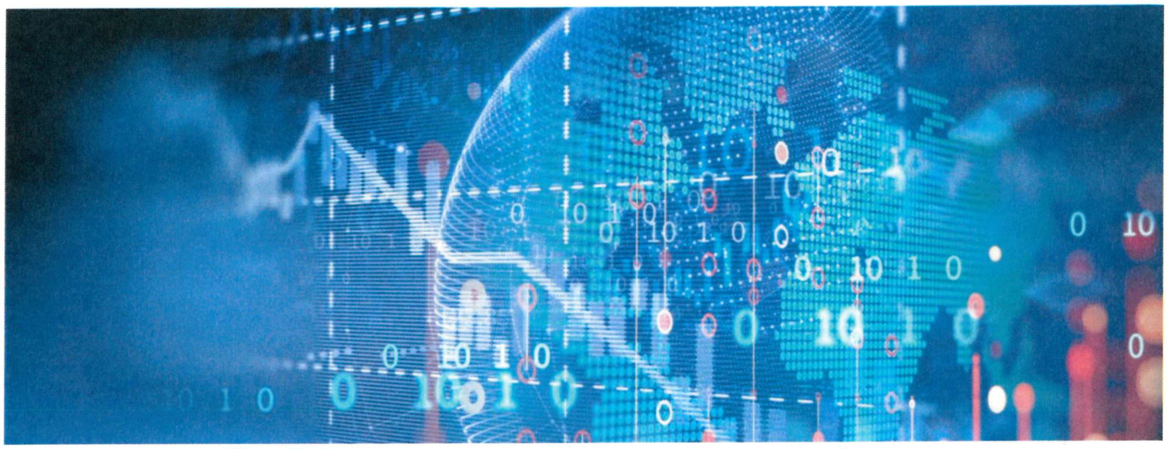


Integris.

City of Eden
IT Assessment Report

Presented to:

City of Eden
120 Paint Rock Street
Eden, TX 76837

Prepared by:

Tim Dickson, Account Executive
tim.dickson@integrisit.com

Ray Miculob, Solutions Architect
ray.miculob@integrisit.com

Date:

Monday, November 13, 2023

Assessment Overview

At Integris, we require all our incoming Empower clients to let us conduct a paid assessment before we start. Why? Because we believe it is the best way to ensure that the work that we do for you is focused, economical, and effective. With a single, comprehensive examination, you will ensure our engagement with you gets off to the right start, helping you:

- Spend wisely, eliminating errors and waste
- Reduce onboarding time
- Identify gaps and inefficiencies in your operations, before we begin
- Create a predictable infrastructure development timeline and budget
- Establish KPIs for your systems, to monitor its health and security

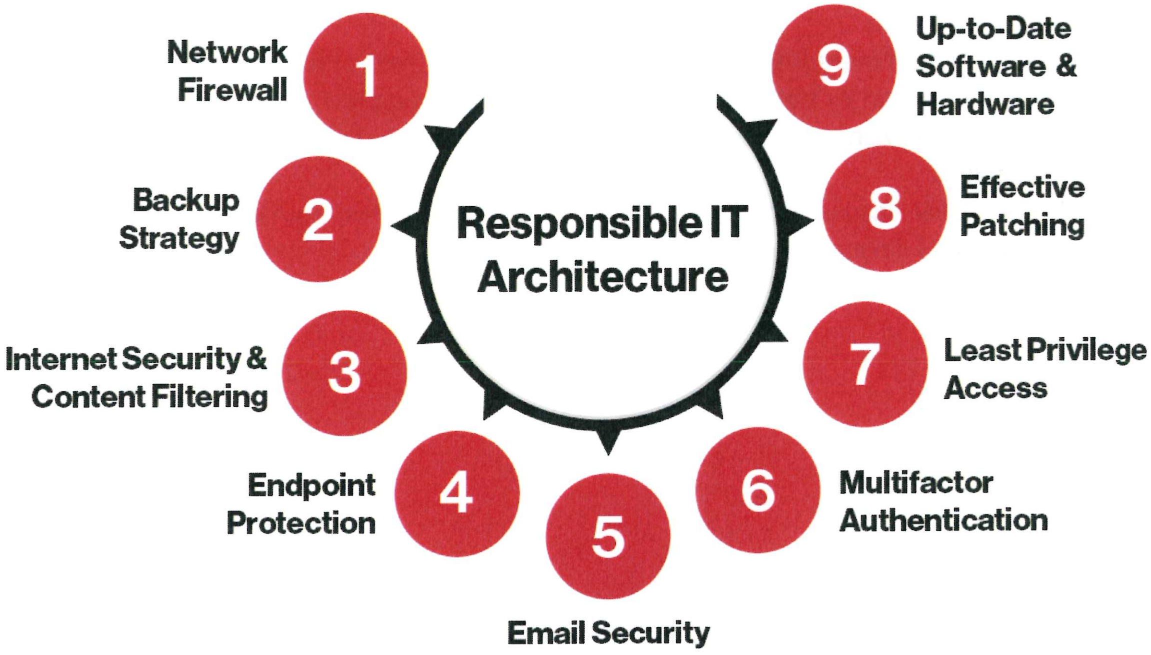
This ensures your systems are aligned with our Responsible IT Architecture.

Responsible IT Architecture

Responsible IT Architecture is our own term. But the idea behind it is simple. We believe that every Empower client should have a baseline of products that keeps their cybersecurity covered, and their productivity assured. Integris can deliver on that promise. The bottom line, however, is this—we will not work with clients unless we are working on a solid IT foundation. With our Responsible IT Architecture program, we strive to:

- Create a network of defense that catches hacks outside and inside your systems
- Create a platform that protects you against outages, disasters, and data loss
- Continuously patch, monitor, and remediate vulnerabilities in your system
- Qualify for cyber risk insurance
- Have proper authentications & access protocols
- Secure all your endpoints
- Install tools that filter and quarantine content
- Calibrate your backups to match your usage and data needs

Our assessment identifies the gaps in your systems and provides the solutions needed to bring your company into alignment.


