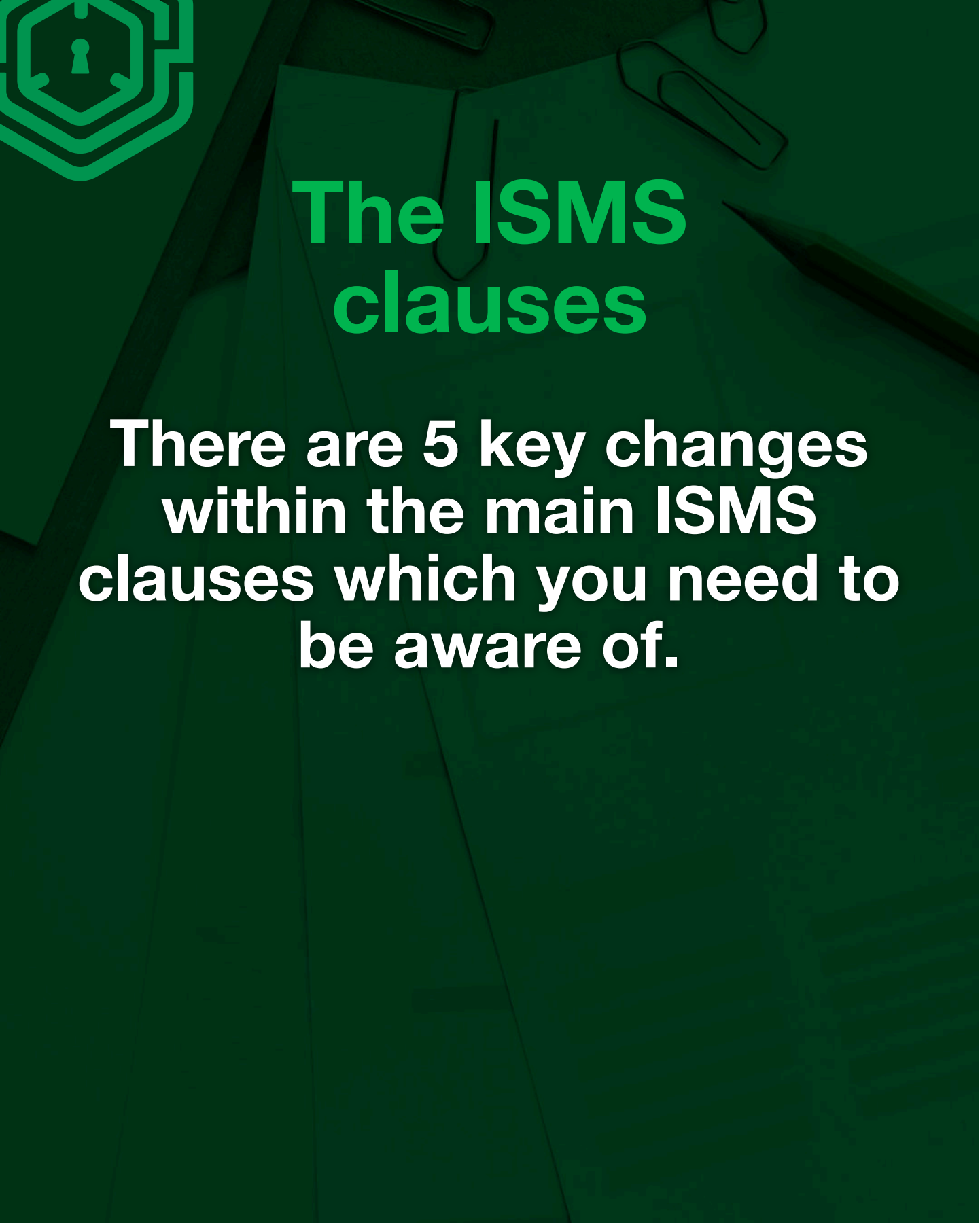
ISO/IEC 27001:2022

What changed in the new version?

2022 updates

In November 2022, a new version of ISO/IEC 27001 was released with a number of changes within both the ISMS clauses and Annex A controls.

So what changed?



The ISMS clauses

There are 5 key changes within the main ISMS clauses which you need to be aware of.

4.2c

Requirements of interested parties to be addressed

Any stakeholders that have interest in your ISMS and want to gain something from it, must have their needs identified and documented, including their expectations.

6.2

Information security objectives

You must have established security objectives and how you will achieve them.

They must also be monitored and available as documented information.

