Cloud Migration Best Practices

Practical Guidance for Sole Practitioners and Small Accounting Firms

September 2019

by Benjamin R. Podraza, CPA, CGMA
CEO | KYNEKTYD

Executive summary

This white paper outlines best practices for sole practitioners and small accounting firms migrating to remote work environments using Microsoft technologies.

It outlines basic protocols and procedures that use cloud technologies to:

- Improve the value of services to clients
- Improve productivity and employee morale
- Secure client data with minimal effort

The intended audiences for this white paper include:

- Sole practitioners and accounting practice leaders looking for guidance on how to increase productivity and preserve client confidentiality in a distributed work environment
- Cybersecurity researchers and professionals interested in practical applications of digital technologies to secure sensitive data

Disclaimer

This document is for informational purposes only. KYNEKTYD MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided “as-is.” Information and views expressed in this document, including URL and other internet website references may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Kynektyd or Microsoft product. You may copy and use this document for your internal, reference purposes.

The information and any opinions expressed in this material do not represent official pronouncements of or on behalf of Kynektyd, Microsoft, the AICPA, CIMA, or the Association of International Certified Professional Accountants. This material is offered with the understanding that is does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date this publication has been released, no guarantee is or can be given regarding the applicability of the information found within to any given set of facts and circumstances. Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this white paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Contents

Prelude

Starting the journey and walking the path

It’s easy to get lost in discussions about automation, cloud computing, big data, blockchain, AI, cybersecurity, and the plethora of other digital transformation clichés that are being thrown around, without ever arriving at an actionable step.

This paper helps accounting professionals overcome that challenge.

BEN PODRAZA
CEO | KYNEKTYD

Let’s start with a hard truth. Digital transformation is going to adversely impact some of the revenue streams that accounting firms currently enjoy. It is prudent for every organization to look at where technology can create a return-on-investment, and tasks that are rules-based and highly-repetitive are good candidates for automation. That represents a good portion of what many accounting firms are currently getting paid to do – i.e. the billable hour — or is it?

Public policy debates surrounding automation have been dominated by the impact on jobs, and we believe this fear-mongering is clouding perceptions. The disruption can be unsettling at first, but most professionals quickly take comfort knowing that their clients have never been buying hours. Accounting firms sell information, and that service will continue to have enormous value. This is not the first wave of change the profession has faced, and we are confident it will not be the last — it will survive.

Embrace automation. It is going to become hard to find human beings willing to do these mundane tasks. Talented professionals are not willing to invest time in low value, repetitive duties, and clients are not willing to pay for it. The focus needs to be on applying new tools to improve the value of information – be it more timely, more accurate, more relevant, or just easier to understand. The technology that will empower professionals to accomplish this lives in the cloud.

A cloud migration involves moving both your data, and your workflows, into a remote setting. It presents a unique opportunity to simultaneously provide more value to clients and greater flexibility to employees. It is the practitioner’s responsibility, however, to ensure that the environment in which this transpires is safe and controlled. The practitioner must be cognizant of their duty to preserve client confidentiality. This paper provides guidance on how to use Microsoft technologies in furtherance to that objective.

This technology wave, this digital transformation, will again change the landscape of the accounting profession, and we expect for the better. We hope that this paper will lay a foundation for operating a secure, cloud-based firm, so that practitioners may innovate with confidence.

Introduction

The motivation to migrate

We believe three aspirations are driving firms to migrate to remote work environments.

Improve service level to clients

We live in an always-on environment. Clients are looking for proactive advisors that can solve problems they don't know they have. New tools are enabling professionals to move from providing historic, to real-time, to predictive feedback. Embracing cloud technologies enables a firm to improve the quality of the information it produces.

The cloud can make it easier to manage client expectations without having employees available 24/7. Clients can more easily participate in projects and have increased visibility as work progresses. Streaming video, screen sharing, secure real-time file transfers, and asynchronous collaboration tools have created less intrusive ways of connecting with clients and improving the quality of those interactions.

Improve productivity and employee morale

If we're not innovating to make each other's lives better, then why do it? As a practice leader, as an advisor to other leaders, we implore you to help keep human beings at the center of any technology initiative. That said, your motivations do not need to be entirely altruistic.

There is a war for talent and employees are gravitating towards flexible, remote work environments. Tools that provide for this kind of flexibility are now available and affordable to small and mid-sized businesses. Facilitating a modern work environment is a differentiator in the employment market.

Security and administrative convenience

As exciting as all these new tools are, for accounting firms, a cloud migration needs to start with a strong cybersecurity and data management program. Most small firms already have hundreds or thousands of users interacting with their IT system via email. It is disorganized, inefficient, and insecure. A cloud migration presents an opportunity to bring that activity under control.

Currently, most cybersecurity incidents begin with email, but many organizations may be overlooking some of their largest threats. As Marc Zadelhoff, former VP, Worldwide Strategy and Product Management for IBM Security, suggests, "when you read the next salacious headline about some breach by an external hacker, remember that these attacks account for less than half of the breaches out there. And remember that the hacker probably used the identity of an unsuspecting employee to pull it off."[1]

Unmanaged, continuous access to client data cannot be the norm in a remote work environment. The cloud provides tools that simplify the administration of a robust cybersecurity and data management program.

Setting a data management policy

Practitioners must be conscious of the fact that the internet is inherently insecure:

> *"The weakness in this scheme (the Internet Protocol) is that the source host itself fills in the IP source host id, and there is no provision in…TCP/IP to discover the true origin of a packet."*[2]

Routers and switches, by design, accept all traffic that is sent to them. The ability to send anonymous and unsolicited traffic has produced criminal enterprises that exploit this vulnerability for profit. Although there have been numerous proposed solutions to improve the underlying infrastructure, adoption is slow and scattered, and breaches have become more frequent. This puts practitioners in a difficult situation.