Responsible IT Architecture
1
Network Firewall
2
Backup Strategy
3
Internet Security & Content Filtering
4
Endpoint Protection
5
Email Security
6
Multifactor Authentication
7
Least Privilege Access
8
Effective Patching
9
Up-to-Date Software & Hardware

The Assessment Process

Our assessment has covered all areas of your IT infrastructure, from your physical network, through your software/hardware assets, to your policies and partnerships. This document includes a gap analysis, a remediation plan, and an infrastructure roadmap and budget. We will help you set goals, and achieve them, so you can take your business to the next level.

What Our Assessments Cover

1. Onsite evaluation of inventory, secure configuration, and access of hardware devices on the network. To include, but not limited to:
2. Laptops, workstations, switches, firewalls, servers
3. Remote evaluation of inventory, secure configuration, and access of software on the network. To include, but not limited to:
4. Operating systems, line of business application, software licenses, remote access, backup & disaster recovery
5. Security software analysis to include, but not limited to, security information and event management (SIEM), internet content filtering, email security gateway, antivirus, multi-factor authentication (MFA), mobile device management (MDM), wireless access control

6. Dark Web Scan – provides organization with a report of your digital credentials on the dark web
7. Executive Summary Report with a list of gaps, risks, best practices, and solutions ranked by business impact (high, medium, and low) associated with each finding, using gap assessment methodology supported by N.I.S.T. framework
8. Vulnerability Assessment Reports including a Security Posture Assessment and Snapshot of Critical Information Security Risks.

Empower Assessment Findings

Our expert engineers have taken a thorough assessment of your entire environment. Feel free to review this document with your current IT provider or IT team and if you would like to take a deep dive into the technical pieces, we are more than happy to schedule a follow up call.

The following technology deficiencies have been discovered during our technology audit:

Business Impact – HIGH

Finding 1. Outdated Server Infrastructure

At the time of assessment, the organization's primary server experienced drive failures. An IT provider was able to recover the server using a secondary server that was already in hand. The secondary server is a Supermicro device that is antiquated and not under warranty.

It is highly recommended that the organization migrate the server's data and services to a new server that is under warranty.

Executive Summary: Mission critical systems and services should be running on platforms that are supported by manufacturer and have valid warranty, so in the event of failure organization has quick access to parts and services needed to bring failed system up.

Finding 2. Incomplete Backup and Disaster Recovery Strategy

At the time of assessment, the server was not being backed up. This puts the organization's critical data at risk. There were also no backups of M365.

As a short-term solution, it is recommended that we implement Integris backups for the server and for M365.

In the long term, the following should be considered:

- Review where critical data resides, what the backup strategy around it is, and how quickly data can be recovered and accessed in the event of disaster
- Ensure each critical data set is backed up and then replicated off-site
- Document recovery process along with RTO and RPO and communicate those metrics to stakeholders

- Create a process around testing existing backup strategy on regular basis and reporting on lessons learned
- Review existing backup retention and confirm if sufficient

Executive Summary: Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. These objectives guide enterprises to choose an optimal data backup plan for their business. Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance." The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity. In other words, the RTO is the answer to the question: "How much time did it take to recover after notification of business process disruption?"

Finding 3. Next-Gen Firewall Requires Follow-up

The FortiGate 30E is not the default gateway for the network. The Frontier modem is plugged straight to the switch and is acting as the default gateway, effectively nullifying the FortiGate's function as a gateway security device. Additionally, the 30E is 1 generation behind and possibly over 5 years of age.

It is recommended that an Integris next-generation firewall with gateway antivirus, content filtering and intrusion prevention/detection features be put in place to protect the organization's LAN.

Executive Summary: Next-generation firewalls have developed out of necessity in today's computing environments, where malware attacks have grown in sophistication and intensity and have found ways of exploiting weaknesses in traditional firewalls. Because the firewall is the first line of defense against such attacks, and protection of the corporate network is of the utmost importance, firewalls have evolved as well to meet modern day threats. Where traditional firewalls have failed is in their inability to inspect the data payload of network packets and their lack of granular intelligence in distinguishing various kinds of web traffic.

Because most network traffic uses web protocols, traditional firewalls cannot distinguish between legitimate business applications and attacks, so they must either allow all or reject all. As a result, next-gen firewalls have been developed to carry out advanced security functions without impacting the latency of the network. Next-gen firewalls can detect and analyze suspicious network patterns as well as decrypt HTTPS/SSL network traffic (approx. 70% of Internet traffic).

Finding 4. Missing Antivirus on Endpoints

Some of the endpoints had Comodo AV installed but there were a few that did not have any.

It is recommended that all endpoints have Integris' EDR solution in place.

Executive Summary: For desktops and laptops, where new viruses and virus outbreaks are most common, one of the main advantages of an enterprise AV system is the ability to manage the software and monitor from a central server. This allows for real-time alerting, updates, and the ability to apply the same configuration to all systems. Standalone systems can be highly effective in searching for and finding vulnerabilities. However, because of the lack of attention from IT administrators, this system may fail very quickly and lead to a compromised network.

Finding 5. Endpoints are not Protected by Internet Content Filtering System

Internet access is currently unrestricted and not monitored, which exposes end users to a wide variety of risks. It is recommended to deploy an intelligent Internet security and content filtering system to provide another layer of protection for all users in the office.

It is recommended to deploy an intelligent Internet security and content filtering system to provide another layer of protection for all users in the office and while outside the office.

Executive Summary: An Internet security and content filtering system enables the users of the network to enjoy the benefits of the Internet while remaining protected from inappropriate or harmful content. It also ensures productivity and maintains compliance for applicable business and regulatory requirements. The system allows for creating and deploying user specific policies, which will not only eliminate access to commonly restricted timewasters, but more importantly, protect users from malicious websites by blocking access to them.

