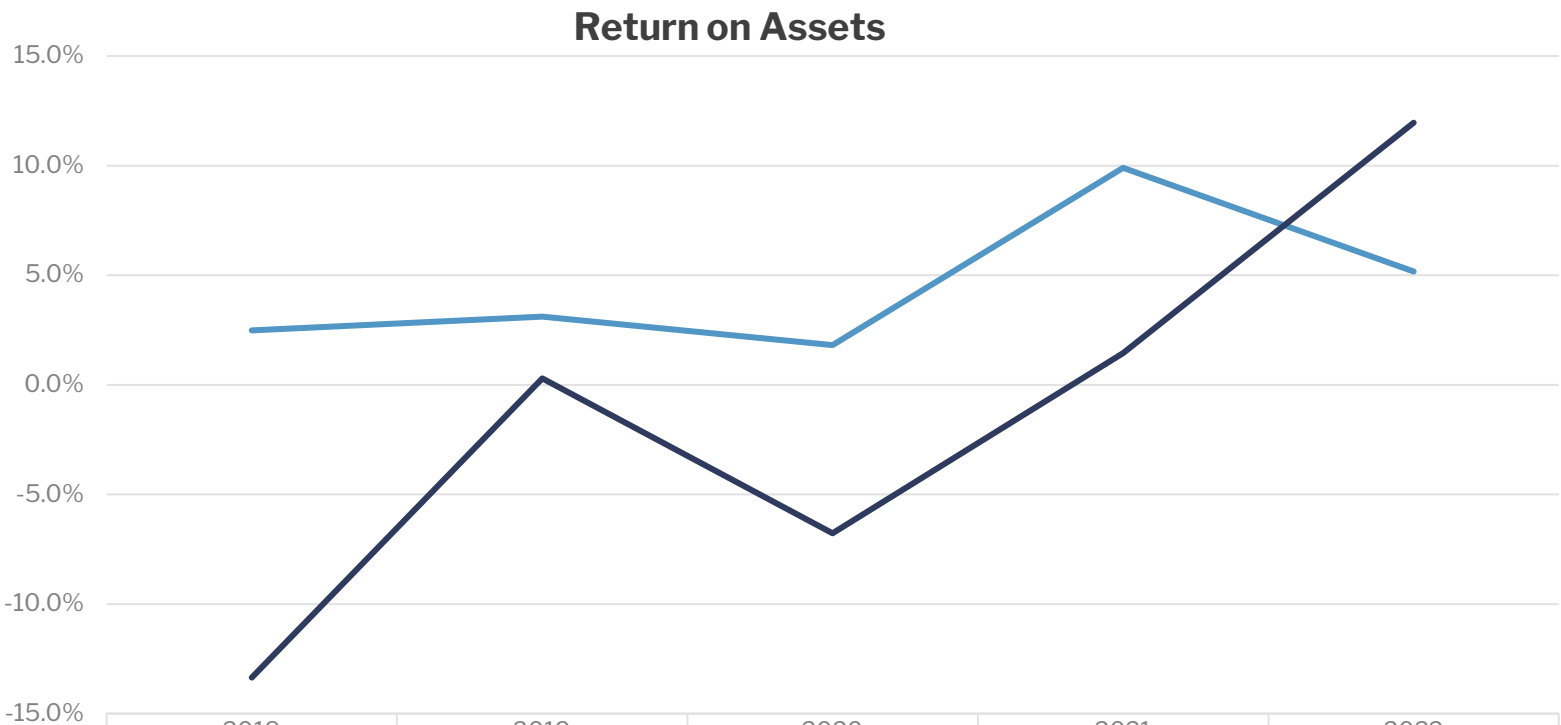
	2018	2019	2020	2021	2022
Average NP	35.88	32.99	34.31	40.42	32.70
Average GO	56.41	53.72	47.94	37.89	36.33

Return on Investments



	2019	2020	2021	2022
Average NP	7.8%	4.9%	15.0%	-8.0%
Average GO	4.3%	2.7%	15.1%	1.1%

Return on Assets



	2018	2019	2020	2021	2022
Average NP	2.5%	3.1%	1.8%	9.9%	5.2%
Average GO	-13.3%	0.3%	-6.8%	1.5%	12.0%

Thanks!

If you have any questions, please feel free
to contact us at
787-725-4545 or by e-mail at
info@galindezllc.com