Information Technology (IT) Audits

What Should you Consider?

www.klm-audit.com.au

KLM & AUDIT COMPLIANCE

What Do IT Audits Provide?

With the evolution of technology we have begun to rely more and more on the use of electronic systems. They store and distribute the information that we use everyday in our businesses.

We trust our systems to hold valuable data such as our intellectual property, as well as sensitive information such as contact details and payment records.

But how do we know we can trust these systems?

An IT audit lets you review your current work practices and the controls in place to ensure they are meeting your needs, aligned with your business polices and are appropriate for the intended use.

While an individual audit scope would be needed for each business, there are a few points and related control checks around your systems that should be considered to ensure you cover the basic compliance requirements

www.klm-audit.com.au

KLM & AUDIT COMPLIANCE

Disaster Recovery Plan (DRP)

Your Disaster Recovery Plan sets out how quickly you could restore your operations at another site should the worst happen and you were unable to continue trading at your current location due to a natural or man made disaster.

Your DRP is an essential document that should be reviewed on a regular basis. It should also be known by all staff long before a disaster occurs to ensure they understand what to expect and what their responsibilities are.

Disaster Recovery Plan (DRP)

Things to consider in your DRP are

- Develop a DRP team to coordinate recovery activities, include a list of responsibilities, contact details and alternative team members should someone be unavailable
- List the location of the secondary recovery site
- An inventory of current electronic and physical assets of the business
- A prioritised schedule for the restoration of functions and departments
- A plan to transfer essential employees to the recovery site, consider also transferring the employees family if the recovery site is located outside the local area
- A list of essential equipment for each stage of the recovery process
- A financial plan for the recovery activities
- A plan to advise employees of the situation and the progress of the recovery. If your communications network is down you may need to look at third party communications providers to assist you
- A list of external suppliers and clients that also need to be advised of your situation

Back Up and Restoration of Data

While your back up procedures should be included in your DRP, they need to be reviewed separately and more frequently.

Depending on the size of your business you need to determine an appropriate back up schedule, preferably using a back up system that confirms if the action was successful. Your back up files should also be stored off site to ensure they are available in the event of a disaster.

Just putting a back up schedule in place is not enough though. You need to test the restoration process to ensure the data is able to be restored correctly with no corruption. Regular restoration of random files is a good way to test this.

Security Controls - Electronic

When looking at the security aspect you need to consider not only the electronic controls but also the physical controls.

In regards to the electronic controls the biggest question is who has access to the administration password? Is there only one administration password or do the relevant IT staff have individual administration logins to allow the recording of who has made a particular change to a system?

The electronic controls should be monitored and reviewed to ensure they evolve as your business grows.

Security Controls - Physical

The physical controls relate to the onsite hardware, in particular any onsite servers.

When looking at server security you would consider the accessibility of the server room itself. Is the room secure? Who has keys to this room and is there a register of access?

Another consideration would be the risk management controls such as fire fighting equipment and the installation of an uninterruptable Power Supply (UPS) as well as the maintenance of this equipment.

www.klm-audit.com.au

KLM & AUDIT COMPLIANCE

User Access – allocation and removal

User access is another area that needs to be looked at from different sides.

Clear guidelines need to be developed in regards to the allocation of appropriate access both on commencement of employment and any change in roles. In addition an approval process should include input from other departments, for example Human Resources, to ensure the correct level of access is granted.

Another aspect of user access is to ensure that when a staff member leaves the business that access is removed in an appropriate timeframe, this should include direct employees and sub contractors who have access to your systems

User Access – Passwords and Emails

In regards to passwords, again clear guidelines should be established in relation to the frequency in which passwords are required to be changed, how many previous passwords are remembered and the number and type of characters that can be used.

While not directly related to passwords, the amount of idle time before the device locks should also be confirmed and enforced.

Emails present another area of risk when staff members leave. Procedures need to be documented to control risks in relation to cancelling remote access to email accounts, removing any out of office replies left on a previous employees account and the length of time emails are forwarded to another staff member.

Code of Conduct

Your IT Code of Conduct will include the policies and procedures relating to electronic communications, internet and social media use.

Depending on the size of your business these policies and procedures may be separate documents or combined in a single Code of Conduct.

As with all your internal documents your Code of Conduct is not a write and forget document. It needs to be reviewed regularly and updated as required.

www.klm-audit.com.au

KLM & AUDIT COMPLIANCE

Strategic Planning

As with any other area of your business the improvement of your IT department and the upgrading of your systems should not be left to chance.

Each time you review your business plan and create your goals and strategies to develop your business your IT requirements should be included.

Not only should clear goals be determined in regards to your improvement strategies, you also need to ensure you have a plan of how you will action these improvements.

www.klm-audit.com.au

KLM &
AUDIT
COMPLIANCE

Project Management

While the strategic planning looks at long term outcomes, you also need clear guidelines as to how you are going to implement changes.

Your IT project management plan should be able to be flexible enough to be used for both your software and hardware changes.

It should also list the project team members and their responsibilities, provide an overview of the project and the goals to be achieved as well as the timeframe for completion of each stage of the project.

Regardless of which department has initiated the project, all possible departments that will be effected by the change should be included in the project team.

KLM & AUDIT COMPLIANCE

Conclusion

The information in this document is a general overview of what you may want to include in your IT audit scope. For larger businesses this may be an audit of your internal IT department, while for smaller businesses, who outsource a majority of their IT services, these could be points you want to confirm with your IT provider.

Ultimately when you are looking at conducting any audit there are a few questions to ask yourself about the task, procedure or policy you are auditing -

- Are they documented? - is there an internal document that explains why you do it this way, who is responsible for it and how it is done?
- Are there control checks in place? - Is there a built in second check to confirm the actions are completed correctly? This can be either a manual check by another staff member of an electronic check by a system
- Does it cover you compliance requirements? - Depending on the industry you are in there are a number of government standards, legislations and regulations that you need to follow. In addition to this there may be contracts or deeds of service that also list requirements you must follow. These need to be considered when creating any internal documents.
- Are they compliant with the goals, ethics and culture of your business? - You have a vision of how your business is to be presented and operate, do your internal documents and work practices reflect that?

www.klm-audit.com.au

KLM &
AUDIT
COMPLIANCE

What To Find Out More?

At KLM Audit & Compliance we specialise in relieving the stress and worry business people often feel when dealing with compliance issues.

By helping businesses achieve a greater insight to their daily operations we educate businesses on the importance and benefit of Internal Auditing.

For one off engagements or longer term projects KLM Audit & Compliance can provide the quality and experience you need.

Contact us today to discuss your compliance concerns

katrina@klm-audit.com 0407 690 046

www.klm-audit.com.au

KLM &
AUDIT
COMPLIANCE