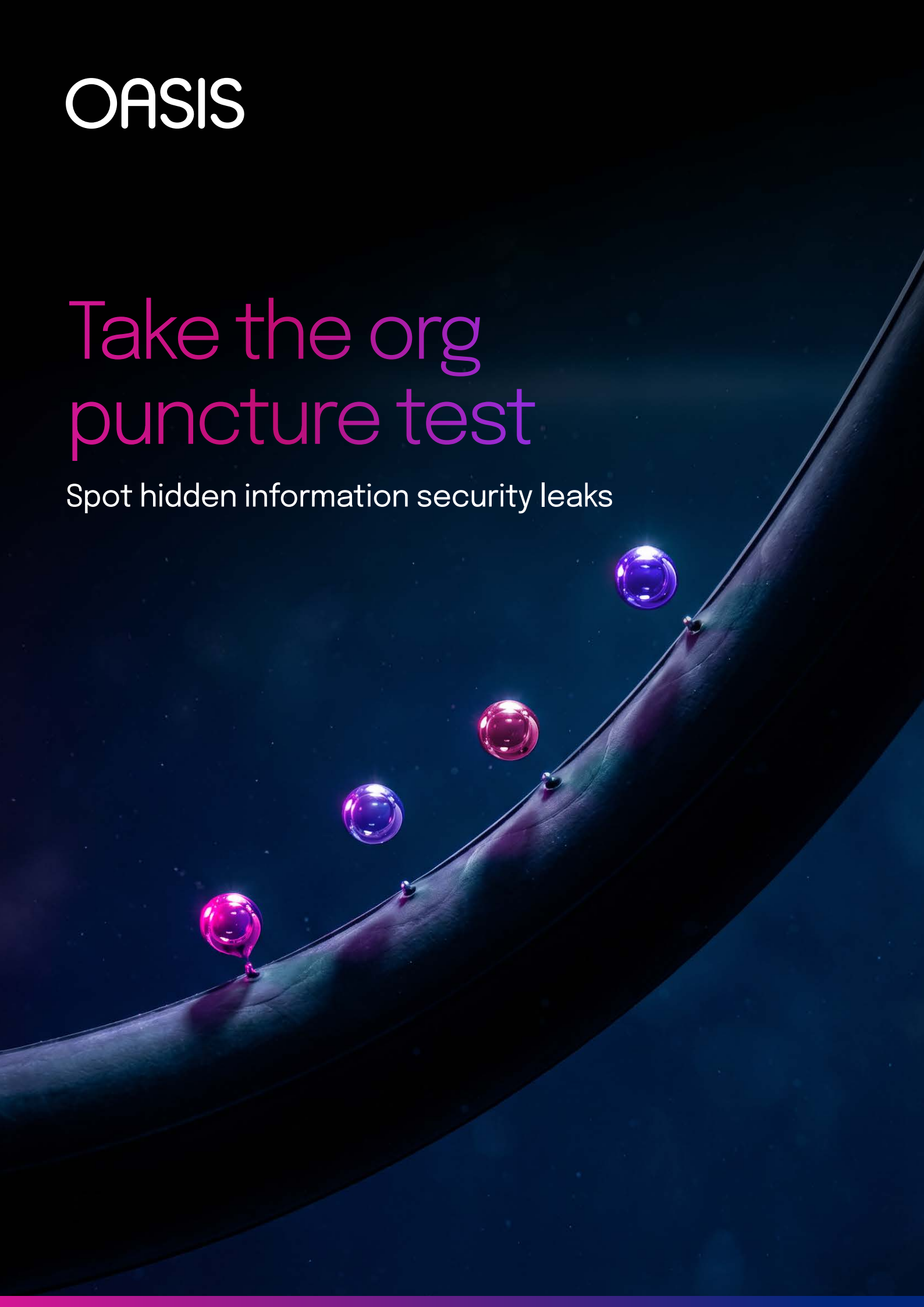
OASIS

Take the org puncture test

Spot hidden information security leaks



Information flows around your organisation like air in a bicycle inner tube.