The AICPA Code of Professional Conduct (AICPA Code) Rule 1.700.001, Confidential Client Information Rule (the Rule), prohibits a member in public practice from disclosing confidential client information without the client's specific consent.

A data breach will create a potential exposure for licensed professionals. Although there is little authoritative guidance about what would constitute due care in such a case, Tracy Fieldman, a managing director in the National Risk and Quality Assurance group at Deloitte Tax LLP, suggests that:

> *"In the case of an unauthorized data breach, in determining whether there has been a violation of the Rule, consideration will be given to whether the member had processes and procedures in place to ensure that client data were secure and that these processes were kept current, communicated to the firm's professionals, and enforced."*[3]

We agree that, in theory, this could provide a practitioner with a potential defense against tort actions should a breach occur, but standards of practice have yet to be developed by the AICPA.

In this paper we propose a set of technology-augmented data management protocols based on the Principle of Least Privilege (PoLP). PoLP is an important design consideration in information security that can limit the damage a breach can cause. It requires that user

[1] Zadelhoff, M. (2016, September 19). The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review. Retrieved from https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[2] Morris, R. T. (1985). *A Weakness in the 4.2BSD Unix TCP/IP Software* (117). AT&T Bell Labs.

[3] Fielman, T. (2017, May 1). Safeguarding confidential client information: AICPA and IRS guidance. The Tax Advisor. Retrieved from https://www.thetaxadviser.com/issues/2017/may/safeguarding-confidential-client-information.html

access be limited to only the resources and information that are necessary for legitimate purposes.

As we look to the future it helps to reflect on the past. There was a time when it was normal for an accountant to report to an administrative desk in the morning to sign out a client file. They were responsible for the file as they worked throughout the day. When they went to lunch, they locked the file in a drawer. At the end of the day, they returned the file. The clerk signed the file back in, and it was placed under lock-and-key until the next morning. This is an excellent example in applying PoLP.

Although it may have been reasonably secure and administratively convenient to provide employees with continuous access to all client records when they were physically in the office, given the highly confidential nature of all CPA firm workpapers, this presents an unacceptable risk in a remote work environment. If an employee is only working on one project, they should not have access to all client records. If PoLP is respected, should an employee's identity become compromised, exposure will be limited to the client files that are currently being used.

We will highlight that the security protocols outlined in this paper make identity, rather than the network, the primary parameter of defense. This is logical in a world where network perimeters continue to become more porous. Perimeter defenses are not effective given the explosion of Bring-Your-Own-Devices (BYOD) and cloud applications. If identity is going to be at the center of security protocols, firms need strong authentication procedures and a means of controlling and monitoring the usage of client data in a distributed work environment.

The anatomy of the solution

Our solution is inspired, in part, by research performed my Roman V. Yampolskiy, who is exploring the intersection of cybersecurity and artificial intelligence (AI). Yampolskiy proposes that "our best hope to defend against AI-enabled hacking is by using AI".[4] For AI to be effective, however, it needs a means to identify patterns of behavior.

Developing and preserving usage logs will provide the data sets needed to effectively deploy AI for this purpose. As Lee and Stolfo pointed out, however, while accuracy is an essential requirement of an Intrusion Detection System (IDS), extensibility and adaptability are also critical when there are multiple "penetration points" into a network system.[5]

We employ several readily available Microsoft technologies to provide the extensibility and adaptability needed to effectively deploy an AI supported IDS.

[4] Yampolskiy, R. V. (2017, May 8). AI Is the Future of Cybersecurity, for Better and for Worse. Harvard Business Review. Retrieved from https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

[5] Lee, W., & Stolfo, S. (2000, November). A Framework for Constructing Features and Models for Intrusion Detection Systems. *ACM Transactions on Information and System Security*, *3*(4), 227-261.

