Accounting for Risk
Managing Risk in a time of constant change
Managing risk in a time of constant change

Ensure your Digital Transformation journey is controlled and secure.

Businesses now operate in an ever-changing environment of regulation, Digital Transformation, risk management and changing work practices. These place serious demands on an organisations' resources.

However, without even realising it, organisations may open themselves up to data security risks while they adapt, change and - in particular - digitally transform. Security within an organisation can focus on protecting an organisation ‘before’ and ‘after’ they transform but what about the transitioning period?

Auxilion offers a Microsoft Certified Cybersecurity Risk Assessment to ensure your Digital Transformation journey is secure. It also provides a clear roadmap for your team. They can then take any necessary actions required to close potential vulnerabilities.

Auxilion offers a Microsoft Certified Cybersecurity Risk Assessment to ensure your Digital Transformation journey is secure. It also provides a clear roadmap for your team. They can then take any necessary actions required to close potential vulnerabilities.
In order to decide how to protect your data and mitigate risk, you must know what actually needs protecting. It’s not just data, but entry points, the knowledge of your employees and the policies, procedures, and plans you have in place. The purpose is not just to deal with unforeseen situations, but to prevent them from occurring in the first place.

The best way to do that is via robust assessments of your company to ensure that you are keeping on top of the various internal moving parts and external influences. Being prepared is a continuous process, not something that can be solved with a particular tool or product. As Digital Transformation specialists, our expertise allows us to properly assess a company’s health, enabling better and stronger decisions to be made.

Auxilion’s Cybersecurity Risk Assessment service ensures an organisation’s Digital Transformation journey is controlled and secure from the start and throughout the process. We have been working with organisations for over 20 years, with a focus on Digital Transformation. Our Microsoft certified solution offers peace of mind and a comprehensive roadmap to organisations who proactively manage risk.

**Migration Risk**

While many organisations believe moving from old systems to new is straightforward, the truth is you are most at risk during the migration phase. For example, a project that sees you migrating from old legacy systems to a new cloud-based system can take up to 18 months. Such movement can leave you open to potential risks and issues, especially when you are in-between migrations.

Digital Transformation is far from straightforward. In fact, many Irish organisations struggle with what it means to be ‘Digitally Transformed’. Microsoft research has found that ‘Irish businesses overestimate their digital readiness, with nearly half struggling to keep up with customers’.

While many people will think of risk occurring at the start or end point of a project, the reality is that a different kind of risk emerges while your organisation is transitioning.

As companies evolve and look to leverage all the benefits for the cloud, they need to understand and predict where potential risk may arise and how to manage it properly. According to LogicMonitor, 83% of enterprise workloads will be on the cloud by 2020 with digital transformation being the leading factor driving this.

The traditional mindset towards IT security, which was often minimalistic and static by nature, is no longer satisfactory in the Cloud era as the threat landscape is expanding and evolving at a much faster pace than ever before.

Every business is different and therefore your awareness of the risks you face, and how you handle them is crucial. Without a clear road map for your Digital Transformation journey that maps out areas of risk and potential vulnerability - failure, data loss, regulatory punishment and reputational harm become almost inevitable.
As a leading Microsoft partner and Digital Transformation specialist, Auxilion works with customers to assess their cybersecurity status and address structural vulnerabilities.

Continuous monitoring

We utilise tried and tested processes and solutions, to ensure our customer journeys are controlled and secure. Our offering gives customers a key indicator of an organisation's exposure to cybersecurity threats based on multiple factors.

Throughout a customer's Digital Transformation journey, we continually assess our customers' security status by providing insight into their potential vulnerabilities, based on data from the company infrastructure and Office365. We then plan a roadmap for the ongoing security of their infrastructure, aligning their policies and procedures with best practice.
The issue of risk management is just as much a concern for the Chief Financial Officer (CFO) as anyone else. Their primary concern is managing and mitigating financial risk to the organisation. However, they now have much greater influence on how enterprise risk is managed, and this has broadened into data protection. However, they have to play catch up with what this new dimension of risk entails.

This is a new cybersecurity world filled with highly motivated hackers and highly sophisticated attacks, companies stand to lose more from a cyberattack than they stand to gain from cutting costs. A CFO may be able to push the financial needle in a positive direction, but by doing so, they may jeopardize cybersecurity. Then, when an attack is successful, minor gains are wiped out by major losses.

What CFO’s need to ask themselves is whether they’re aware of the risks associated with digital transformation and do they know how to address them. As organisations change the way they deliver IT services to users, partners and clients, it brings new concerns.

