Master O365 Governance, Enforce Security Policies, and Achieve Regulatory Compliance

Master O365 Governance, Enforce Security Policies, and Achieve Regulatory Compliance

By Doug Barney

Top IT pros understand the value of a well-oiled IT machine that is efficient, safe, abides by compliance regulations, and fully serves the strategic business needs of the organization through proper IT governance.

Now that Office 365 is running the productivity show, IT managers need to insure the Microsoft cloud suite helps meet all these goals – and that means supporting true IT governance, regulatory compliance, and that O365 and its end users comply with the organization's security policies.

Part One: Why O365 Governance Matters

There are two ways to look at IT governance – governance in the broadest sense and governance as it applies to Office 365. We will delve deeply into the latter, while also offering advice on overall IT governance.

Microsoft has an overall definition of IT governance that relates to their IT Maturity Model, but also looks at Office 365-specific governance issues, and defines a governance plan this way. "Governance is the set of policies, roles, responsibilities, and processes that control how an organization's business divisions and IT teams work together to achieve its goals. Every organization has unique needs and goals that influence its approach to governance. Larger organizations will probably require more—and more detailed—governance than smaller organizations. A good governance plan can:

- Streamline the deployment of products and technologies, such as SharePoint
- Help keep your organization's system secure and compliant
- Help ensure the best return on your investment in technology"

Governance is a broad area with a lot to chew on, and demands high-level organizational involvement and commitment. Fortunately, the return is more than worth the effort, as MIT Center for Information Systems Research (CISR) can attest. "MIT CISR research has found that firms with effective IT governance have 20% higher profits than their competitors," MIT CISR explained. "We define IT governance as a framework for decision rights and accountability to encourage desirable behavior in the use of IT. IT governance focuses on a small set of critical IT-related decisions: IT principles, enterprise architecture, IT infrastructure capabilities, business application needs, and IT investment and prioritization."

Governance is a broad area with a lot to chew on, and demands high-level organizational involvement and commitment.

Part One: Why O365 Governance Matters

Using O365 Without Governance

As mentioned, IT governance is all about aligning IT and IT solutions with business needs and strategy so that IT helps the organization meet key goals and objectives.

In the case of Office 365 governance, the SaaS platform must be secure so it does not threaten business viability, cost effective so it does not harm the bottom line, a maximizer of productivity so it strengthens the bottom line, and reasonably easy to manage so IT can optimize use and quickly solve productivity sapping problems.

Office 365 must also be managed in what Gartner calls "an effective, efficient and compliant fashion", which means IT administrators must be highly skilled and working with a large enough staff to master all O365 complexities, or get a technology solution that does this for them.

Governance and Training

Microsoft believes that a positive return on investment (ROI), and maximizing productivity is achieved through learning and adoption. Great training, good resources, and effective search are keys to user adoption," Microsoft said.

The Problem of Misconfiguration

IT governance posits that the IT staff works efficiently, and has a high-level view of security and how IT protects the network, applications and end users. Part of that is configuring users and services with care, and managing privilege. In fact, Gartner and Forrester both indicate that 80% of SaaS breaches stem from misconfiguration, inappropriate user behaviors, or incorrectly elevated user permissions.

Gartner argues, *"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes."* Correctly understanding your company's existing configuration and management is the first step towards implementing solutions that immediately improve a tenant's security. Meanwhile, monitoring and enforcing policies is the responsibility of Office 365 IT professionals, and is a must-do best practice to reduce your breach perimeter.

"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes."

– Gartner

Part One: Why O365 Governance Matters

For enterprises, correctly defining configurations and appropriate user behaviors are best practices. However, misconfiguration is still possible due to operator workarounds or operator error. That is why it is so important to monitor and enforce your configuration best practices including policies and baselines, and thus fully secure your SaaS environment.

With CoreView automation, deprovisioning goes from up to 20 hours down to under 10 minutes. This saves a typical organization about 1,000 hours a year in manual IT admin activities, while at the same time improving quality of service and reducing human errors. We found that a company with 10,000 employees could save 950 hours of administration time per year, at a projected savings of $45,600 a year – just by properly using RBAC to set Office 365 admin permissions.

Implementing Zero Trust

An important security management and protection paradigm is zero trust. IT used to have a trusted network and trusted users, and an external network and untrusted users. As part of this approach, IT installed a DMZ.