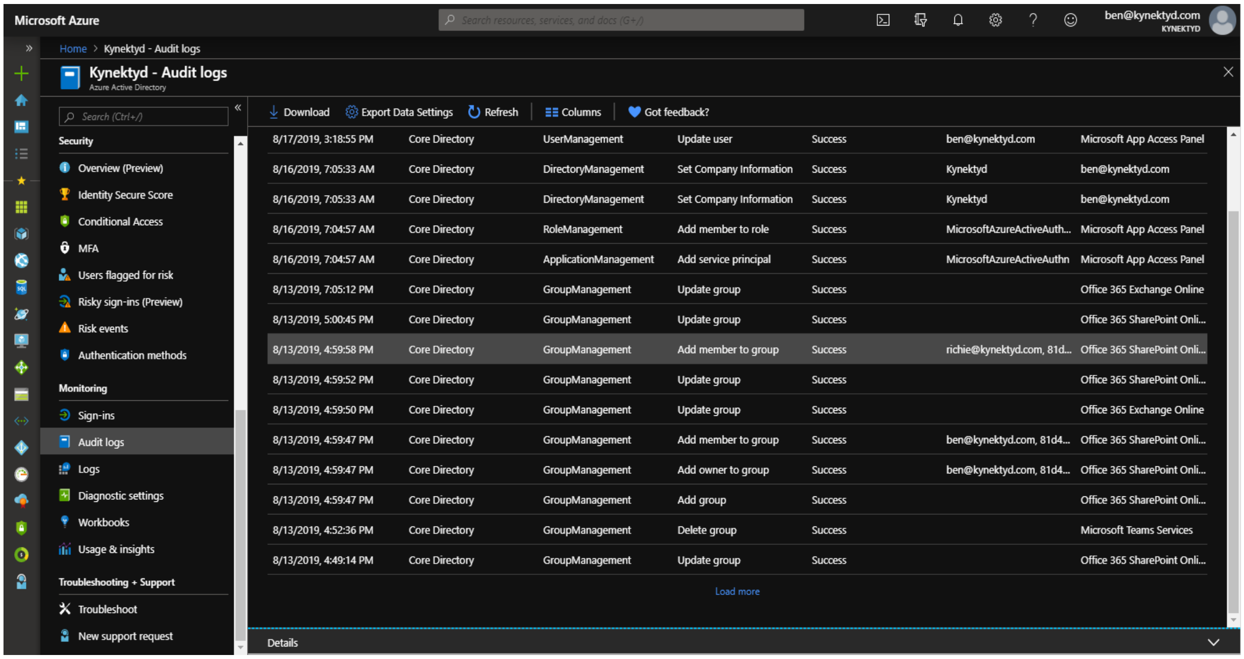
Microsoft Azure Active Directory

Azure Active Directory (AD) is a comprehensive, cloud based, identity and access management solution that is used to identify, authenticate, and authorize individuals seeking access to technology systems and electronic data. It includes modern authentication features that provide the extensibility and adaptability required from a modern IDS. It enables multi-factor authentication (MFA), conditional access, and secure end point protection via Microsoft Intune. It puts identity at the center of security protocols. Basic Authentication, which relies on usernames, passwords and perimeter defenses, is simply not effective.

Our solution aims to:

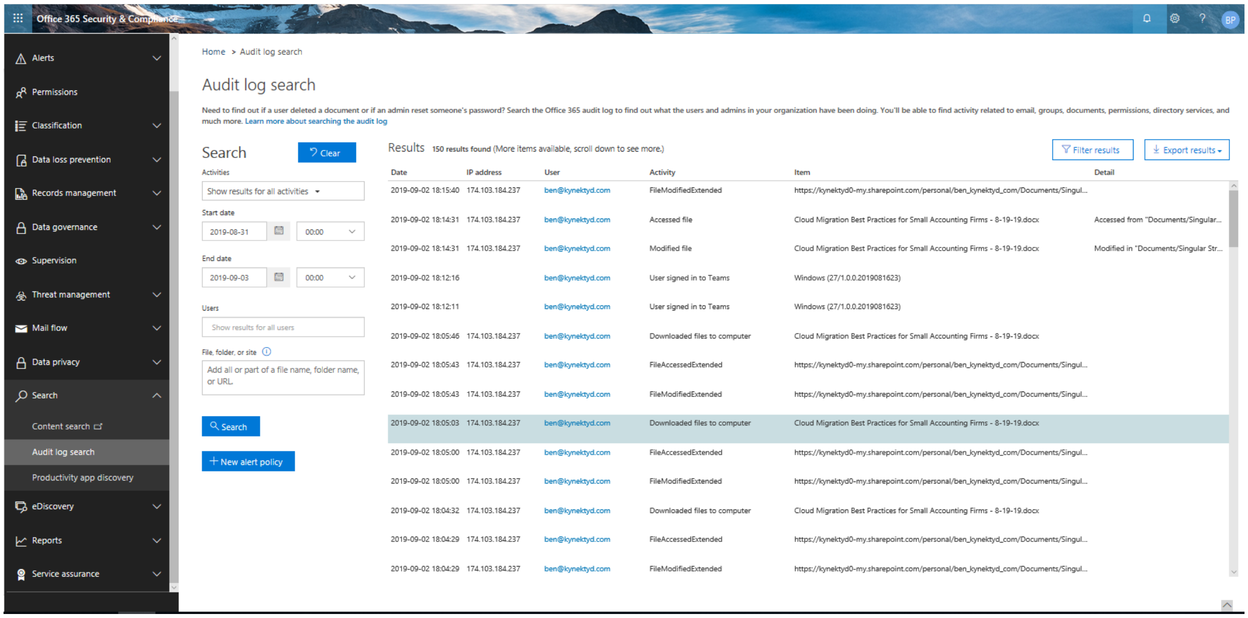
1. Employ Azure AD to create a record of each time an administrator grants or revokes a user's permission to view a client's record, and each time those permissions are used to access a client record. Figure 1 is an example of a log showing the extension of privileges to a user in Azure AD. Figure 2 shows a user exercising those privileges to downloading a file to their local machine.
2. Provide Azure AI with a clean usage log to parse for abnormalities.

Azure AI is continuously monitoring activity. It uses adaptive machine learning algorithms and heuristics to identify risk events to help detect suspicious actions as they occur. The effectiveness of this technology, however, is a function of the quality of information it receives as input. Consistent usage patterns will increase the effectiveness of the IDS.