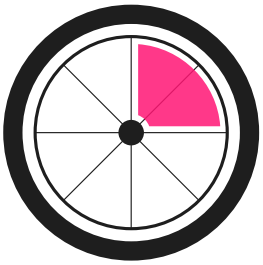
It's on paper. It's stored on servers. It's backed up on tapes. It's in the cloud. It's everywhere.

Keeping tabs on so many places is tough. One tiny breach could cause the whole organisation to collapse.

Take our test to find out where information could be bubbling out of your organisation. Then use our 4-step org puncture repair kit to seal up the gaps.

Quadrant one:

Physical documents



How secure are your processes for managing, moving and storing hardcopy documents and files?

Do you know what information you hold in hardcopy, and where?

Have you carried out a 'lift the lid' exercise to get an initial sense of what archive boxes, cupboards and deep storage hold?	Yes ☐	No ☐
Have you carried out a full audit of your document archive?	Yes ☐	No ☐

Is your information stored appropriately?

Are potentially business-critical or confidential files stored securely offsite to avoid fire or flood damage, theft, or the risk of being destroyed by mistake?	Yes ☐	No ☐
Are delicate or fragile documents kept in environmentally-controlled facilities?	Yes ☐	No ☐

Are your hardcopy documents retained and disposed of in line with regulations?

Are you confident paper files are being processed in line with data protection regulations - e.g. not stored longer than necessary?	Yes ☐	No ☐

Do your business continuity plans include hardcopy fallbacks?

Do you keep offline or paper copies of critical continuity plans (as recommended by many industry regulators)?	Yes ☐	No ☐
If yes to the above, are these copies stored securely offsite, but where they can be accessed quickly?	Yes ☐	No ☐
Do your business continuity plans allow for communication without email or other digital communications during IT outages?	Yes ☐	No ☐

Mostly yes?

Great work, no punctures here.

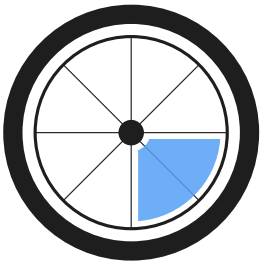
Mostly no?

Urgent action needed: Get in touch for no-obligation advice from our experts.

GET IN TOUCH

Quadrant two:

Scanned documents



Are your scanned and digitised documents opening you up to security issues?

Is your scanning process robust?

If you digitise paper documents, can you audit the full process, including receipt, scanning, file handling, and disposal of originals? Yes ☐ No ☐

If your documents are taken offsite for scanning, are they monitored at every transportation stage – i.e. kept in barcoded boxes and delivered in GPS-tracked vehicles? Yes ☐ No ☐

Is your information shared appropriately?

Once digitised, are your files shared securely – e.g. via secure email or delivered directly into your electronic document records management system (EDRMS)? Yes ☐ No ☐

Are your hardcopy documents scanned in line with regulations?

Are your documents scanned in line with BS 10008 standards: Legal Admissibility of Electronic Information, so they could be used in legal proceedings if necessary? Yes ☐ No ☐

Are you confident the originals are being stored or destroyed in line with data protection rules and other industry regulations? Yes ☐ No ☐

Mostly yes?

Great work, no punctures here.

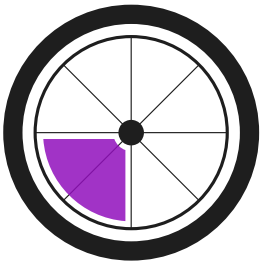
Mostly no?

Urgent action needed: Get in touch for no-obligation advice from our experts.

GET IN TOUCH

Quadrant three:

Digital documents



What procedures and systems govern the safe management of your digital files?

How do your teams collaborate on digital documents?

Are your employees trained and supported to share digital files in line with your security and compliance procedures?	Yes ☐	No ☐
Are you confident employees aren't bypassing unwieldy or unfit-for-purpose systems in order to speed up file-sharing?	Yes ☐	No ☐
If employees need to transfer confidential data, such as for audits, subject access requests (SARs), or freedom of information (FOI) requests, do you have the facility to provide a secure 'digital briefcase'?	Yes ☐	No ☐

Are your digital file management systems fit for purpose?

