DataGuard

INFORMATION SECURITY FOR BEGINNERS

How to best implement ISO 27001

YOUR SPEAKER

SOPHIE WILLIAMSON

Lead Auditor and Senior InfoSec Consultant

INTRODUCTION TO INFORMATION SECURITY AND ISO 27001

Information security covers all the ways an organisation protects their data and information that is stored and processed.

This includes policies and procedures to prevent unauthorised parties from accessing company information.
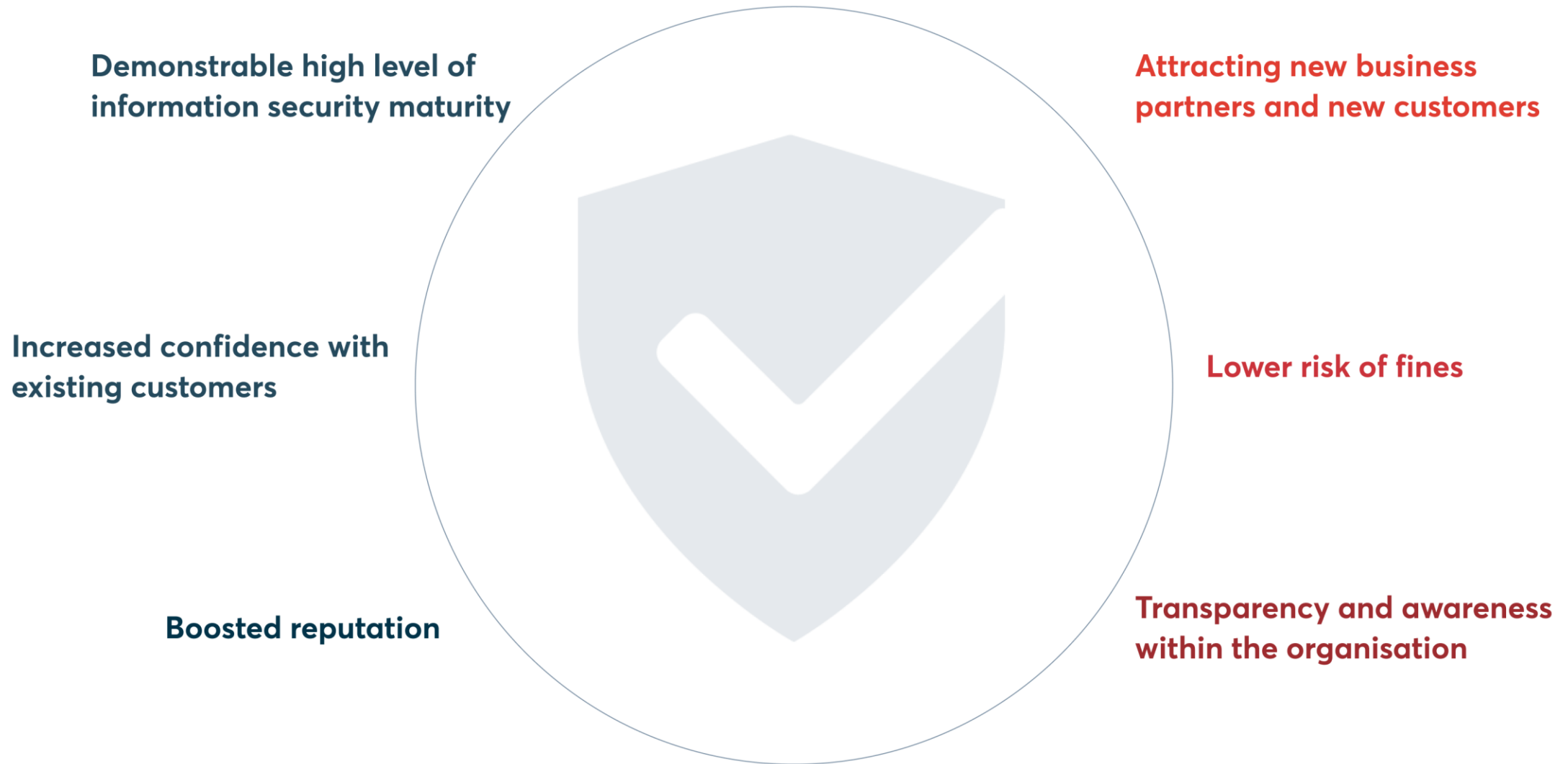
+ **Improved risk management and information security policies & procedures**

+ **Impact on organisational culture**

BENEFITS OF BECOMING ISO 27001-CERTIFIED

HOW AN ISO 27001 CERTIFICATION BENEFITS YOUR BUSINESS

Demonstrable high level of information security maturity

Attracting new business partners and new customers

Increased confidence with existing customers

Lower risk of fines

Boosted reputation

Transparency and awareness within the organisation

MAIN OBJECTIVES OF INFORMATION SECURITY

HOW TO BEST PROTECT YOUR INFORMATION

RISK ASSESSMENT & TREATMENT

Where do vulnerabilities exist and how can they be exploited?