8/17/2019, 3:18:55 PM	Core Directory	UserManagement	Update user	Success	ben@kynektyd.com	Microsoft App Access Panel
8/16/2019, 7:05:33 AM	Core Directory	DirectoryManagement	Set Company Information	Success	Kynektyd	ben@kynektyd.com
8/16/2019, 7:05:33 AM	Core Directory	DirectoryManagement	Set Company Information	Success	Kynektyd	ben@kynektyd.com
8/16/2019, 7:04:57 AM	Core Directory	RoleManagement	Add member to role	Success	MicrosoftAzureActiveAuth...	Microsoft App Access Panel
8/16/2019, 7:04:57 AM	Core Directory	ApplicationManagement	Add service principal	Success	MicrosoftAzureActiveAuthn	Microsoft App Access Panel
8/13/2019, 7:05:12 PM	Core Directory	GroupManagement	Update group	Success		Office 365 Exchange Online
8/13/2019, 5:00:45 PM	Core Directory	GroupManagement	Update group	Success		Office 365 SharePoint Onli...
8/13/2019, 4:59:58 PM	Core Directory	GroupManagement	Add member to group	Success	richie@kynektyd.com, 81d...	Office 365 SharePoint Onli...
8/13/2019, 4:59:52 PM	Core Directory	GroupManagement	Update group	Success		Office 365 SharePoint Onli...
8/13/2019, 4:59:50 PM	Core Directory	GroupManagement	Update group	Success		Office 365 Exchange Online
8/13/2019, 4:59:47 PM	Core Directory	GroupManagement	Add member to group	Success	ben@kynektyd.com, 81d4...	Office 365 SharePoint Onli...
8/13/2019, 4:59:47 PM	Core Directory	GroupManagement	Add owner to group	Success	ben@kynektyd.com, 81d4...	Office 365 SharePoint Onli...
8/13/2019, 4:59:47 PM	Core Directory	GroupManagement	Add group	Success		Office 365 SharePoint Onli...
8/13/2019, 4:52:36 PM	Core Directory	GroupManagement	Delete group	Success		Microsoft Teams Services
8/13/2019, 4:49:14 PM	Core Directory	GroupManagement	Update group	Success		Office 365 SharePoint Onli...

Figure 1: Azure Active Directory (AD) usage log. The highlighted item demonstrates the addition of a user to a group.



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: Show results for all activities

Start date: 2019-08-31 00:00

End date: 2019-09-03 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Results 150 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity	Item	Detail
2019-09-02 18:15:40	174.103.184.237	ben@kynektyd.com	FileModifiedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:14:31	174.103.184.237	ben@kynektyd.com	Accessed file	Cloud Migration Best Practices for Small Accounting Firms - 8-19-19.docx	Accessed from "Documents/Singular...
2019-09-02 18:14:31	174.103.184.237	ben@kynektyd.com	Modified file	Cloud Migration Best Practices for Small Accounting Firms - 8-19-19.docx	Modified in "Documents/Singular Str...
2019-09-02 18:12:16		ben@kynektyd.com	User signed in to Teams	Windows (27/1.0.0.2019081623)	
2019-09-02 18:12:11		ben@kynektyd.com	User signed in to Teams	Windows (27/1.0.0.2019081623)	
2019-09-02 18:05:46	174.103.184.237	ben@kynektyd.com	Downloaded files to computer	Cloud Migration Best Practices for Small Accounting Firms - 8-19-19.docx	
2019-09-02 18:05:43	174.103.184.237	ben@kynektyd.com	FileAccessedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:05:43	174.103.184.237	ben@kynektyd.com	FileModifiedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:05:03	174.103.184.237	ben@kynektyd.com	Downloaded files to computer	Cloud Migration Best Practices for Small Accounting Firms - 8-19-19.docx	
2019-09-02 18:05:00	174.103.184.237	ben@kynektyd.com	FileAccessedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:05:00	174.103.184.237	ben@kynektyd.com	FileModifiedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:04:32	174.103.184.237	ben@kynektyd.com	Downloaded files to computer	Cloud Migration Best Practices for Small Accounting Firms - 8-19-19.docx	
2019-09-02 18:04:29	174.103.184.237	ben@kynektyd.com	FileAccessedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	
2019-09-02 18:04:29	174.103.184.237	ben@kynektyd.com	FileModifiedExtended	https://kynektyd0-my.sharepoint.com/personal/ben_kynektyd_com/Documents/Singul...	

Figure 2: Microsoft 365 Security and Compliance Audit log. The highlighted item represents a user downloading a file to their personal computer.

Microsoft Office 365 Security and Compliance Center

Functionality that lives at the directory level is supported by security protocols within the integrated Microsoft 365 environment. Among other things, Office 365 users enjoy visibility of data usage at the file level. As demonstrated in Figure 2, once auditing is activated, a log is generated that shows each time a user accesses a file, where they were, when they did it, and what device they were using.

Microsoft SharePoint

Microsoft SharePoint is a platform for creating an intranet of sites that combine lists, libraries, applications, configuration, and content types. The migration to a SaaS platform significantly simplifies the administration of SharePoint sites. SharePoint is a robust product with many potential applications, but we are primarily attracted to the permissions management and archiving features that simplify the firm's data management procedures. SharePoint can accommodate the dynamic and unstructured nature of an accounting firm's data sets more elegantly than the folder-file structure used in Windows.

Microsoft Teams

Microsoft Teams has become one of the most rapidly adopted applications in Microsoft's history. Our solution takes advantage of functionality that can be used to collect and store the conversations, video and audio meetings, and brainstorming sessions that occur as part of developing a practitioner's work product.

Implementing data management controls

Protocols presented in this paper describe one potential data management solution. It is important to note that these examples are intended to be descriptive and not prescriptive. Essential details have been *intentionally* omitted in the interest of making the conceptual design easier to understand by our target audience. Due care is a matter of professional judgement that must always take into account all facts and circumstances, particularly in a rapidly evolving technological environment.

With that said, at the highest level of abstraction, we have actors and assets. Our actors can be managed using the Azure AD identity management framework, but we also need a framework for managing the assets. In accounting firms, each data asset is generally connected to a single legal entity, but it is not unusual for a client relationship to consist of multiple legal entities. A client project may require an employee to access more than one entity file at a time to complete their work.