6.3

Planning of changes

Any changes to your ISMS need to be planned and plans must be documented.

8.1

Operational planning and control

Changes to 8.1 are purely wording, with no actual material changes that impact compliance.

Wording aligns with the broader scope of the standard beyond the term 'information security'.

9.3.2c

Changes in needs and expectations of interested parties

This aligns with the 4.2c change ensuring stakeholder's needs are continually assessed and is not a one-off task.

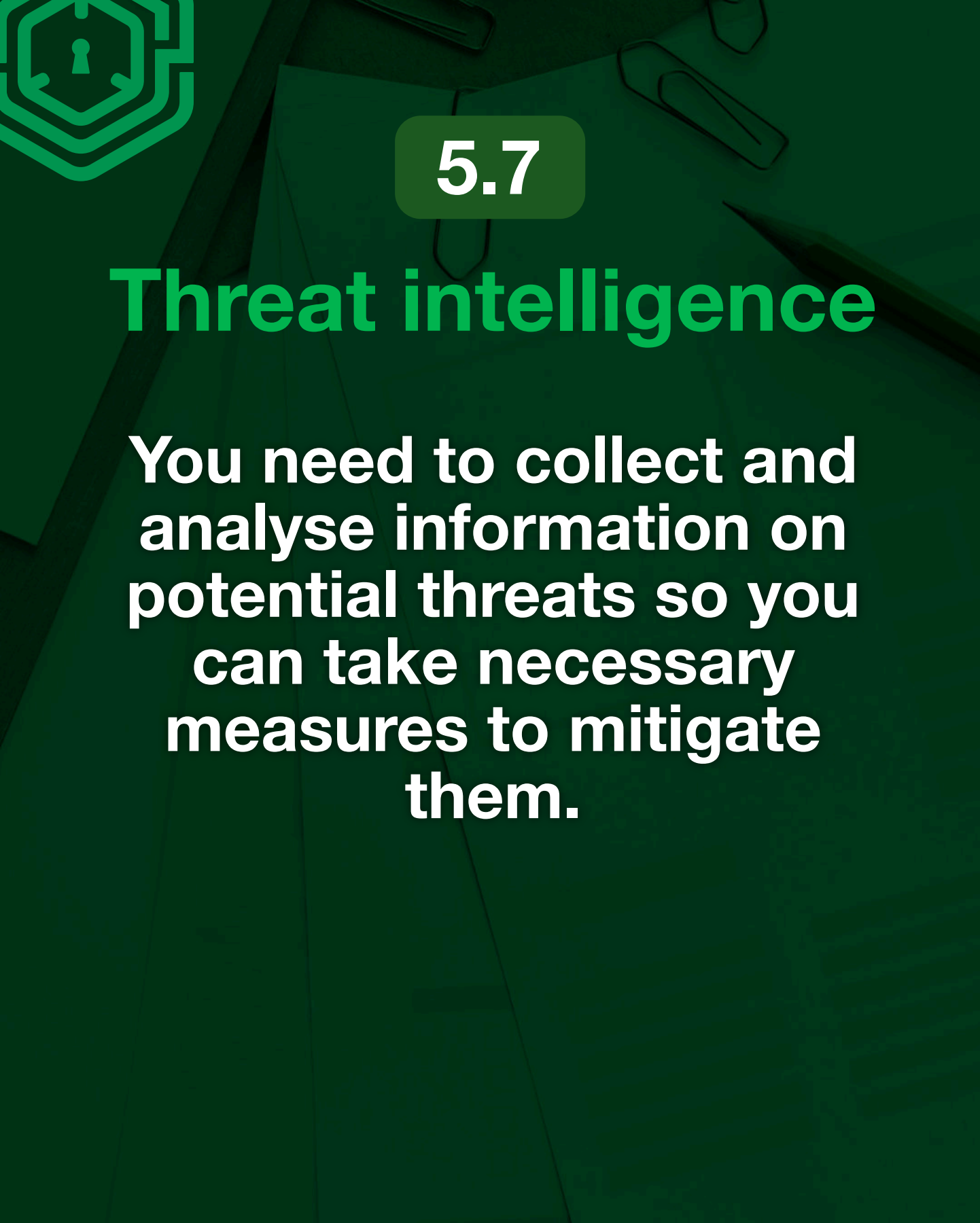
Annex A Structure

Annex A is now structured into 4 groups making control intent clearer:

