G2L Oxygen

Optimise your Tech:
Optimise your Business

Your Company Name

Welcome to the G2L system health check: a free deep dive survey designed to evaluate systems and processes your business currently employs to form its technical and operation solutions.
IT systems and practices have a habit of evolving; this can leave an organisation vulnerable to:

- Incorrectly handled data
- The potential for personal, and professional liabilities
- Decreased business efficiency
- Unnecessary dependencies from third party software
- Legacy compatibility issues
- Hardware reliability challenges
- Network attacks

How does it work?

All information is treated in the strictest of confidence, however, if you would like to request an NDA, email us at NDA@g2l.uk or click the NDA link on the website.

This information is designed to create a robust structure for a half day consultancy workshop, where we discuss strengths and potential pain points, along with their solutions, and benefits of implication.

In most cases, the inability to answer a particular question, can actually be useful. Very often questions that are left blank allow us to focus on areas where you may need a little more support.

What happens next?

You will receive the results as a pdf., and the information within it can be used to help build strategies for IT policy decisions.

At G2L we specialise in helping organisations plan and implement IT strategies, you might want to book a half day workshop where we can expand on the survey with you.

We can help you create an IT policy document and help you source any additional technical support, resources, policies or procedure your company may need.

What is Covered in Oxygen?

Third Party System Reliance

One of the things we look at in the survey is a significant reliance on third party applications: if a company is reliant on a third party system for key data or decision making processes, this may present a vulnerability, that could cause problems in the future.

Third party applications are generally ‘add-on’ solutions to your in-house systems, with the update management processes beyond the control of your organization, this can sometimes present challenges to your IT departments.

Here are some common issues:

- Occasionally third-party application updates are not compatible with your organizational system logic: Result = time consuming troubleshooting, reconfiguration issues and staff re-training.
- A third-party application may be discontinued, leaving a system disparity.
- A serious application failure leaving you at the mercy of the company owning the application.
- The risk of compromising sensitive data.

The fewer third-party applications and processes incorporated into your organizations’ systems, the more robust those systems will be.

Backups

A backup policy, should clearly describe how a backup is performed, and where the backup’s are stored, this should form a large section of any disaster recovery procedure.

The next crucial aspect of any back-up process should be the procedure to recover critical systems in the event of a catastrophic failure.
It would be an advantage to know how quickly systems can be up and running, and the level of confidence there would be regarding the integrity of the recovered information?

The foundation of any bespoke business solution should begin with the analysis of critical system data, establish (verify) its source, and how it is to be used, this will form the building blocks for all that follows in terms of functionality and aesthetics.

Data

Even among large organizations it is common to find departments that cannot trust in the integrity of their data. They have multiple containers under several different formats, each with overlaps of information stored elsewhere. Their data is not stored in a properly normalized relational database, and there are numerous transcription errors due to the way the data is collected.

Under General Data Protection Regulations (GDPR), relevance is no longer even a choice, it is actually the law. But even if it were not, the success of a business is reliant on the correct data being collected, and the ability to disseminate that data to the right people, in a format that allows them to take an action or make a decision.

Data and Access Security

Ransomware attacks (along with other hacking techniques) are costing commercial and industry sectors millions in lost revenue annually, resulting in lost business hours, insurance claims, general operational inconvenience, as well as the challenges in customer confidence.

Simple steps can be taken to protect against such attacks, and should be implemented and maintained, and the survey will identify potential weaknesses in data security.

Data and Access Security

During the system check we ask a lot of question about your data, this is because companies in the UK still have to comply with (GDPR). Following Brexit, the UK passed laws that set the same requirements as the EU version of these regulations; therefore, it is as important as ever to understand and comply with these rules.

When considering these regulations, GDPR applies to data point of access, and not the point of origin.

A system hosted in America, with the data is used by people in Europe (point of access), that data would fall under the jurisdiction of GDPR. Whereas a system hosted in Europe (point of origin) exclusively for people in the US would not need to meet GDPR governance.

GDPR Principles

- Lawfulness, Fairness & Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity & Confidentiality
- Accountability.

Find out more

Location and Resource

Each point of access into any attribute of your business systems, is a potential node of vulnerability. The security of any system is only ever as strong as its weakest part. Training users on good housekeeping techniques is critical to mitigating these weaknesses, for example, not leaving logged in machines unattended, ensuring all personal devices (used to access business processes) are properly protected, and all passwords are properly maintained.

Our survey will help identify where points of vulnerability may exist, and allow us to provide guidance on ways to improve your systems and procedures.
In addition, your answers will allow us to ensure that your locations, including any home offices, are properly supported when and where needed to ensure the absolute minimum of system down time.

Software

The survey examines software by separating it into two different categories, commercial products. and bespoke solutions.
There are a number of reasons we examine software when looking at a company's IT policy, these reasons range from licensing through to the appropriate tools being used for the job: using the right software is fundamental to operational efficiency, and data integrity.

Data and Access Security

Hardware support (just like Software support) is another critical element to the effective operation of the organization, so it needs to be fit for purpose.

The range of hardware support should include laptops, desktops, and Macs. But not forgetting mobile devices and tablets, printers, and any embedded systems the organization uses.

Networks should be fit for purpose, with all points of access properly protected.

Start the healthcheck at www.g2l-oxygen.com

And Remember...

Don't be afraid to leave a question blank, if you don't know (or there doesn't seem to be an appropriate answer, that still tells us something that is of high value to our overall analysis of your current tech solutions.

Answers are submitted in complete confidence, and all information revealed will only be used to help have the best technology, policies, and procedures your organization will need for the foreseeable future.