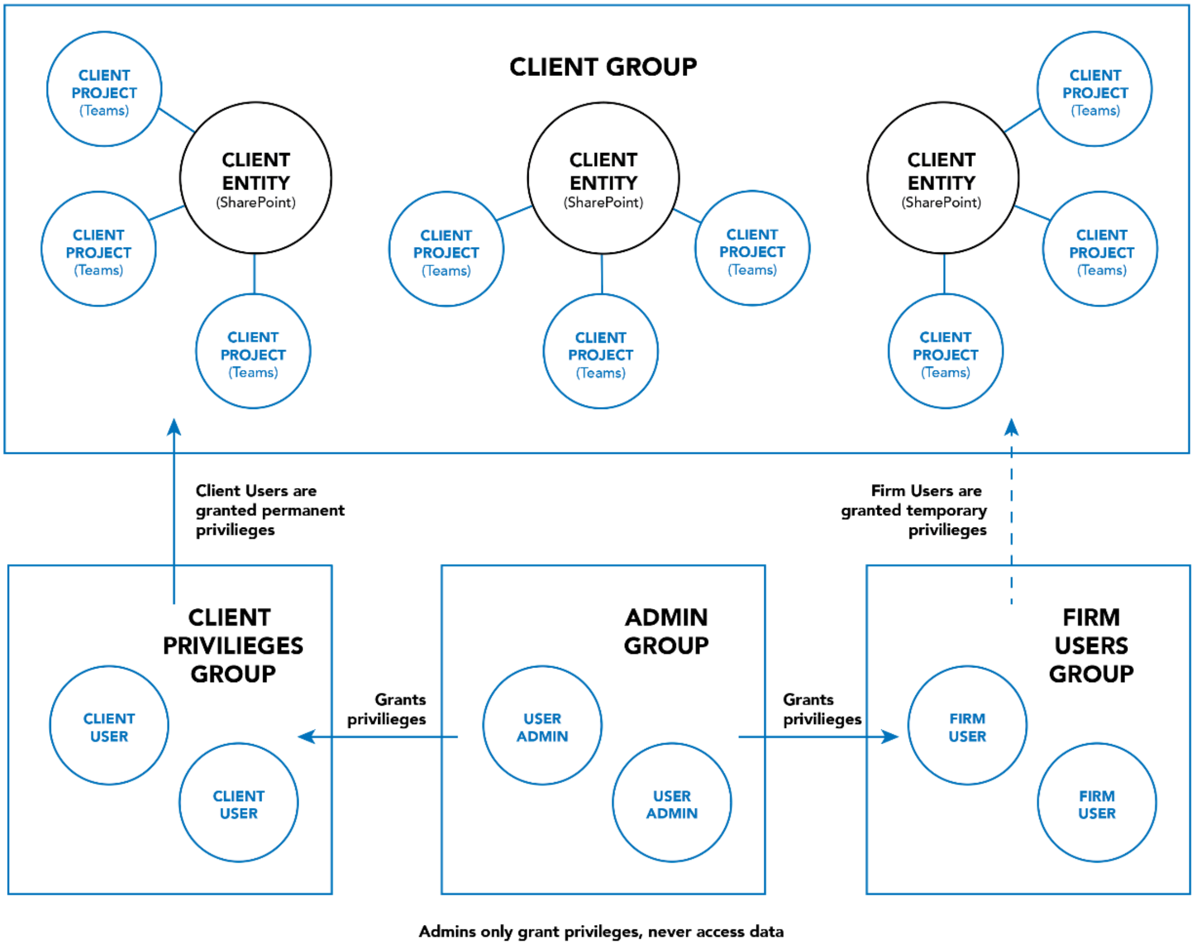


Figure 3: Identity and data management framework using Microsoft technologies.

We have recognized, for some time, that the Windows folder-file structure does not allow a practitioner to elegantly organize client records given the dynamic nature of the client relationship structure. We also considered that although technology may permit a practitioner to extend and revoke privileges on a file-by-file basis, the cost-benefit of such an elaborate protocol may not be warranted.

Our design attempts to strike a balance between what is convenient and what is secure by using an Azure AD Group to represent the client relationship. The Client Group owns all the firm's data assets (i.e. SharePoint Sites and Teams). Users are extended privileges to use those assets by adding and removing them from the Client Group. When no users are in the Client Group, no one has access to the firm's data assets.

We have stopped short of writing actual procedures, but we have included protocols for identity management, data management, and privilege management in the Appendix to elaborate how the model in Figure 3 can help reduce a firm's exposure. Again, these protocols are intended to be descriptive, not prescriptive. There are many ways a practitioner could obtain clean usage logs for an IDS.

One notable practical limitation of our design is that if a practitioner is using more than one cloud-based solution, it becomes more difficult (but not impossible) to obtain usage logs that Azure AI could use to identify abnormal behavior. Incomplete usage logs limit AI's effectiveness.

Establishing a cybersecurity program

The regulatory landscape surrounding privacy and cybersecurity is evolving in the direction of greater control. There have been several regulatory developments, but accounting professionals have always had a duty to protect their clients' confidentiality, both ethically, and because in the US, accounting firms have been required to comply with the provisions of the Gramm-Leach-Bliley Act (GLBA) since 1999.[6]

The procedures outlined in this paper provide a framework for controlling access to client data, but it is not a cybersecurity program. Technical and procedural security measures beyond the scope of this paper need to be documented, monitored, evaluated, and improved. Microsoft's tools provide the infrastructure and applications to implement controls, but it is ultimately the firm's responsibility to develop a program that ensures the preservation of their client's confidentiality.