With the zero trust model, the organization only allows access between IT entities that have to communicate with each other. There is no such thing as a trusted user anymore, or even a trusted server. Instead, IT secures every communications channel, because IT does not know who is listening in on the router. IT removes generic access to anything; that access has to be granted specifically. It cannot be inherited, and it has to have a purpose. This is Microsoft's way to implement zero trust throughout an organization.

Our new CoreDiscovery solution will help admins understand, manage, secure, and drive application adoption for their O365 tenant.

Part One: Why O365 Governance Matters

One problem is that implementing zero trust in Azure Active Directory (Azure AD) is highly complicated. "I think the Microsoft approach would probably get you there -- eventually. In contrast, CoreView has a straightforward check box model that gets you to zero trust and least privilege access through our operator access and functional access control model," CoreView Solution Architect Matt Smith explained. "Now contrast Microsoft's complexity with the simple CoreView approach. Our permissions model is all check box-based. The example I typically use is mailboxes. If I want to give someone the ability to create mailboxes, I check a box. Now that person can create mailboxes. If I want to scope it, I put that person in a virtual tenant that is created in a couple of minutes just by looking at properties of Azure Active Directory (AD). Now that person can only create mailboxes for people in the sales department, for example."

This ties into role-based administration since those mailbox permissions are functional-based. CoreView can truly dive deep, and offer highly granular role-based permissions – even offer short-term admin roles. "If I want to give you the function as a help desk person of forwarding SMTP mail because somebody is out on long-term leave, I check some boxes. If I want to give it for just a period of time, I set off a workflow engine that says, 'Grant this operator the ability to forward SMTP mail for a period of an hour or two.' That works really well with workstation folks, who have to roll out OneDrive to workstations; you want to give these folks the ability to change the password on a desktop, but just for the next hour and a half or so while they are rolling OneDrive," Smith said.

This is far simpler than the Microsoft role-based administration model. In Azure Active Directory, Microsoft has defined many roles. One is Application Administrator, which includes 71 different attributes an Application Administrator gets permission to do something with – to read or write or change. "Nobody, not even folks at Microsoft, knows precisely what all of these attributes exactly mean and what this functionally gives the ability to do. How can an IT admin look the chief security officer (CSO) in the eye and say, 'I gave them Application Administrator rights, and know precisely what he's now able to do?' They cannot. Moreover, Microsoft does not define what those rights are," Smith argued.

CoreView can truly dive deep, and offer highly granular role-based permissions – even offer short-term admin roles.

Part One: Why O365 Governance Matters

In the CoreView model, if IT checks the box so a person can create mailboxes, that person can create mailboxes – but cannot do anything else. They cannot change somebody's password, or look up what they are doing in Skype or in Teams. "This is a critical security area. Nobody has truly deployed least privilege access within the Microsoft Office 365 ecosystem – unless they use CoreView," Smith said.

These concerns are too often overlooked – much to the detriment of O365 tenant security. "It's a hard conversation to walk into the CSO's office and say 'You've been running at significant risk from a least privilege access standpoint since you implemented Office 365, which might've been several years ago. You're not following best practices, and you don't know what people are able to do in the platform.' That is a tough conversation to have, and it has to be very delicate as well," Smith argued.

Maximizing ROI, Reducing TCO

With Microsoft Office 365, you pay for users through individual licenses. However, Microsoft does not consider whether all your selected users indeed use the services allocated. That is the job of IT.

Whether paid for licenses are used or not is a huge consideration, and source of immense savings when you downsize to only the licenses you truly need. CoreView finds that, on average, organizations cut licensing costs by 30% after they analyze actual Office 365 usage.

The solution is to find inactive Office 365 licenses and reallocate them with ease.

With CoreView, you easily discover all inactive, oversized and duplicated Office 365 licenses and can cancel or reallocate them without ever leaving the CoreView management platform. This stops overspending, and at the same time identifies departments with low application adoption.

You can get a free CoreView Office 365 Health Check to discover license savings, application usage, and the security state of your Office 365 environment.

In the CoreView model, if IT checks the box so a person can create mailboxes, that person can create mailboxes – but cannot do anything else.

They cannot change somebody's password, or look up what they are doing in Skype or in Teams.