Finding 6. Insufficient Email Continuity and Security

Organization uses M365 for its email needs and its built-in antispam system to ensure that no unwanted and vulnerable messages end up going to end user's mailboxes. Those built-in tools are often not sufficient to prevent phishing and other email related threats. It is recommended to employ a 3rd party email security gateway to inspect incoming and outgoing email for the organization.

It is recommended to deploy Integris Email Security for M365. We will also implement email encryption as this was a desired feature.

Executive Summary: Email remains the number one method of communication for most organizations. It is also the number one method used by cybercriminals to infiltrate your network, steal, or corrupt your data and damage your reputation. Methods of attacking email are growing more targeted, more sophisticated, and more dangerous. A secure email gateway is essential to protecting your business from malicious content contained within emails by preventing them from reaching their intended recipient. By placing malicious emails into quarantine or blocking the sender, a secure email gateway significantly reduces the number of successful compromises of user credentials, email hosts and sensitive company data. A secure email gateway offers a robust framework of technologies that protect against these email-borne threats. It is effectively a firewall for your email, and scans both outbound and inbound email for any malicious content. At a minimum, most secure gateways offer a minimum of four security features: virus and malware blocking, spam filtering, content filtering and email archiving.

Finding 7. Multifactor Authentication for M365 not Enforced

The organization's M365 environment is not enforced with multifactor authentication. This puts the organization's data at elevated risk.

It is recommended that MFA be enforced for all accounts.

Executive Summary: Multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multi-factor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and/or what the user is (biometric verification). The goal of multi-factor authentication is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Finding 8. Regular User Accounts with Administrative Rights

The PCs that were assessed did not have regular accounts as local admins. However, we found that a daily use M365 account is a global admin.

It is recommended that global admin accounts be separate accounts to mitigate security risks.

Executive Summary: An account with administrative access has the power to make changes to a system. Those changes may be for good, such as updates, or for bad, such as opening a backdoor for an attacker to access the system. While an administrator would hopefully not do anything nefarious to his/her company's systems purposefully, the act of using administrative accounts for daily activities can lead to just that.

Allowing a systems administrator, especially one with Domain Administrator privileges, to access his/her e-mail and the Internet via their administrative account makes it easier for attackers to introduce malware via a phishing attack or gain those credentials by using impersonation, which is a common attack in the Microsoft Windows environment.

Finding 9. Weak Patch Management Strategy

All Windows endpoints are configured with native Windows patch management. Patches are not tested before being deployed and there is no process in place. It is also clear that no other applications beyond the Windows operating systems are being patched on a regular basis (Java, Adobe, etc.), which could open serious security holes for the network.

It is recommended to implement Integris Patch Management to ensure endpoints are updated and secure.

Executive Summary: Patch management is a strategy for managing patches or upgrades for software applications and technologies. A patch management plan can help a business or organization handle these changes efficiently. Software patches are often necessary to fix existing problems with software that are noticed after the initial release. Many of these patches have to do with security. Others may have to do with specific functionality for programs. Proper patch management strategy includes all applications deployed in production environment and allows for deploying only patches that have been tested and approved by administrators.

Finding 10. Weak Password Management Strategy

Passwords for critical systems are kept in a binder.

It is recommended that passwords be kept in a proper password management system like LastPass or 1Password.

Executive Summary: A password management system is essential for both personal and business use. It is a software application designed to store and manage passwords securely, eliminating the need for users to remember multiple complex passwords.

Business Impact – MEDIUM

Finding 11. PC Life Cycle Management/Lack of Standardization

The organization has a mix of Asus and custom-built PCs. They are all running Windows 11 Pro and are domain joined. The warranty and age of these PCs are unknown.

It is recommended that critical PCs be under warranty and within 5 years of age to mitigate downtime.

Executive Summary: Standardizing PCs is crucial for businesses and organizations to ensure efficiency, cost-effectiveness, and compatibility. By establishing a standard hardware and software configuration, organizations can streamline their IT processes, reduce downtime, and minimize compatibility issues.

Standardization also simplifies IT management by allowing administrators to manage a consistent set of hardware and software across the organization. It facilitates software updates and maintenance, enabling administrators to apply updates across the organization simultaneously. Standardization also provides better security by ensuring that all systems have the latest security updates and patches.

In addition, standardizing PCs can result in cost savings due to bulk purchasing of standardized hardware and software. It can also reduce training costs for employees, as they only need to be trained on a single standard system, rather than multiple variations.

Finding 12. M365 Deployment Requires Follow-Up

Certain M365 hardening features are not in place. We recommend reviewing and remediating any discrepancies of the following items:

- External Banners
- Retention Policies
- Data loss prevention (DLP) policies
- Unified Audit Logging
- Mailbox Audit Logging
- Secure accounts not accessed in last 30 days

It is recommended that the existing configuration be reviewed and remediated to ensure it aligns with industry best practices and/or any compliance requirements that the organization may have.

Executive Summary: In Microsoft 365, there are currently close to 1000 security options and switches that should be reviewed at the time of implementation and then on a regular basis to ensure compliance with organizations policies and desired security posture. It is often assumed that security is enabled by default with cloud applications, but that is unfortunately an incorrect assumption.

Finding 13. Network Infrastructure Requires Follow-Up

The Netgear GS724T switch is end of life as of 9/2023. The Unifi wireless access points are installed behind a printer and low to the ground which is not optimal.

It is recommended that the switch be replaced to ensure uptime. The Unifi access points should be mounted up high and not behind objects that can obstruct wireless signals. Consider replacing the Unifi APs as well as the age of the existing ones is unknown.