Research from BT found that CIOs and CFOs are more likely to see a data breach as a more damaging incident than the unexpected departure of a CEO, a profit warning to shareholders, a product recall or major service outage.

The traditional way of looking at IT security is no longer relevant when you are taking advantage of the Cloud, as the threat landscape is constantly evolving at a faster rate. As you change the way you work, so too do the risks that your business faces and they can be unique to your business.

The solution to this is a robust approach to security and clear processes that ensures everyone knows what to do, what measures have been taken and why such measures are in place.

One way the organisation can gain insight into their cybersecurity risk, and understand where to invest in, is through Auxilion’s Cybersecurity Risk Assessment services. We ensure your Digital Transformation journey is controlled and secure from the start. Outlining clear assessment reports, detailed roadmaps and defined investment ensures your organisation is protected against cybersecurity risks.

Research from BT found that CIOs and CFOs are more likely to see a data breach as a more damaging incident than the unexpected departure of a CEO, a profit warning to shareholders, a product recall or major service outage.

It can be delivered in two ways: As a once-off project where the assessment will provide a snapshot of an organisations’ cybersecurity risk score or as a service delivered on a quarterly basis.

The latter is recommended as it allows organisations to constantly assess their cybersecurity risk score, carry out recommendations and regularly check in to see how much these changes have benefited the company.

The more frequently your security practices are updated, the lower the cost is in the long-run. Carrying out a major once-off upgrade can be expensive but if you’re doing smaller incremental changes, the overall cost can be lower in the long-run.
By investing in security skills and governance tools, you can build up to the required level of knowledge needed to keep up with these changes.

Gartner estimates that the majority of Cloud security failures in the next four years, between 2019 and 2023, will be due to customer faults. As a result, companies are investing heavily in improving cloud security, from the transition to the end goal and beyond.

These predicted failures are also driving the demand of consultancy and managed services which are an essential part of the security landscape, as only the largest companies have the resources to do this in-house. Engaging with consultancy and managed services can significantly strengthen both your expertise and knowledge without requiring businesses to invest significant amounts of money into technology.

By investing in security skills and governance tools, you can build up to the required level of knowledge needed to keep up with these changes.

Considering how more CFOs see a data breach as the biggest worry, ahead of a product recall or profit warning, it makes sense to partner with an organisation like Auxilion to help you make sense of these new changes. There can be a disconnect between what CFOs see and the rest of the board, which is why a simple, practical plan to help tackle risk management is key.

Technology is but one part of the puzzle and while approaches like password-less authentication - like touch ID and certification - are gaining popularity, they should be seen as pieces to a jigsaw. A CFO must be able to see the full picture before all the places fall into place. CFOs need to move the organisation from being reactive to proactive.
Reducing risk

Digital transformation is not simply reaching the destination but also considering where the journey brings you and the route you take. It is an ever evolving and challenging task. Moving from the familiar to the unknown can bring a number of challenges, no matter how much you research or prepare. With an experienced partner, that process can be smoother and seamless.

About the Cybersecurity Risk Assessment

Auxillion’s Cybersecurity Risk Assessment Service (CRAS) will identify any vulnerabilities within an organisation from a technology, human and compliance perspective, providing a clear risk score action plan to help organisations mitigate risks as they move the cloud and quickly digitally transform. This helps the C-Suite clearly understand and mitigate risk while providing the CIO/IT Manager with an easy to implement method of documenting progress in minimising vulnerabilities.

About Auxilion

Auxillion is an award-winning provider of I.T. services, delivering bespoke solutions for public and private organisations in the UK and Ireland. Auxilion’s range of I.T. services include; consulting, project management, project delivery and managed services. Backed by one of the largest project management teams in the country, we ensure the successful delivery of your IT projects, programmes and strategies.

As an award-winning Microsoft Gold partner, we deploy Microsoft technologies that improve agility and deliver growth for our clients. Through our ISO accredited and ITIL standard led service operations centres in Dublin and Sheffield, Auxilion delivers technology support to our clients 24/7, 365 days a year, so no matter where your people work, Auxilion is there to support them.

Our parent company, I.T. Alliance, is a trusted partner of the world’s leading outsourcing providers for over 20 years. This experience enables us to match the right technology to your business needs and provides access to a team of over 500 technical and project specialists. Our resourcing services team provides tried and tested IT and business professionals to clients across a wide variety of positions and industries.

Book Your Cyber Security Risk Assessment here.