Managing Partner Forum®
ADVANCING THE BUSINESS OF LAW

THE MANAGING PARTNER'S GUIDE TO IT AUDITS

by

Lee Hovermale and ***Don Champagne***
FlexManage

FEATURED ARTICLE

POWERED BY
TheRemsenGroup
Smart Strategies for the Forward Thinking Law Firm

TheRemsenGroup.com

flexmanage

The Managing Partner’s Guide to IT Audits

LEE HOVERMALE AND DON CHAMPAGNE

An Information Technology Audit is the examination and evaluation of the firm’s information technology infrastructure and its policies and procedures to determine whether the IT systems are up and available at all times, are safeguarding the firm’s assets, safeguarding data integrity and operating efficiently to achieve the firm’s established goals and objectives, including the firm’s responsibility to protect its clients’ data. IT auditors examine not only physical security controls but also overall business and financial controls that involve the IT systems to determine the risks to the firm’s information assets and help identify ways to minimize that risk.

An IT Audit is not about ordinary accounting controls, traditional financial auditing, or compliance testing. However, the auditor will assess the design and efficiency of controls to determine whether they are suitable to properly mitigate risk.Risk factors include system-related issues, change management and vulnerabilities and other factors related to your technology.In fact, a company’s IT infrastructure brings a unique risk to the firm that would not exist without IT being present.

For example, some of these risks include:

- Cyber-attacks through website or hosted platforms
- Infection by virus or malicious software
- Denial of service attacks
- Ransom attacks
- Phishing emails
- Loss or leakage of confidential information

Your reliance on your IT department or outside IT service provider can also be a risk depending on their technical ability and staffing level for the services expected of them. Without periodic evaluation and examination, these risks can become reality and go unchecked for extended periods of time.

As the firm’s chief executive officer, you are the person ultimately responsible to ensure that the IT systems and controls are aligned with the firm’s goals and legal requirements and are being managed, maintained, updated and kept current. In many cases, you are relying on your COO, an internal IT professional and/or your outside service provider to manage these risks. However, that reliance does not replace your ownership of this responsibility. It is therefore imperative that you understand what systems and policies are involved in protecting the firm’s data, how they work and the level of risk you and your firm will accept. When it comes to the acceptable level of risk, you should determine your Recovery Time Objectives (RTO) and your Recovery Point Objectives (RPO) and the cost per day of the firm being shut down.These metrics should be identified and included in your overall Disaster Recovery/Business Continuity plan. The development of a DR/BC plan should start with a Business Impact Analysis (BIA) which addresses these needs by practice area, office and for the firm overall. If your firm has not formalized a DR/BC plan for all potential disasters, you should begin that process. However, that is a subject for another time.

RTO is the length of time that a service level within your business must be restored after a disaster or disruption to avoid unacceptable consequences associated with a break in business continuity. For example, most firms feel that they cannot be without email for more than one day. The RTO for email would be 24 hours. Your IT system should, therefore, be designed around being able to meet this RTO. RPO is the maximum period in which data might be lost from an IT service due to a disaster or disruption. For instance, email may be needed within 24 hours, however, you may feel that your time and billing system can be down for one week before it negatively affects the business. These are metrics that you must plan with your management team before deciding on your IT system design. These metrics should be published to the firm to set the expectation with the partners and will be what you will be graded against when a disaster occurs. Your internal IT department or outside service provider should be keenly aware of your specific RTO's and RPO's and manage to them. Of course, the level of risk you are willing to accept is always based on the cost to cover that risk. This is where an experienced IT consultant can assist you with developing your DR/BC plan and your IT system to meet those requirements.

To be certain that your IT system is being managed and maintained to meet these requirements, it is best practice to have an IT audit performed periodically to document your compliance level and provide a roadmap for remediation when needed. This cannot be performed by your own IT department or service provider as they are the ones actually being audited. As you know from experience, there are many issues that arise in a normal business month that affect your IT systems. Some are more problematic than others and some are down-right disasters. Fixing problems during a crisis is often done with the goal to fix it ASAP. Some fixes are just temporary or workarounds. After every disruption event, your IT person or vendor should document the changes made in your system and prepare a post-mortem written report for you and your COO that explains what happened, why it happened, lists what needs to be done to permanently fix the problem along with the cost of the fix. Unfortunately, most IT people have difficulty with documentation and these follow-up steps get lost once the crisis is averted and they get back to handling their backlog of work that built up during the crisis. Your COO is responsible for the management of his team and should be managing this process.

Other areas that cause a system to fall out of compliance include:

- The time involved to maintain the infrastructure is often put on the back- burner due to your IT department's workload;
- Delaying infrastructure refresh of hardware and updating software;
- Cost of maintaining IT; and
- Lack of understanding the consequences of not performing regular maintenance and refresh.

Over time, your well-designed system is no longer configured the way it was initially and could eventually result in a slowness in your system causing the productivity of your attorneys and staff to suffer and ultimately a crash/outage. For these reasons, it is best to bring in an independent third-party IT auditor to verify and evaluate your IT systems.

An IT Audit should cover the following areas:

- Review of all documented policies and procedures, IT budget and actual IT spend
- Review of DR/BC Plan including RTO & RPO
- Basic internal & external security scan
- Patching process and status (servers, network devices, workstations)
- Endpoint security
- Network file share security
- Backup Redundancy
- Offsite backups and failover sites
- Sample file level data recovery
- Ransomware attacks prevention and response processes
- Active Directory accounts review
- Password policies (User and IT systems)
- Encryption (including server drive level encryption)
- Wireless network security
- Version status of applications
- Security logs archiving
- Review age of infrastructure hardware (servers, storage devices, network devices, switches, workstations,etc.) in all locations
- Review of physical server rooms, UPS, cooling systems/ ventilation, etc.
- Interviews with executive leadership, attorneys and staff around feedback of systems and IT support
- User services and training

This may seem daunting, but every law firm, regardless of size, must deal with these issues or face the cost of downtime from an event that could probably have been averted with proper planning and regular system maintenance. An IT consultant can help you and your COO navigate these waters by explaining your technology, supporting your IT department as a resource for the more complex issues and solutions and providing on-going strategic advice to you and your management team.

Lee Hovermale | *Chief Executive Officer, FlexManage*
lhovermale@flexmanage.com.

Don Champagne, CPA, CGMA | *Regional Director, FlexManage*
dchampagne@flexmanage.com.