Executive Summary: Business-class switches and wireless access points offer distinct advantages for organizations seeking robust and efficient network solutions. Business switches excel in reliability, scalability, and advanced management, supporting features like VLANs, QoS, redundancy, and heightened security measures. They are tailored for demanding network environments, ensuring consistent performance, and accommodating expansion needs. In contrast, business-class wireless access points provide superior coverage and capacity, accommodating a larger number of concurrent users and offering dual or tri-band support for reduced interference. These access points often come with centralized management capabilities, advanced security features, and seamless roaming to enhance network efficiency and security. Overall, business-class switches and wireless access points are essential for organizations requiring high-performance, scalable, and secure networking solutions.

Businesses opting for these solutions benefit from enhanced network performance and reliability, enabling efficient data handling and minimizing downtime. Moreover, the advanced management features empower administrators to configure and monitor networks effectively, while the robust security measures protect against unauthorized access and threats. With a focus on scalability and seamless integration, business-class switches and wireless access points are ideal choices for organizations seeking resilient, high-performing networking infrastructure to support their growing needs and ensure uninterrupted operation.

Finding 14. Information Security Officer

The organization does not have a clearly defined responsibility for information security. Depending on the firm's long-term strategy and resources, it is recommended to either bring Chief Information Security Offices on staff or engage with consulting firm to provide ongoing oversight and leadership for information security.

Executive Summary: In the rapidly evolving world of cybersecurity, installing a firewall and having a staff meeting about phishing emails isn't going to cut it anymore. Federal regulations like HIPAA, EU GDPR, NYDFS clearly outline the minimum-security requirements all businesses need to comply with to be considered secure. To remain compliant, your business needs policies and procedures in place that go way beyond a firewall. A Chief Information Security Officer (CISO) understands these regulations and how they apply to your business and technology infrastructure.

Business Impact – LOW

Finding 15. Internet Redundancy

The organization has 1 cable internet circuit from Frontier. **It is recommended** that redundant Internet connections be put in place to mitigate downtime.

Executive Summary: Due to the ever-increasing reliance on the internet, many businesses have implemented or are considering a secondary, redundant internet connection. Having a failover is particularly important if your voice traffic flows through your internet connection and if most of your mission critical business applications are cloud-based. Internet service is less expensive than ever. A second internet connection, a router with the right capabilities and some configuration time is inexpensive insurance against an event that could bring the productivity of your employees to a grinding halt.

Finding 16. Information Technology Governance Needs Follow-Up

It has been noted that the organization does not have policies or may have policies that are out of date that define processes and procedures around IT management, i.e., change management policy, user account management policy, incident response policy, remote access policy, etc. This could create confusion and inconsistent results across the organization, but also puts the organization in a potentially non-compliant position with certain regulations. Your assigned Integris vCIO can work with the organization to create or update these policies.

Executive Summary: IT governance provides a structure for aligning IT strategy with business strategy. By following a formal framework, organizations can produce measurable results toward achieving their strategies and goals. A formal program also takes stakeholders' interests into account, as well as the needs of staff and the processes they follow. In the big picture, IT governance is an integral part of overall enterprise governance.

Finding 17. End User Education Program – Human Firewall

Organization does not have a program or process to educate its users about existing and upcoming cybersecurity threats.

It is recommended to engage an automated system to train users via a series of mandatory videos and randomized follow up exercises, i.e., phishing campaigns.

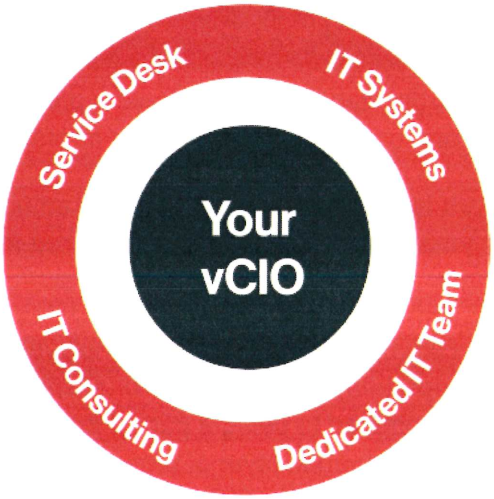
Executive Summary: The definition of a human firewall is straightforward. It is a commitment of a group of employees to follow best practices to prevent as well as report any data breaches or suspicious activity. The more employees you have committed to being a part of the firewall, the stronger it gets. The importance of this added human layer of protection lies in the fact that many breaches are due to employee error. Software, too, makes mistakes, i.e., sometimes allowing phishing messages through or red-flagging real communications. Therefore, it is felt that the vigilant human can see potential hazards software misses and can prevent errors from being made. However, to have your firewall be as successful as possible, it is important to ensure there is a system in place to support it.

Empower your team with the right technology.

To provide a complete and effective IT team for our clients, Integris has developed a unique approach that gives our Clients the best possible experience – the Empowered Approach.

Integris' Empowered Approach is a great fit for any client without IT staff, who is looking for a mature and reliable IT support partner, so the organization can stay focused on running a successful business. When engaged, Integris proactively manages client's IT infrastructure, supports all end users, and prevents downtime that can impact Client's business and productivity.

The Empowered Approach is divided into four service areas: Service Desk, IT Systems, IT Consulting, and a Dedicated IT Team, overseen by an Integris virtual Chief Information Officer (vCIO), who provides advice on best practices and strategy.



Service Desk

Our Service Desk is responsible for providing network, server and computer support to our clients and their end users. This includes unlimited phone and remote support. Onsite support is available for any issues that cannot be resolved remotely. Options to extend coverage for companies in multiple time zones and specialized use cases are available.

In addition, Service Desk includes:

- Incident Tracking & Ticketing – each service request is logged and tracked in our ticketing system
- Technology Vendor Management:
  - Internet service provider
  - Phones
  - Printers
  - Line of business applications

IT Systems

IT Systems is responsible for keeping the entire Information Technology environment up and running, secure, and backed up. All of that is being monitored 24x7x365 and includes:

- Network and system monitoring
- Patch management
- Backup management (for Integris backup systems)

Dedicated IT Team

Your Dedicated IT Team is focused on proactive maintenance of your environments. They complete proactive network maintenance and regular inspections of your technology environment to verify its stability, security, and performance as well as alignment with industry best practices. That also includes:

- Thorough documentation of environment
- Confirm Integris' standards across all systems
- Deep understanding of line of business applications
- Understanding of company, users, and technology goals

IT Consulting

In a competitive business environment, organizations that take a strategic approach to technology are best able to overcome competitive pressures, surmount technology challenges, and foster lasting success.