Do you have a document-sharing system designed for your organisation and industry (as opposed to a generic cloud-based tool)?	Yes ☐	No ☐
Are you able to apply access controls to your document management and sharing systems, so only authorised personnel can see confidential or sensitive data?	Yes ☐	No ☐

Is your data as secure and compliant as possible?

Is your data held within the UK, or if not, do your international data transfers comply with GDPR rules?	Yes ☐	No ☐
Do you have retention policies and automated disposal built into your systems so that data can be deleted in line with data protection and industry regulations?	Yes ☐	No ☐
Are you easily able to retrieve version control and other tracking data for audit purposes?	Yes ☐	No ☐

Mostly yes?

Great work, no punctures here.

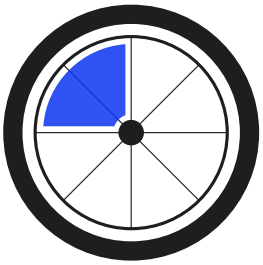
Mostly no?

Urgent action needed: Get in touch for no-obligation advice from our experts.

GET IN TOUCH

Quadrant four:

Data backups



Is your data backed up in such a way that it can't be lost or hacked?

How secure are your backups?

Have you put systems in place to ensure you're not 100% reliant on cloud data backups?	Yes ☐	No ☐
Is your backup 'air-gapped' – i.e. not accessible from any network, by being stored on tape at a secure, specialist, off-site facility?	Yes ☐	No ☐

Are your backups held in line with regulations?

Are you able to demonstrate to industry regulators that your critical data exists in an immutable, offsite, physically secured format?	Yes ☐	No ☐
Are you able to provide a documented chain of custody for your back-up tapes?	Yes ☐	No ☐

Are your backup procedures robust and reliable?

Are you confident documentation tracking your backup tapes is complete and accurate?	Yes ☐	No ☐
Are tapes monitored to make sure they're not used for longer than they should be?	Yes ☐	No ☐
Do you have a rotation schedule for your backup tapes?	Yes ☐	No ☐
Are your tapes stored in a purpose-built, climate-controlled facility with 24/7 monitoring?	Yes ☐	No ☐
Are your backup tapes securely destroyed in line with your retention rules?	Yes ☐	No ☐

Mostly yes?

Great work, no punctures here.

Mostly no?

Urgent action needed: Get in touch for no-obligation advice from our experts.

GET IN TOUCH

4 step puncture repair kit

How we can help you plug security gaps at every level.

Step one:
Physical documents

Confidential, sensitive, valuable or business critical hard copies should be stored offsite in professional facilities.

Physical documents stored with OASIS are:

- Catalogued and barcoded
- Protected from fire, flood or other damage
- Security monitored 24/7
- Tracked in transit
- Stored in vaults if they're high value or sensitive
- Available whenever you need them, via scan-on-demand or secure van delivery
- Securely shredded by vetted staff when no longer needed

Step two:
Scanned documents

Digitisation makes documents easier to search, share and manage. But they must be scanned correctly in order to minimise security risks.

OASIS scanning services include:

- High volume archive or back scanning
- Scan on receipt and digital mailrooms
- Robust quality control procedures
- Secure off-network backups to protect against hacking
- Secure delivery of digital files into your systems
- Integration with business continuity and recovery tools
- Documents scanned in line with BS 10008 standards: Legal Admissibility of Electronic Information

Step three:
Digital files

Providing the systems your employees need to securely view, share and manage documents is critical.

FileSmart:

- Converts your SharePoint Online into a powerful document management system
- Keeps all data within your own IT domain
- Offers policy-driven retention and automated disposal
- Creates full audit trails and compliance reporting
- Enforces naming, filing and version control
- Introduces granular access permissions
- Lets employees share files in a secure 'digital briefcase'

Step four:
Data backups

Keeping air-gapped data backups means you can be confident your information won't be hacked and can be easily retrieved for business continuity.

OASIS tape backups offer:

- Scheduled collections
- Secure, GPS-tracked transit
- 24/7 security monitored and climate-controlled offsite storage
- Structured tape rotation
- Full audit trail
- Certified destruction at end of life

OASIS

Ready for the road ahead?

If you need help sealing up potential security leaks, get in touch. Our specialists are ready to get your organisation back up to speed with airtight document management operations.

Get in touch

oasisgroup.com