As the firm undertakes review of its own compliance initiatives, it is important to understand where Microsoft's responsibilities end and where the firm's responsibilities begin. This is the guidance on shared responsibility from Microsoft's literature:

> "The security of your Microsoft cloud services is a partnership and a shared responsibility between you and Microsoft. Microsoft is responsible for the Azure platform and the physical security of its datacenters (by using security

[6] Podraza, B. (2015, September). The Painful Realities of a Data Breach, 31, 18-19. Retrieved from https://issuu.com/ascpa/docs/az_cpa_sept_2015

> protections such as locked badge-entry doors, fences, and guards). Azure provides strong levels of cloud security at the software layer that meets the security, privacy, and compliance needs of its customers.
>
> You own your data and identities, the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components over which you have control. Microsoft gives you security controls and capabilities to help you protect your data and applications. Your degree of responsibility for security is based on the type of cloud service."[7]

This is a good time to point out a key advantage of migrating to the cloud – the ability to rely on service providers' SOC2 audit reports for meeting the firm's ethical and regulatory obligations. These reports cover representations made by an organization with respect to the security, availability, processing integrity, confidentiality, and privacy controls of their systems.[8]

This alleviates the practitioner from having to undertake independently verifying the systems they are relying on are functioning as advertised. Microsoft has the most comprehensive portfolio of compliance offerings of any cloud services provider. Having a single source for all compliance related materials will reduce the total cost of ownership for the firm as they look to meet their ethical obligations.

Modernizing your practice

With this foundation in place, a firm is positioned to flourish. Taking assertive action to preserve client confidentiality is where the digital transformation journey begins, but it does not end there. With appropriate protocols in place, a firm can innovate safely, embrace change, and lead its clients to a bright future.

With that in mind we want to reveal some additional opportunities we see for practitioners looking to modernize their practice using Microsoft technologies.

Microsoft Teams

As we mentioned earlier, Microsoft Teams adoption is growing organically and explosively. We will lay out some protocols to provide a starting point for a Microsoft Teams implementation, but this only begins to scratch the surface of what is available.

Although we encourage a disciplined approach to managing client data, we encourage a creative approach in adopting Microsoft Teams. This is an evolving product. Providing employees with the opportunity to create ad-hoc Teams, add additional tabs, and use the application freely will help discover new ways to use this tool.

[7] https://azure.microsoft.com/en-us/blog/microsoft-incident-response-and-shared-responsibility-for-cloud-computing/

[8] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

The communications features in Teams (e.g. conversations tab, integrated chat, audio and video conferencing, file and screen sharing, Wiki channel) can facilitate workflows that are more efficient and organized than what can be accomplished in an in-office work environment. You must, however, use the tools with some discipline to achieve the desired objectives.

In the product's current form, when a new Team is formed, it includes a single channel called General. That Channel will have three tabs; Conversations, Files, and Wiki. Although it is possible (and advisable) to consider using additional features, we are going to focus on how the current out-of-the-box Teams structure can be used to organize client data and communication.

Conversations

The first tab in every Team is Conversations. This is an asynchronous communications platform similar to a social networking site. Users can start new posts, and review or reply to their teammate's posts, when it is convenient for them. The Conversations tab can be used to collect ancillary conversations that are often an important, but undocumented component, of the firm's work product.

Each Channel has its own email address and emails sent to that address are posted in the Conversations tab. This is a great way to reduce email clutter and contain those conversations in a record that is attached to the rest of the workpapers. Organizations that use Teams religiously will see a reduction in the volume of email transactions.

Information from meetings, such as chat conversations and recorded video, can be pushed onto the Conversation tab. Users can attach files, pictures, videos, and emojis to posts, and they can use the @ feature to filter messaging. For instance, if a user wants to point a post at someone specifically, they should include an "@username" in the post and the specified user will be notified that they have been tagged. For everyone else in the team, that post can be considered FYI.

Files

The Files tab in Teams is linked to the Documents section in an associated SharePoint site. This is where the data the users load into this Files tab resides. Since we rely on SharePoint to manage the unstructured data, the folder-file structure should not be complex. It may make sense to create a standardized folder structure for items like 'Client Provided Documents' or 'Rollover Workpapers'.

As a general practice, each project file should be atomic, meaning that the records in the project file should be enough to defend the work product, but the practitioner should also be conscious of whether they are retaining unnecessary duplicates of records. Best practices dictate the destruction of documents when they are no longer required to be retained. The destruction cycle can be automated, but each document in the file is placed there by a person. Individuals developing support for work product must be cognizant of the firm's document retention and destruction protocols before they archive record sets.

Wiki

The Wiki tab is going to be useful for ongoing structured communication. It could potentially be used to keep meeting minutes. Each Wiki Section can be used to track an ongoing issue or task that the team is working on. The team can use the Wiki Conversations breakout functionality to document updates as the conversation progresses from meeting to meeting.

Microsoft Planner and Microsoft Project Online

Managing projects and employees in a distributed fashion can be a challenge. Microsoft has integrated tools into the Office 365 family to assist with that.

Planner is included with Microsoft Teams. It is a lightweight tool that enables a team to quickly specify tasks, drop them in buckets, and assign team members and completion dates.

Users in Planner can see all tasks assigned to them, but they are not able to see tasks assigned to other users. For this reason, we believe that it may be a best fit solution for sole practitioners that simply need to keep their clients abreast of what the firm needs, but it may not be a great fit for firms that need to track multiple projects and resources.

Microsoft Project Online is the step-up from Planner that provides tools to track projects, tasks, and resources. It provides visibility as to who has capacity or where a team member may need support. Project can also be integrated with Teams, and data from Project pushed to the firm’s billing system.

Azure AD Usage and insights report

Employee oversight can be difficult in a remote work environment. Azure AD Usage and insights reports show usage statistics by resource, such as Exchange, Teams, or SharePoint. Drill down reports provide logs of each time a user accesses a resource, the device they used to access the resource, and where they were when they did it.