We provide technical leadership and direction for operational improvements to streamline your business and fuel growth. Our team will assist with purchasing, the creation and review of annual IT budgets, sharing thought leadership, and so much more. Integris's vCIO service will be led by a Senior Engineer with the business acumen to lead your company's long-term technology initiatives. Your vCIO will proactively work with the point of contact to assess security, risk, and productivity so your organization is getting the most out of every dollar spent on IT.

- Formulate strategic IT goals
- Plan the IT budget
- Plan disaster recovery and business continuity
- 3rd party technology research and software evaluations and consultation
- Analyze, and rework business processes related to IT
- Facilitate technology change
- Regularly schedule technology business reviews

Monthly Managed IT Service Solutions

Summary:

Empower+ Managed IT Services with Responsible IT Architecture Remediation Project

Total Monthly Fee: **$2,828.83** Total One-Time Investment: **$18,074.00**

Empower Managed IT Services with Responsible IT Architecture Remediation Project

Total Monthly Fee: **$2,313.83** Total One-Time Investment: **$18,074.00**

**Financing options are available for the one-time investment over 36 months. Please let us know if you would like more information.*

Option #1: Empower+

Empower+ combines the local presence and expertise of our engineers and vCIOs with our always-on help desk and ticketing system. Our team truly becomes a part of your team. You can review our full service schedule here.

- New user setup as per Integris defined checklist/process
- Departing user termination as per Integris defined checklist/process
- New desktop/laptop computer setup (if hardware purchased from Integris as per Integris defined new computer setup checklist/process)
- Technology vendor management (copier company, ISP, etc.)
- Integris' standard network documentation
- Access to on-call team outside of business hours (after hours support billed on hourly basis)

Up to 13 computers included

- Each additional computer - $155.00
- Desktop related issues are covered M-F between 8:00 AM to 6:00 PM
- Guaranteed critical system down event response time – 4 hours

Up to 1 network included

- Each additional network - $475.00

Regularly scheduled proactive on-site visits

Access to on-call team for after-hours support - $195/hour x 1.5, upon receiving approval from client

36 – month commitment

Option #2: Empower

Empower includes all the expert monitoring, strategic management, and services you need, without the onsite services you may not need. It is a perfect solution for companies that are remote, or whose physical infrastructure footprint is minimal. You can review our full service schedule here.

- New user setup as per Integris defined checklist/process
- Departing user termination as per Integris defined checklist/process
- New desktop/laptop computer setup (if hardware purchased from Integris as per Integris defined new computer setup checklist/process)
- Technology vendor management (copier company, ISP, etc.)
- Integris' standard network documentation
- Access to on-call team outside of business hours

Up to 13 computers included

- Each additional computer - $115.00
- Desktop related issues are covered M-F between 8:00 AM to 6:00 PM
- Guaranteed critical system down event response time – 4 hours

Up to 1 network included

- Each additional network - $475.00

On-site support billed on hourly basis at reduced rate – $195/hour, upon receiving approval from client

Access to on-call team for after-hours support – $195/hour x 1.5, upon receiving approval from client

36 – month commitment

Responsible IT Architecture Remediation Plan. The following includes the Business Impact High Findings that require immediate attention.

- Finding 1 – Server Upgrade
- Finding 2 – Backup and Disaster Recovery
- Finding 3 – Next Generation Firewall
- Finding 4 – Integris EDR
- Finding 5 – Integris Internet Security
- Finding 6 – Integris Email Security
- Finding 7 – Integris MFA
- Finding 8 – Admin Rights Remediation
- Finding 9 – Patch Management
- Finding 10 – Password Management

Finding	Monthly Subscriptions	License/hardware	Labor
1	$0	$10,300	$6,084
2	$593	$0	$1,900
3	$84.33	$150	$950
4	$38.50	$0	$1,950
5	$21	$0	$1,950
6	$56	$0	$950
7	$21	$0	$1,950
8	$0	$0	$780
9	$0	$0	$780
10*	$0	$0	$780
Remediation Subtotal	$813.83	$10,450	$18,074
Empower	$1,500	-	-
TOTAL	$2,313.83	$10,450	$18,074

IT Assessment Solutions

***Please note** that the following is a line-item breakdown of projected costs for each of the 17 findings. The applicable costs for Findings 1-10 (Business Impact High) are reflected in the total monthly and total one-time costs listed on page 18.*

1. Build new server and migrate data and services. (Finding 1)
   - **Estimated costs**
     - $10,300 in server hardware, UPS, and Windows licensing
     - $6,084 for installation and configuration
2. Implement backups for servers and M365 (Finding 2)
   - **Estimated costs**
     - $565/month for Integris BDR Platform
     - $28/month for Integris M365 Backups
     - $1,900 in labor to deploy
3. Install and configure Integris Empower Firewall (Finding 3)
   - **Estimated costs**
     - $84.33/month for Integris Empower Firewall
     - $150 for rack mount kit
     - $950 to install and configure
4. Install and configure Integris EDR (Finding 4)
   - **Estimated costs**
     - $38.50/month for Integris EDR
     - $1,950 in labor to deploy
5. Implement cloud hosted Internet Security and Content Filter (Finding 5)
   - **Estimated costs**
     - $21/month for 7 endpoints
     - $1,950 installation and configuration
6. Configure and deploy Integris Email Security (Advanced) (Finding 6)
   - **Estimated costs**
     - $56/month for 7 M365 accounts
     - $950 in labor to deploy Email Security and Encryption