How do we handle existing risks? (Treat, Accept, Delete, Transfer)

ASSET INVENTORY MAINTENANCE

Where is your information stored and processed?

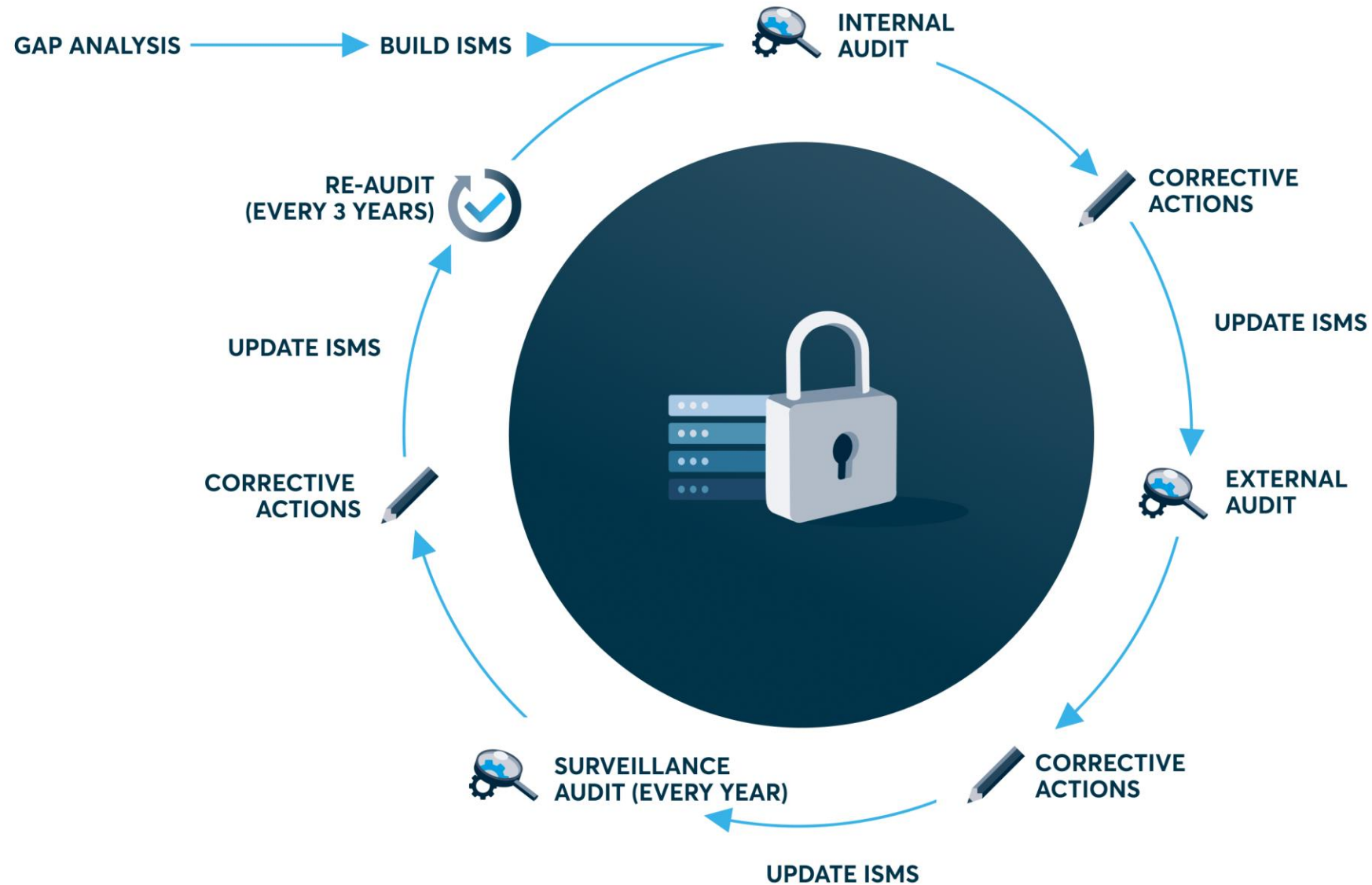Which equipment and software is being used?

PREPARING FOR AN EXTERNAL AUDIT & COMMON CHALLENGES

8 STEPS TO CERTIFICATION

Gap Analysis

1

Recommendations

2

Asset Management

3

Risk Management

4

Policies

5

Documentation

6

Internal Audit and Management Review

7

External Audit

1. Documentation Review
2. Review & evidence of controls

8

GETTING CERTIFIED

ISO 27001 IS A CONTINUOUS JOURNEY

GAP ANALYSIS → BUILD ISMS → INTERNAL AUDIT

CORRECTIVE ACTIONS

UPDATE ISMS

EXTERNAL AUDIT

CORRECTIVE ACTIONS

UPDATE ISMS

SURVEILLANCE AUDIT (EVERY YEAR)

CORRECTIVE ACTIONS

UPDATE ISMS

RE-AUDIT (EVERY 3 YEARS)