1. Organisational controls
2. People controls
3. Physical controls
4. Technological controls

Annex A Controls

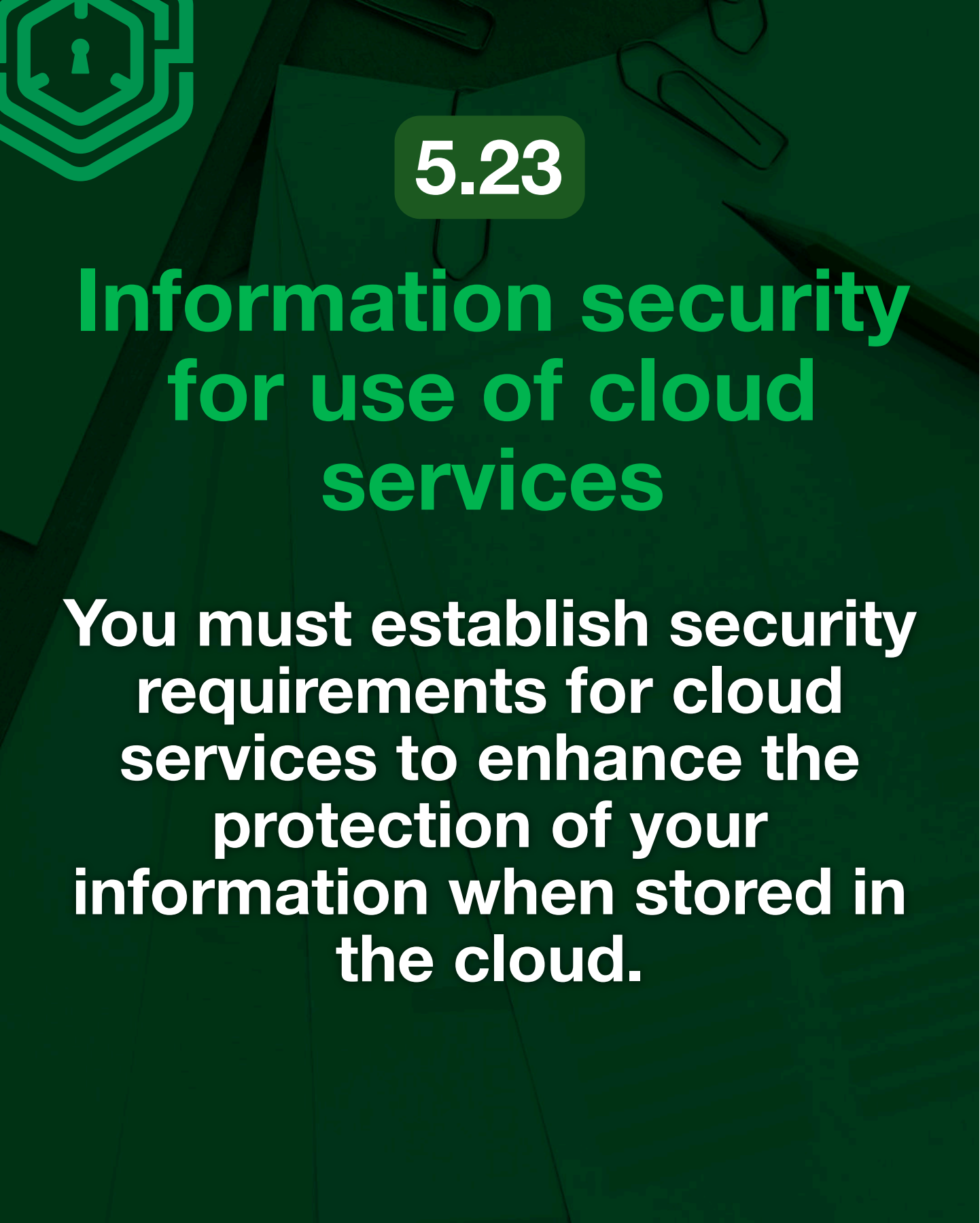
There are 11 new controls added to Annex A which address controls and control objectives of your ISMS.



5.7

Threat intelligence

You need to collect and analyse information on potential threats so you can take necessary measures to mitigate them.