7. Deploy Integris MFA (Finding 7)
    - **Estimated costs**
        - $21/month for 7 accounts
        - $1,950 in labor
8. Review and remediate local admin rights (Finding 8)
    - **Estimated costs**
        - $780 in labor
9. Implement managed Windows and other 3rd party software updating strategy for all desktops, laptops, and servers. (Finding 9)
    - **Estimated costs**
        - $780 installation and configuration

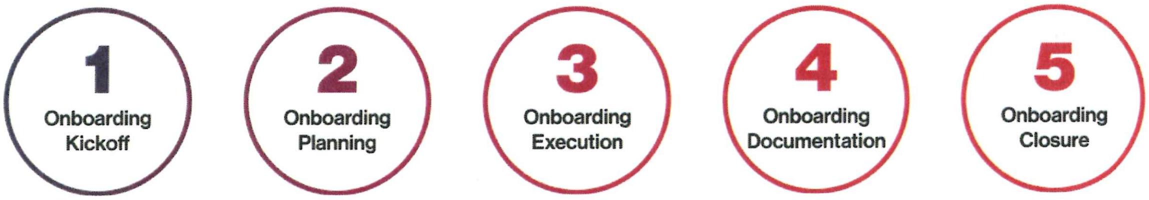
    ***Note**: Patch management is included in Empower solution at no additional charge (installation and configuration charge still applicable)*
10. Implement password management system (Finding 10)
    - **Estimated costs:**
        - $780 to assist with implementing password management system

    ***Note**: Cost of Password Management app not included.*
11. Phased replacement of PCs (Finding 11)
    - **Estimated costs**
        - $1,500 average cost of PCs
12. M365 Hardening (Finding 12)
    - **Estimated costs**
        - $780 in labor
13. Replace switch and replace/mount APs in ideal locations (Finding 12)
    - **Estimated costs**
        - $1,400 in switch and AP hardware costs (1 each)
        - $780 installation and configuration

      ***Note**: May need assistance from low voltage vendor to install new AP drops*
14. Deploy Integris vCISO services (Finding 14)
    - **Estimated costs**
        - $3,450/month

15. Configure secondary Internet connection (Finding 15)
    - **Estimated costs**
        - $300-$500/site for extra Internet connection
        - $1,170 in labor to configure and test failover/failback
16. Engage vCIO to assess vendors (Finding 16)
    - **Estimated costs**
        - Included with Empower agreement
17. Configure and deploy Security Awareness Training (Finding 17)
    - **Estimated Costs**
        - $350/month for up to 25 users
        - $1,450 in labor to deploy

Onboarding



The transition period is typically 30 days and includes collaboration with your current provider for the knowledge transfer of all IT systems details and credentials.

We recommend you continue service with your current provider during this time. This overlapping approach makes the transition more seamless.

Plus, the incumbent IT provider will be more likely to cooperate with account transfer details if your account is still active.

Key onboarding details cover:

- Introduction to your vCIO, Technical Operations Manager, and Project Manager at the Client Kick-off Meeting.
- Review contracted services and transition details.
- Deploy Integris remote monitoring and management tools.
- Explain how to contact Integris' support team

- Swiftly remove the highest priority risks and create a future-focused technology roadmap.
- Review and schedule remediation project to implement Responsible IT Architecture controls and address other findings highlighted in the assessment report.
- Document all critical systems, including new user setup checklist and new computer setup process
- Secure the environment and ensure that only Integris has access to the network after all systems have been documented.

Our top-notch project coordination ensures that your team knows exactly when to expect down time, transition day-to-day end user support, the impact on the business while the onboarding is being implemented and what the overall timeline is for each step of the project.

Exclusions

- Parts, equipment, or software not covered by vendor or manufacturer warranty or support.
- Costs to bring the Client's environment into compliance with Client Infrastructure Standards
- Costs of any parts, equipment, shipping, or courier charges
- The cost of any software, licensing, software renewal, or upgrade fees
- The cost of any 3rd Party Vendor or Manufacturer Support or Incident Fees
- Services and Repairs made necessary by the alteration or modification of equipment other than authorized by Service Provider including hardware or software installations or configuration changes made by Client or Client authorized third party
- Failures due to acts of God, building modifications, power events (outage, surge, brownout), or other adverse environmental conditions
- Programming (modification of software code) or troubleshooting of 3rd party addon applications and/or plug-ins
- Support and maintenance of proprietary and custom software applications
- Website, software, SharePoint design, development, and hosting services
- Costs related to any audit or legal proceedings including discovery, subpoenas, court ordered actions
- Employee-owned laptops and PCs or any device not explicitly covered under an Integris' agreement
- Incident Response and remediation for cyber security/data breach and/or a major system vulnerability (which would not be addressed by regular patching process)
- Requests for training outside of those services explicitly offered by Integris
- Security cameras/CCTV installation or maintenance

- Environmental moves (building moves, remodels, internal relocations)
- Travel time and costs outside of 50-mile radius from Integris' office assigned to support the client.

Term, Service Pricing, and Billing Summary

- The term for the service is 36 months unless otherwise specified in the Service Order.
- The term will automatically renew for a 12-month term thereafter.
- Minimum pricing and baseline quantities are defined on the initial service order
- [Empower or Empower+] is billed monthly per endpoint (desktop, laptop, or server - physical or virtual) and per network (physical or virtual)
- [Empower or Empower +] is audited monthly. Endpoints and networks outside of quantities defined in initial service order will be billed in addition to baseline monthly fee at specified price (per endpoint and per network) and billing will align with counts at the time of the audit.
- [Empower or Empower +] is billed a month in advance and payment is expected within 15 days from the invoice date (NET15)
- The first invoice covers two (2) billing periods – the first month of service and second month billed in advance.
- First month is billed depending on actual day when services started:
    - 1 – 8th day of the month – Integris will invoice for a 100% of monthly fee
    - 9 – 23rd day of the month – Integris will invoice for 50% of the monthly fee
    - 24th – last day of the month – Integris will not invoice for services rendered that month
- Monthly charges begin the day after initial implementation is completed (the minimum required for Integris to effectively provide support to and monitor client's environment). Initial implementation is completed at the time Integris deploys support agents to at least 75% of client's endpoints.
- Invoices are processed and delivered on or about the 1st of each month.
- Empower is a subject to annual price increase of CPI (Consumer Price Index) + 2%

Integris Master Service Agreement and Integris Full Terms and Conditions
Should you decide to become a client, these two documents will be reviewed in detail.