Microsoft Flow

Microsoft Flow is a cloud-based software that enables employees to create and automate workflows and tasks across multiple applications and services without the help of software engineers. Although not everyone needs to become a Microsoft Flow expert, all accounting professionals can benefit from developing a rudimentary understanding about where it can help them be more productive.

Although clients may be willing to pay for value, employees are generally exchanging their time for money. Flow empowers accounting professionals to work more efficiently. If employees are performing repetitive, rules-based tasks, Flow may be able to automate the task without a line of code being written.

Business Intelligence

Visualization software, like Microsoft Power BI, is changing the way accounting professionals communicate information to users. This is an exciting development because it enables professionals to effectively service a larger client base. Although spreadsheets and financial statements will have their place, many people respond better to charts, graphs, and other visual representations of data.

With Power BI, the practitioner has control over what is being displayed and who it is being displayed to. There is value in helping individuals understand how to interpret information and what actionable steps should be taken. This has the potential to expand the scope of information reporting services accounting firms provide to their clients.

Concluding remarks

Embracing Agile to a brilliant future

Digital accounting leaders are pushing Agile's evolution. Embracing an Agile methodology means that work will begin without a clear endpoint in mind. This contrasts with the waterfall method most firms employ in delivering their accounting services. With a waterfall, a structured plan and clear outcome is determined before the work is started.

Digital transformation is not going to work that way. The answers that were correct three years ago are not correct today, and there is a good possibility that the answer that is correct today, will be wrong next week, if not sooner. At the same time, there is an overabundance of information available on every topic. Information analysis can quickly lead to paralysis. It is best to begin by setting some broad objectives, and then start walking the path. That is the methodology we have prescribed in this paper.

We encourage you to make your clients part of your firm's transformation experience. That is also consistent with an Agile mindset. Accepting new modes of communication will help you increase engagement between employees and clients. The outcome of your journey is certain to be better if you keep the end-user involved in the evolution of your service delivery model.

We have only touched on the potential that is available once your firm is operating safely in the cloud. New productivity tools are being introduced daily. Microsoft is updating the Azure certification tests every three to six months because that is how quickly the product is evolving. We are entering an era where computers can see and hear, and soon, we expect, they will be able to interpret and respond. Accounting professionals are well-positioned to apply technology in ways that help people understand and trust one another, while preserving their privacy.

As amazing as all these technologies are, in our view, there will never be anything more beautiful than the human mind – i.e. natural intelligence. We encourage you to use data and information wisely. It is in the abnormalities, inconsistencies, and perceived flaws that people will find serendipity that eludes artificial minds.

Appendix – Sample Protocols

Identity management protocols

Data access will be controlled using the user's identity as the primary parameter of defense. Modern authentication will be required for all users.

1. Each firm user or administrator account will be assigned an Azure AD P1 or P2 license.

2. Client users that have Microsoft 365 identities can be set-up for inter-tenant collaboration, which enables them to use the same identity they use to access their company's internal resources, to access resources made available to them by the firm.

3. If the client does not have a Microsoft 365 identity, the firm should assign an Azure AD P1 license to each client user. Client user accounts should never be shared by multiple users.

The Principle of Least Privilege (PoLP) dictates that users be assigned the minimum privileges necessary to do their job.

1. Firm users will be assigned a User Member account.

2. Client users will be assigned a User Guest account, and they will be added to a Client Privileges Group that will apply 'deny assignments' to restrict their ability to access and modify documents. Because deny assignments override privileges extended in other Groups, this provides an administratively convenient way of extending common privileges to Firm and Client users. For instance, the deny assignments could be used to apply restrictions on the guest users' ability to view internal files or modify files that are part of the firm's work product. Client Users, therefore, will have different visibility and file use privileges than Firm Users when added to the same Client Group.

4. The firm will maintain two Global Administrator accounts to ensure that client data will always be available should one administrator become unavailable.

5. Administrators should only use their administrator accounts for administrative purposes. This includes the creation of users and groups and the assignment and revocation of privileges. Other duties performed by individuals with a Global Administrator account should be performed in a separate User account. Global Administrator accounts should never be used to access client data.

Data management protocols

Four types of objects are created for every new relationship.

1. One or more Client User accounts. Each Client User should have a separate account – i.e. no account sharing permitted. Each Client User is added to the Client Privileges Group.

2. A Client Group account representing the client relationship. Each Client User account is added to the Client Group.

3. One or more Client Entity sites are created in SharePoint. The Client Group is added as a contributor to each Client Entity site.

4. One of more Client Teams. The Client Group is added as a contributor to each Client Team.

EXAMPLE:

If a new client brings in tax preparation engagements for a personal return, an operating corporation, and a real-estate partnership, the administrator would create:

- A Guest User account for the primary contact
- A Client Group to control the privilege assignments associated with the relationship
- Three Client Sites, one for each legal entity, and
- Three Client Teams, one for each tax preparation engagement

Following this protocol, the only user(s) that have continuous access to the client's records are the client and the administrator. If a Client User account becomes exposed, the exposure is limited to their own records. If the administrator accounts are never used to access client data, that abnormality is easily identified and contained.

Privilege management protocols

1. Privileges to access client data should only be extended to team members involved in the project when they are working on the project. Generally, PoLP will dictate that data be exposed at the beginning of an engagement and revoked at the end, but if the firm knows a project is going to be postponed for some time, it is wise to postpone extending privileges until the work begins.

2. The only individual(s) that should have continuous access to client data are the clients themselves. This is one of the primary motivations of making the migration – to make information more accessible to your clients. The firm will likely want to publish deliverables, like income tax returns and financial statements, in the document libraries. The firm may consider using Office 365 sensitivity labels and encryption to provide additional security to files that are highly confidential and continuously available via Client User accounts.