MANAGING YOUR ISMS POST-CERTIFICATION

MANAGING YOUR ISMS POST-CERTIFICATION

Using your information security management system (ISMS) as a reporting and checking tool:
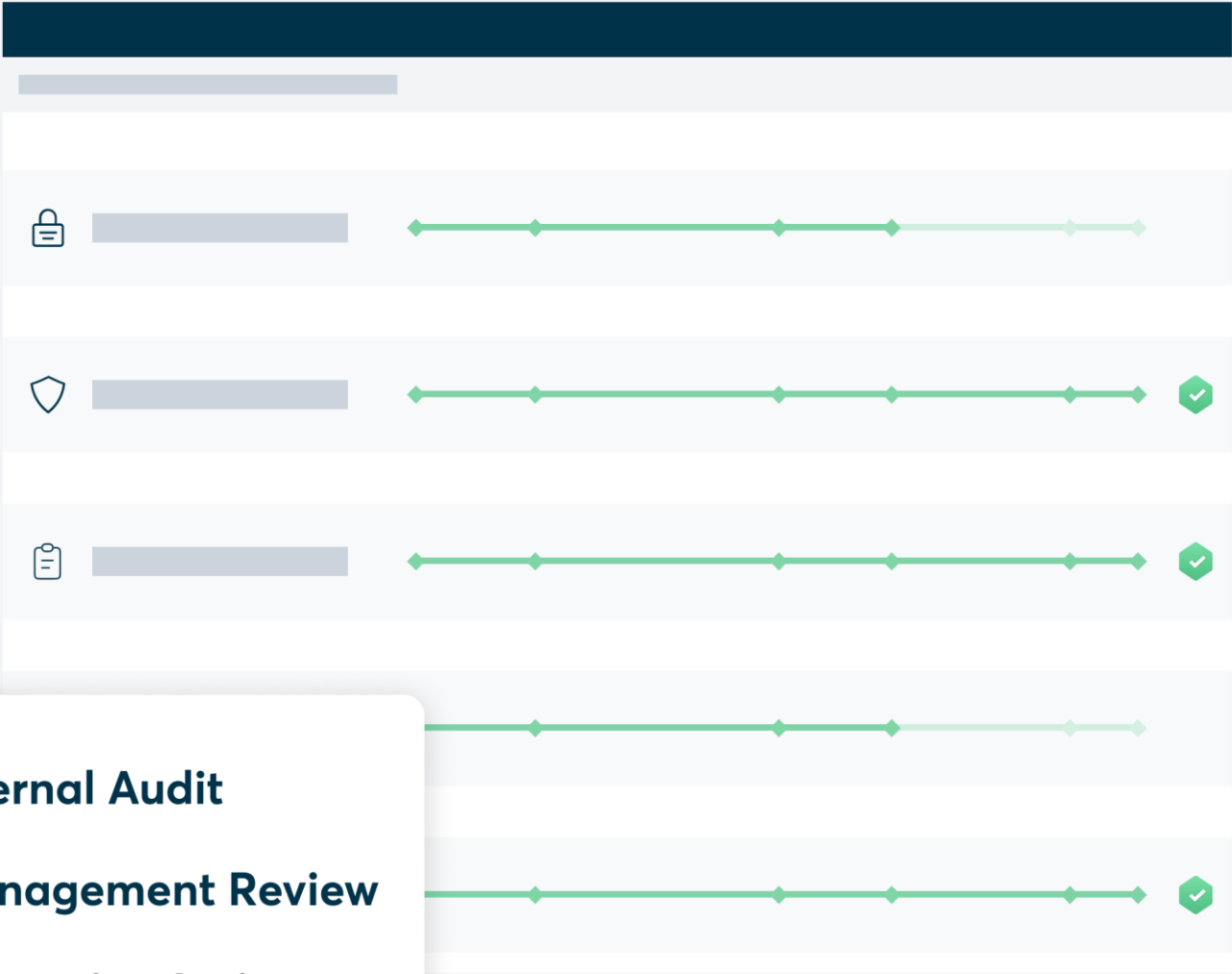
IMPORTANT STEPS

- ✓ **Build an internal audit programme**
- ✓ **Evidence the effectiveness of controls**
- ✓ **Perform management review meetings**
- ✓ **Review the output and KPIs of the ISMS**
- ✓ **Update the risk register and outstanding risks**

- ✓ **Internal Audit**
- ✓ **Management Review**
- ✓ **Corrective Actions**

KEY TAKEAWAYS FOR STRONGER INFORMATION SECURITY

**BE
PROACTIVE**

**INVOLVE
STAKEHOLDERS**

**BE
PREPARED**

SUCCESSFULLY IMPLEMENTING AN ISMS HELPS YOUR ORGANISATION
IDENTIFY, MANAGE, AND REDUCE THE RISKS TO BETTER PROTECT VALUABLE DATA.

ROADMAP:
ISO 27001
IMPLEMENTATION

dataguard.co.uk/download/iso-roadmap

EXPERT ADVICE
FOR YOUR ISO
CERTIFICATION

contact@dataguard.com