Our Team is Your Team

At Integris, we are on a mission to bring together the personal service of local IT providers with the power of a national network.

We believe that is simpler than it sounds. Our offices offer high-touch IT services that clients love from highly experienced local team members. Our national network allows us to offer best-in-class services like dedicated vCIOs, specialized security and compliance advisory services, and more.

Our name, "Integris," stands for integrity. And it is something we aim to deliver, every day.

Our values

People first
Integris is powered by people, so it is important we do not get wrapped up in the wires. Our people always come first.

Do the right thing
Our name is rooted in integrity. It is the heart of how we run the business and guides everything we do.

Get it done right
A single checkbox can make or break our business. No detail is too small. We want to make it right.

Own it
Every team member owns their part. We take responsibility for our clients and hold each other accountable. Success is in the numbers.

Your Local Integris Leadership

Our local leadership team of managing director, strategic operations manager and technical operations manager focus on building long-lasting, trustworthy partnerships with our clients. Check out your local team's page on our website: https://integrisit.com/locations/

Mark Blalack
Managing Director

Amy Calcich
Strategic Operations Manager

Holly Connor
Technical Operations Manager

Integris in Your Community

Girl Scouts of Texas

Austin, TX

Girl Scouting builds girls of courage, confidence, and character, who make the world a better place.

Any Baby Can

Austin, TX

We are a proud sponsor of Any Baby Can. Their mission is to build, develop and nurture families to unlock each child's full potential. They are a non-profit organization in Austin we have sponsored and supported.

References

Gunze Electronics

JD Morgan
Phone: 512-413-6991
Email: Jmorgan@gunzeusa.com
Website: https://www.gunzeusa.com/

Watkins Insurance Group

Herschel Cone
Office: (512) 452-8877
Email: hcone@watkinsinsurancegroup.com
Website: https://watkinsinsurancegroup.com/

Any Baby Can

Albert Ruiz
Phone: 973-665-9100
Email: Albert.ruiz@anybabycan.org
Website: https://anybabycan.org/

Claire Reiswerg

Sand 'N Sea Properties
Phone: 409-7975501
E-Mail: clairea@sandnsea.com
Website: https://www.sandnsea.com/

Testimonials

Visit Clutch for detailed, multi-faceted reviews, conducted by analysts who personally interview Integris clients by phone.

Clutch's formal process includes business entity verification, payments and legal filings, and financial verification.

Clutch analysts solicit highly structured feedback by asking each Integris client the same five questions:

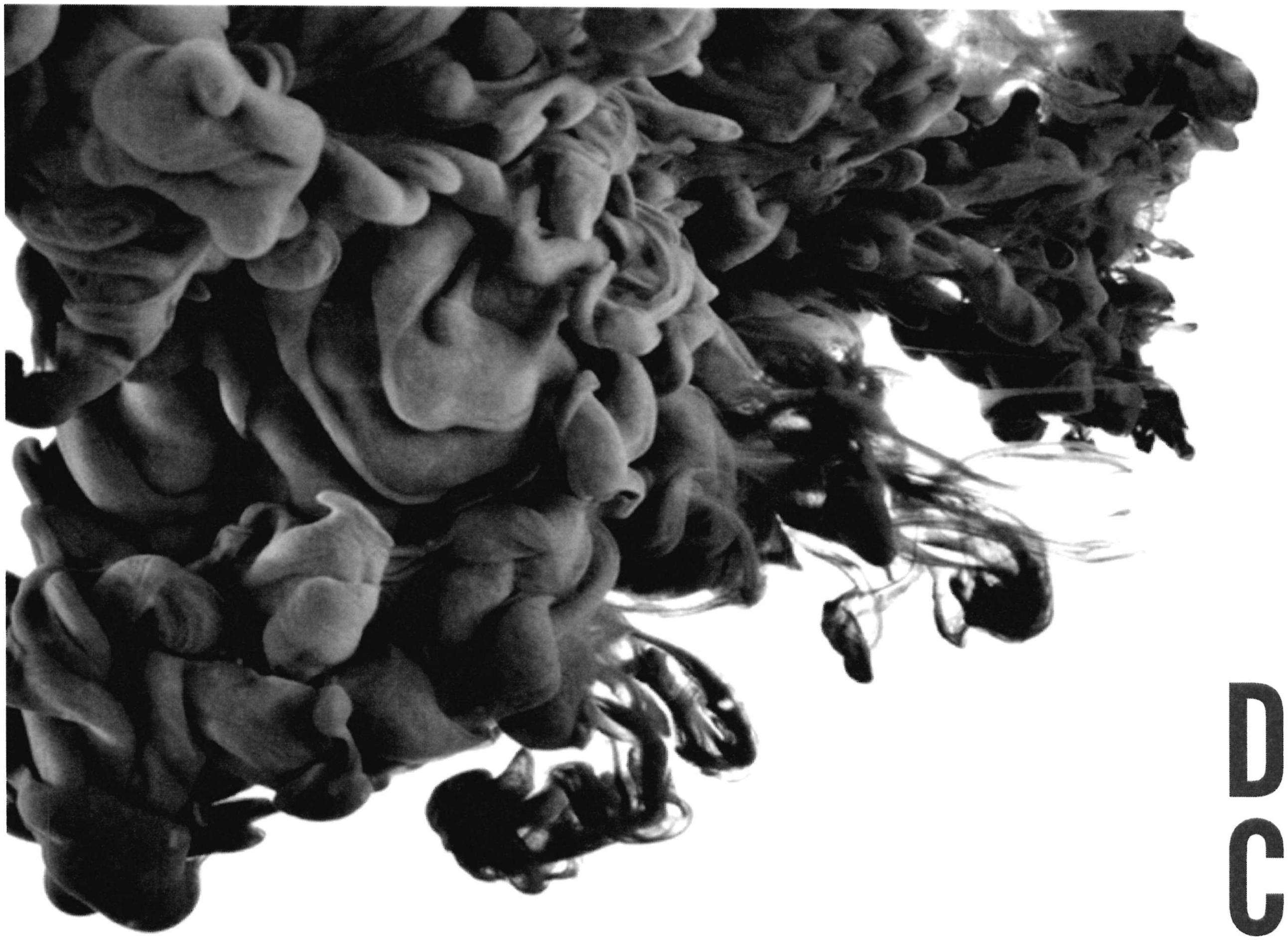
- What evidence can you share that demonstrates the impact of the engagement?
- How did Integris perform from a project management standpoint?
- What did you find most impressive about them?
- Are there any areas they could improve?
- Do you have any advice for potential customers?