5.23

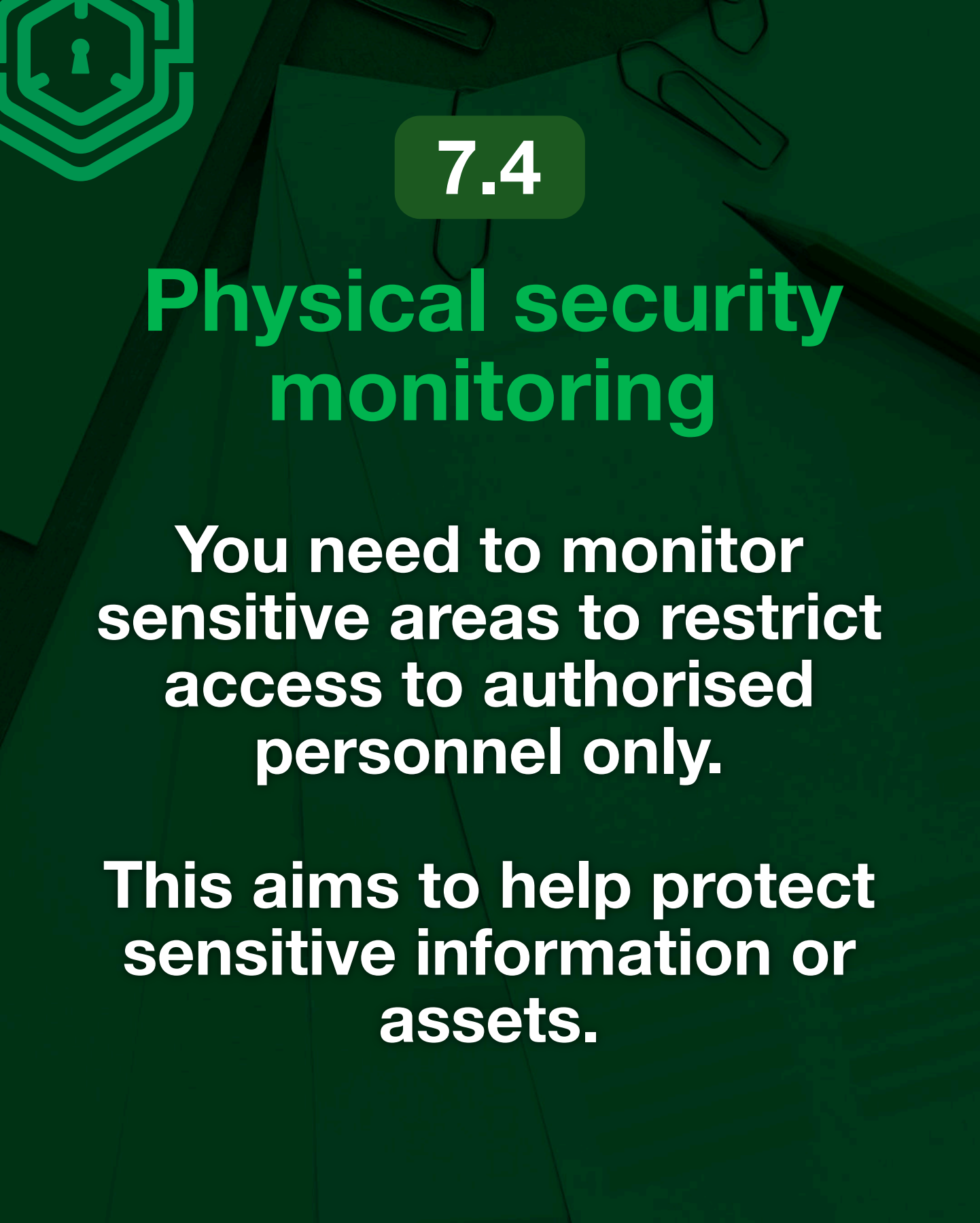
Information security for use of cloud services

You must establish security requirements for cloud services to enhance the protection of your information when stored in the cloud.

5.30

ICT readiness for business continuity

Your information and communication technology systems must be prepared to handle potential disruptions, ensuring that critical information and assets are available when required.



7.4

Physical security monitoring

You need to monitor sensitive areas to restrict access to authorised personnel only.