3. Clients are extended read-write privileges to a Client Documents folder that resides in each entity’s SharePoint site (in lieu of a client portal on the firm’s website). Enforcing a short document lifecycle in these data-transfer folders is advisable. Deleting any record that is older than 3 or 6 months should prevent stale data from creating unnecessary exposure.

A similar destruction policy is recommended for firm email accounts. Important correspondence should be forwarded into the Teams Conversation tab, where it will be retained with the rest of the associated workpapers. Email should not be used for perpetual storage.

4. When a new engagement is secured, the Administrator creates a new Microsoft Team and makes the Client Group for that client a member of the Team.

5. At the beginning of the engagement (or when work commences, whichever is later), the administrator adds members to the Client Group. This provides employees working on the project with access to all the Client Entity sites and Client Projects associated with the relationship. If the firm wishes to restrict the client's visibility on a project (e.g. an audit engagement), this can be accomplished by applying additional deny assignments.

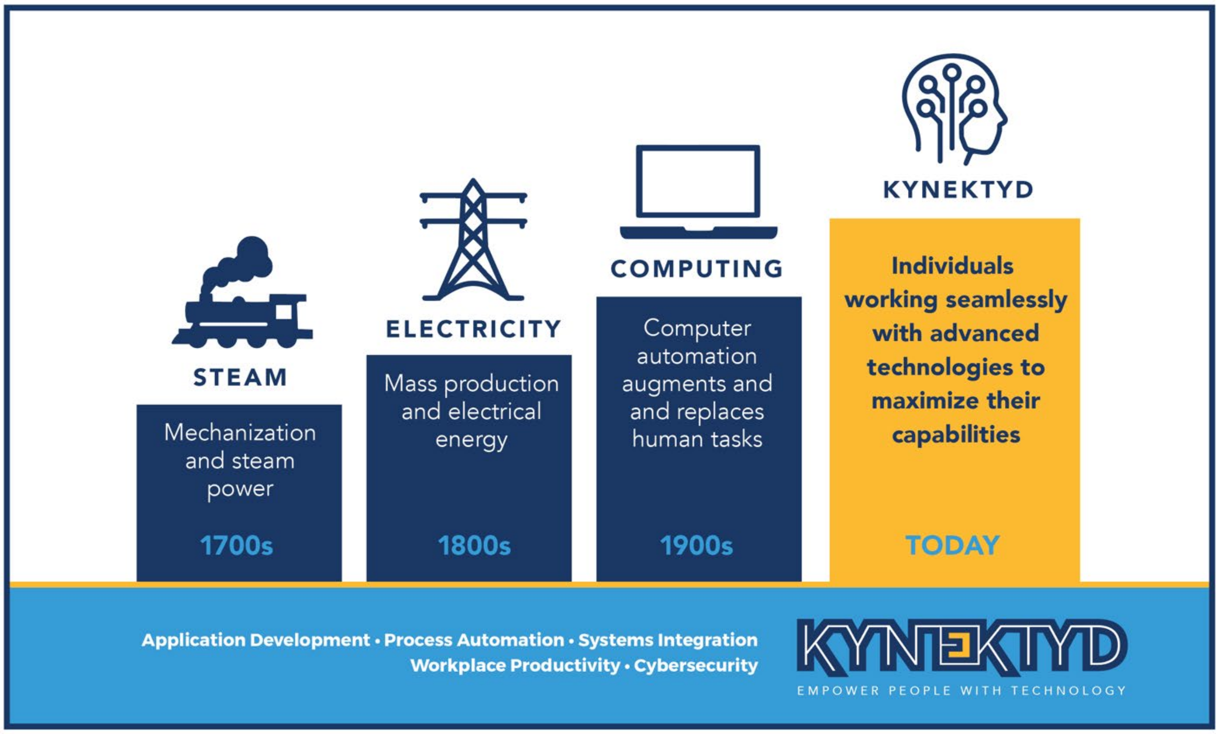
6. When the engagement is completed, the administrator will remove the team members from the Group, which removes their ability to access the client data. The Team (and the associated SharePoint site) will be archived in a read-only format, and a destruction date will be set in conformance with the firm's document retention policies.

Following this protocol, should an employee's user account be breached, the exposure would be limited to the clients that the employee is currently working on, rather than the firm's entire client population. The practitioner should consider additional precautions consistent with Microsoft best practices concerning the storage of highly-sensitive data on SharePoint sites.[9]

[9] https://docs.microsoft.com/en-us/microsoft-365/enterprise/teams-sharepoint-online-sites-highly-regulated-data

About Kynektyd

Kynektyd develops, deploys, and supports technology solutions that help organizations operate more efficiently and profitability. The objective is to maximize the value organizations realize from their technology investments, while keeping human interests at the center of that innovation.



STEAM

Mechanization and steam power

1700s

ELECTRICITY

Mass production and electrical energy

1800s

COMPUTING

Computer automation augments and and replaces human tasks

1900s

KYNEKTYD

Individuals working seamlessly with advanced technologies to maximize their capabilities

TODAY

Application Development • Process Automation • Systems Integration
Workplace Productivity • Cybersecurity

KYNEKTYD

EMPOWER PEOPLE WITH TECHNOLOGY

Report Author

Ben Podraza is the Chairman and Chief Executive Officer of Kynektyd. A second-generation CPA, Mr. Podraza applies 30+ years of experience controlling the flow of information to help Kynektyd's clients deploy technologies to do the same. Ben hold B.S. and M.S. degrees from Arizona State University and is licensed in Wisconsin and Arizona.

kynektyd.com

September 2019

ISBN: 978-0-578-57466-0