"I have been a customer for more than a decade. Integris is an example of the way Managed Services should be done. We will continue to be a customer for years to come."

Chris Ragland
Partner & CEO
Ragland Realty & Management
AUS

Integris' biggest impact for CentraSol is they give us peace of mind! If something goes wrong, we have someone knowledgeable in all aspects of IT. The amount of work they put in to make sure their clients are not left behind, no matter how big or small, is something not all IT services do.

Mike Johnson
President
CentraSol
FTW



DARKWEB ID

DARK WEB COMPROMISE REPORT

Prepared for @edentexas.com

Nov 14, 2023

OF EXPOSED CREDENTIALS FOR YOUR COMPANY

34

EXTERNAL THREAT INTELLIGENCE

Are you monitoring for compromised data that can be used to exploit your business?

□ Yes □ No

DATA BREACH & PRIVACY LAW COMPLIANCE

Do you have a compliant data breach response plan in place?

□ Yes □ No

YOUR INFORMATION IS ALREADY EXPOSED

This information is used to compromise your corporate services such as: Office 365, payroll services, VPNs, remote desktops, banking, VOIP, ERP, CRM, social media access, ID Theft.

DARKWEB ID

WE IDENTIFY

COMPROMISES
Throughout your organization.

WE MONITOR

24/7/365

- Hidden chat rooms
- Private websites
- Peer-to-peer networks
- IRC (Internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

WE REPORT

80,000+
Compromised emails daily.

Certified in Dark Web Monitoring

Most Recent 34 Compromises

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
09/21/23	cityadmin@edentexas.com		id theft forum	Data Breach	eye4fraud.com	6
08/07/23	golf@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	5
08/07/23	cindy_adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	5
08/06/23	cindy_adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	4
02/28/23	Cindy_Adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	6
02/28/23	golf@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	5
01/06/23	econdev@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	3
01/05/23	estellaalba@edentexas.com	life*****	id theft forum	combolist	Not Disclosed	None
05/07/22	golf@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	4
05/06/22	golf@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	5
04/07/22	estellaalba@edentexas.com	8e50*****	id theft forum	combolist	Not Disclosed	None
12/15/21	cindy_adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	4
11/13/21	cityadmin@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	4
11/11/21	cindy_adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	6
11/08/21	cindy_adams@edentexas.com		id theft forum	Not Disclosed	Not Disclosed	6
07/14/21	utilityclerk@edentexas.com		id theft forum	Data Breach	Not Disclosed	4
07/14/21	econdev@edentexas.com		id theft forum	Data Breach	Not Disclosed	4
02/12/21	econdev@edentexas.com	pepp*****	id theft forum	combolist	Not Disclosed	None
07/29/20	cityadmin@edentexas.com		id theft forum	Data Breach	apollo.io-july2018	2
07/29/20	cityadmin@edentexas.com		id theft forum	Data Breach	apollo.io-july2018	3
07/29/20	econdev@edentexas.com		id theft forum	Data Breach	apollo.io-july2018	3
11/25/19	utilityclerk@edentexas.com		id theft forum	Data Breach	profileinformationfrompeopledatalabs(pdl)andoxydata.io	2

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
11/25/19	econdev@edentexas.com		id theft forum	Data Breach	profileinformationfrompeopledatalabs(pdl)andoxydata.io	2
10/29/19	econdev@edentexas.com		id theft forum	Data Breach	sharethis.com-contentmanagementplugins	1
10/28/19	cityadmin@edentexas.com		id theft forum	Data Breach	canva.com	1
09/22/19	econdev@edentexas.com	pepp*****	id theft forum	combolist	Not Disclosed	None
03/23/18	econdev@edentexas.com	kate*****	id theft forum	combolist	Not Disclosed	None
02/04/17	estellaalba@edentexas.com	8e50*****	id theft forum	Data Breach	elance.com	6
01/27/17	estellaalba@edentexas.com	este*****	id theft forum	combolist	Not Disclosed	None
12/27/16	utilityclerk@edentexas.com	jose*****	id theft forum	combolist	Not Disclosed	None
06/29/16	estellaalba@edentexas.com	0x8E*****	social media	Data Breach	myspace.com	1
06/09/16	econdev@edentexas.com	5cb8*****	social media	combolist	linkedin.com	None
06/09/16	utilityclerk@edentexas.com	a028*****	social media	combolist	linkedin.com	None
11/11/13	econdev@edentexas.com	CDup*****	Dark Web Site	combolist	adobe.com	None

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

DARKWEB ID

HOW ARE CREDENTIALS COMPROMISED?

PHISHING

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLES

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACKS

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

39%

Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500

Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

$1 - $8

Typical price range for individual compromised credentials

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.