Part One: Why O365 Governance Matters

Maximizing Productivity

Driving application adoption is essential to maximizing Office 365 investment. Key to a successful adoption plan is clustering users based on different service usage and behavior – which helps drive targeted adoption and training campaigns.

Once you have an adoption strategy, it is time to train your users. Experts have found that standard training (classroom and eLearning) are not optimal since users forget 70% of what they learned within 24 hours.

The solution? – Adoption campaigns and Just in Time Learning (JITL). CoreView's CoreAdoption usage insights and adoption campaigns ensures all employees keep pace as things change.

Meanwhile, CoreView's CoreLearning is a Just in Time Learning (JITL) system with 2,000+ how-to videos lasting from 30 second to 3 minutes. The secret sauce is these videos are context sensitive, and play as the user is working with the application. Read our Just in Time Learning (JITL) whitepaper to find out more.

You can get a free CoreView Office 365 Health Check to discover license savings, application usage, and the security state of your Office 365 environment.

Part Two: Security Policy Compliance

When IT pros hear the word compliance, regulations first spring to mind. The second thought is about security policy compliance. After all, all the defense in depth tools won't make you safe if end users and IT infrastructure don't align with security policies, or even worse, if you have not security policies at all! In short, IT needs to be able to quickly and easily create policies, update them on the fly, discover security policy infractions in real-time through alerts, and fully enforce policy compliance through proper management solutions.

Creating Real-Time Monitoring and Alerts for Security and Compliance Issues

When it comes to alerts, IT either has so many it cannot see the ones that really matter, or too few, with little to no visibility into critical issues. The answer is enabling real-time monitoring and alerts for potential security compliance issues in the Office 365 environment.

One CoreView customer used to **spend 10 to 50 hours every month writing and running custom PowerShell scripts to decipher the millions of log entries and search for security problems.** Now they leverage CoreView to provide automated alerts for security issues on an almost real-time basis. Whenever a known issue is reported within any of the different Office 365 event logs, the CoreView monitoring agent creates an alert and notifies the specific IT admins to take action.

Once alerted with the appropriate information about the security issue, the IT admins can take immediate action to rectify the situation and close the security concern. Another customer said they **now have hundreds of these CoreView security compliance alerts configured within their environment to empower them with the real-time knowledge of non-compliance activities so they can be remediated quickly.**

One CoreView customer used to **spend 10 to 50 hours every month writing and running custom PowerShell scripts to decipher the millions of log entries and search for security problems.**

Now they leverage CoreView to provide automated alerts for security issues on an almost real-time basis.

Part Three: Regulatory Compliance

The Problem: Not Taking Care of Compliance

Compliance is a big security and economic issue. There are almost daily incidents of fines occurring due to GDPR and other issues, and IT is not usually able to respond quickly.

If you are not aligned with what your top peers are saying and doing, it is a sign of security weakness. How does a shop know how well it handles security? Looking at peers shows you have at least done your due diligence. If we have not approached best practices, if we cannot measure ourselves with how others are doing in the industry, then we are likely at a severe deficit. That is a career-limiting move.

The way that CoreView surfaces this information is through our enhanced version of Secure Score, which shows exactly how Office 365 shops are doing against their peers, measuring items such as doing proper configuration management, and applying least privileged access.

Many compliance regulations ask shops to collect data logs for a specified period of time. However, Microsoft gives you only the last 30 days of data logs (now moving to a full year, but only for E5 licenses).

Dealing with GDPR and the Right to Be Forgotten

There is much involved in being compliant with GDPR that many IT pros do not always think about. A critical flaw in GDPR, in fact one of the foundations of GDPR, is the right to be forgotten. "How can I forget you, if I do not know precisely who you are and what you did while you were here?" asked CoreView's Smith. "I cannot forget those things unless I have a record of what you did."

Fortunately, with CoreView, not only do you know who 'Joe User' is, but in the CoreView system, that user has a unique serial number that is stored and used as an account ID. If that 'Joe User' leaves and a new user with the same name starts later, IT will know which 'Joe User' performed a particular action or was the owner of this particular, say, file. That is because all the actions of both Joe Users are tracked and audited. Without CoreView, all that information goes away as soon as IT deletes Joe User and is not stored externally in an audit log, the way CoreView does.

The way that CoreView surfaces this information is through our enhanced version of Secure Score, which shows exactly how Office 365 shops are doing against their peers, measuring items such as doing proper configuration management, and applying least privileged access.