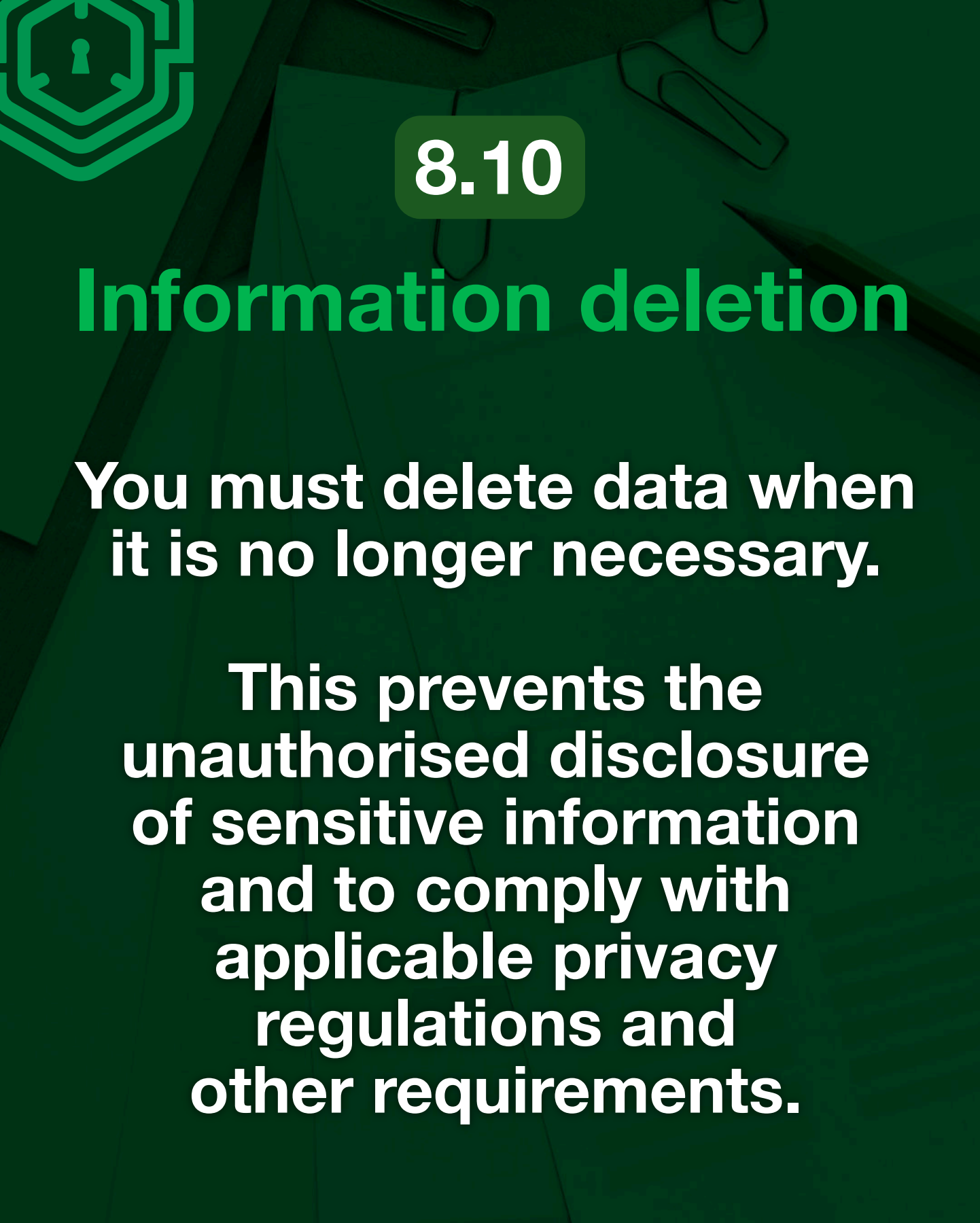
This aims to help protect sensitive information or assets.

8.9

Configuration management

You must manage the entire security configuration lifecycle of your technology.

This ensures a sufficient level of security at all times and prevents any unauthorised changes.



8.10

Information deletion

You must delete data when it is no longer necessary.

This prevents the unauthorised disclosure of sensitive information and to comply with applicable privacy regulations and other requirements.

8.11

Data masking

You must use data masking in conjunction with access control mechanisms to restrict the exposure of sensitive information, particularly personal data that is regulated by privacy laws.

8.12

Data leakage prevention

You need to apply data leakage prevention measures to prevent the unauthorised disclosure of sensitive information and to detect any such incidents in a timely manner.

8.16

Monitoring activities

You must monitor your systems to identify any unusual activities and take appropriate incident response measures if necessary.

8.23

Web filtering

You must manage and control which websites your users are accessing to protect your systems.

8.28

Secure coding

You must establish and apply secure coding principles to your software development processes to minimise security vulnerabilities in the software.

Want More Information?

For more detailed information about the changes in ISO/IEC 27001:2022, visit our insights page!

https://morrisec.com.au/insights

MORRISEC