Part Three: Regulatory Compliance

"You cannot be GDPR compliant unless you capture and store that kind of information. How do I apply compliance regulations that say I have to be able to notify people when there is a breach – and at the same time, be able to forget somebody when they file their right to be forgotten?" Smith asked.

That is a deep pain point that requires a deep solution. Fortunately, CoreView tracks and stores all this information for admins and end users. On the admin side, for instance, CoreView can produce a report in seconds of every single administrative action an IT staffer has taken on the Office 365 platform since they started. End users are tracked in a similar way. "Why can't I do that in Office 365 Admin Center? A bank teller can tell you every single check they have cashed, exactly how much money came in for deposits, and how much money went out. Banks keep those logs for seven years due to banking regulations. However, Office 365 shops using the native Admin Center cannot tell today exactly what administrators did in the platform -- and yet CoreView can," Smith explained.

Stopping Compliance-Busting Breaches

Most all compliance regulations require defenses against breaches, and can even punish organizations that have been breached. Stopping breaches, and performing forensics on attacks that slip through, are critical parts of an effective compliance strategy.

On the admin side, for instance, CoreView can produce a report in seconds of every single administrative action an IT staffer has taken on the Office 365 platform since they started.

End users are tracked in a similar way.

Part Three: Regulatory Compliance

The CoreView Solution – Understand Who Your Users Are and What They Are Doing

CoreView, and in particular, the CoreAdmin tool, helps set up administrators that are specific to a location, functional set of users, or other attributes. This means admins know who their users are, and have a manageable set of end users to handle.

At the same time, CoreView tracks application usage, so you know which applications handle the most work, and when end users are misusing the system. The 'single pane of glass' CoreView console offers deep insight into how end users are configured, and where they might be misconfigured.

With CoreView, you can monitor your configurations and usage policies. If a misconfiguration or a misusage has been detected, you can immediately remediate it as well as enforce those policies using the CoreView RPA automation capability.

With CoreView, policy management moves from a manual and error-prone process to one that is intuitive, easy and automated.

CoreView tracks application usage, so you know which applications handle the most work, and when end users are misusing the system.

The 'single pane of glass' CoreView console offers deep insight into how end users are configured, and where they might be misconfigured.

Identify — and Solve — Security Compliance Pain Points

Ten Questions to Ask

1. What are the top three challenges you face when performing Office 365 and Azure AD security audits?
2. What shortcomings in the Admin Center and other management tools impact you the most?
3. How do you identify users who are breaking the security compliance guidelines for Office 365?
4. Is there currently a process to perform regular security compliance audits for Office 365?
5. How do you provide security auditing and analysis to your legal team responsible for performing research?
6. Would it be helpful to configure real-time automated alerts for your top-10 security compliance issues?
7. Do you provide Global Admin Rights to remote administrators so they can support their local business units?
8. Do you currently have custom PowerShell scripts that help with reporting on Office 365 security compliance?
9. How do you currently perform your audits for Office 365 security compliance?
10. What is your escalation process for requested data loss analysis audits? Who performs those audits and how?

Get Started with CoreView — for Free

Our new CoreDiscovery solution will help admins understand, manage, secure, and drive application adoption for their O365 tenant. Learn more on the CoreDiscovery product page: https://www.coreview.com/corediscovery/.

Get your free software at the CoreDiscovery sign up page: https://www.coreview.com/core-discovery-sign-up/.

Want to learn how CoreView prevents overspending on licenses, underusing applications, or mismanaging security and configurations? Our free CoreView Office 365 Health Check diagnoses all your Office 365 problems. Sign up for an Office 365 Health Check and we will build a detailed 20-page report to cure all your Office 365 ills.

Not ready for a full custom report? You can still take a look at a Health Check sample report.

Want to see firsthand how CoreView solves Office 365 problems and tightens security, just request a demo.

About the Author

Doug Barney was the founding editor of Redmond Magazine, Redmond Channel Partner, Redmond Developer News and Virtualization Review. Doug also served as Executive Editor of Network World, Editor in Chief of AmigaWorld, and Editor in Chief of Network Computing.

Not ready for a full custom report? You can still take a look at a Health Check sample report.

Want to see firsthand how CoreView solves Office 365 problems and tightens security, just request a demo.