panaseer

18 crucial benchmarks for your cybersecurity control objectives and standards

Contents

Introduction

When it comes to cybersecurity governance, have you ever asked yourself: “What does good look like?” We hear this question a lot in conversations with customers and partners. They want to know if they’re meeting or exceeding industry norms.

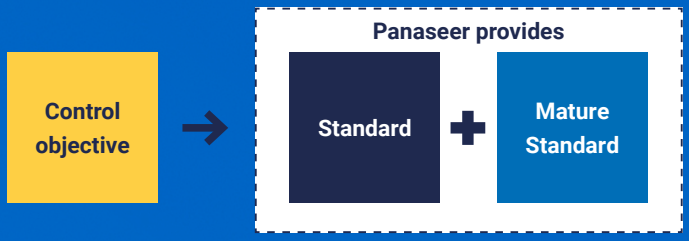
Discussing specifics around security governance is rare in the industry. Organizations are understandably reluctant to share details around security control objectives and related standards, in case they reveal vulnerabilities or weaknesses in security posture.

To help solve this problem, we’ve created a list of 18 benchmarks for cybersecurity controls and standards. It’s based on our own expertise and experience supporting cybersecurity posture management at some of the largest organizations in the world, as well as research and discussions with industry analysts, security experts, framework organizations such as CIS, and security communities.

This list will help you get a deeper understanding of your current security governance maturity and provides guidance on what you should be aiming for as you continue to improve your security posture management.

For each control objective, we provide an initial standard and a mature standard. The standard provides a guideline for how often measurements should be made, how quickly you should react, or the level or risk that should be accepted.

Once you’re successfully meeting the initial standard, you can further reduce the overall risk to your organization by working to achieve the mature standard.



By no means should organizations only use 18 control objectives, but these can help as a starting point and next steps for maturing your cybersecurity governance and measurement.

What are security control objectives and standards?

We've aligned these definitions to the Compliance Forge Reference Model[1], commonly referred to as the Hierarchical Cybersecurity Governance Framework (HCGF).

Standards are statements that explain what will be measured to comply with a control objective.

Control objectives are targets for the implementation of controls. Each is addressed by a standard.

1 ComplianceForge Reference Model: Hierarchical Cybersecurity Governance Framework (HCGF)
https://www.complianceforge.com/reasons/hierarchical-cybersecurity-governance-framework/

Controls coverage objectives

Measuring controls coverage shows the completeness of control deployment across your environment, answering the question: "Are my controls where I expect them to be?"

This helps give context and transparency to your measurement program, provides awareness of what information you can't capture, and indicates where gaps exist that need to be fixed.

> **To provide a high level of confidence in your overall security posture, you need to know that your controls are working effectively, and that you have 100% coverage where you expect them.**
>
> **You need to understand where the control gaps are in your environment.**
>
> David Fairman, CIO and CSO at Netskope

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
Expected EDR coverage	How many devices are covered by endpoint, detection, and response (EDR) tools?	Report into console every **7 days** (accounts for devices offline due to user vacations/downtime etc)	Report into console **every day** that device is seen on the network in another source
Expected CMDB coverage	How many devices are in the CMDB?	Servers and workstations report into CMDB every **7 days**	All devices reporting into CMDB **daily**
Expected AV coverage	How many devices are covered by antivirus tools?	Scan devices every **7 days** (accounts for devices offline due to user vacations/downtime etc)	Scan devices **daily** where device is seen on the network in another source
Expected vulnerability scanner coverage	How many devices are covered by vulnerability scanners?	Whole environment (all devices) scanned every **30 days**	Authenticated scan of all devices (but especially externally-facing infrastructure) every **7 days**
Expected patching tool coverage	How many devices are covered by patching tools?	Check every device is included in a patch cycle within every **30 days**	Check every device is included in a patch cycle within every **7 days**

It's important to note that changes can occur to the coverage standards when addressing specific active threats such as zero-day vulnerabilities.

Vulnerability and patch objectives

Vulnerabilities should be prioritized based on their criticality, with those that pose the biggest risk being fixed within the shortest timeframe.

As you mature and can identify additional prioritization factors, such as whether the vulnerability is being actively exploited or is present on an internet-facing or business-critical device, you may further develop and enhance the standard.

> **Unpatched vulnerabilities are often the entry doors to successful cyber-attacks. Any enterprise but also smaller organizations need to understand their attack surface and this includes not only IT but also IoT and OT.**
>
> Andreas Wuchner, Field CISO at Panaseer

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
Vulnerability patching SLA adherence	Are vulnerabilities patched within established thresholds?	Based on vulnerability properties. Remediate: ■ Critical/high vuln – **30 days** ■ Medium vuln – **90 days** ■ Low vuln – **180 days**	Based on vulnerability and device properties. Remediate: ■ Exploitable vulns on externally-facing or business-critical devices – **2 days** ■ Critical vulns on other server devices – **7 days** ■ Critical vulns on workstations, network devices and other devices – **14 days**

You can get a better understanding of the effectiveness of your patch management by highlighting patching that isn't completed on time. In other words, when your patch thresholds are breached. It can also be valuable to evaluate patch SLA breaches based on properties of the patch to be applied and the device. Organizations should aim to mature their standards based on several factors, including:

- Information you learn about the device (e.g. who owns it, whether it's internet-facing);
- Threat (exploit) associated with the vuln;
- Speed at which you can act as an organization (usually determined by your resources).

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
Patch SLA breaches	Are patches rolled out within established thresholds?	Based on patch properties. Patch: ■ Critical/high severity missing patch – **30 days** ■ Medium severity missing patch – **90 days** ■ Low severity missing patch – **180 days**	Based on patch and device properties. Patch: ■ Missing patches on externally-facing devices – **daily** ■ Missing critical patches on servers – **7 days** ■ Missing critical patches on workstations, network devices and other devices – **14 days**

Endpoint objectives

You should ensure endpoint controls are not only present on each asset, as highlighted by the “coverage” section, but also effective. You can do this by measuring whether antivirus signatures and EDR versions are up to date.

> **To provide a high level of confidence in your overall security posture, you need to know that your controls are working effectively, and that you have 100% coverage where you expect them.You need to understand where the control gaps are in your environment.**
>
> David Fairman, CIO and CSO at Netskope

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
AV signature updates	Are you running the latest version of antivirus?	Update **daily**	Update **daily**
EDR version	Are you running the latest version of EDR?	Device on latest policy minus three versions, evaluated **daily**	Device on latest version, excluding test versions, evaluated **daily**

User awareness objectives

Supporting a cybersecurity aware culture is an effective way to help stop many breaches. According to **Verizon's 2022 Data Breach Investigations Report**[2], 82% of data breaches involved a human element. So, the more your organization's employees are aware of cyber risks and how they affect the business, the safer your organization becomes.

While it can be difficult to measure a culture of user cyber awareness, it is essential to understand basics such as phishing to get the journey started.

> **"The difficulty is really caring about cybersecurity. The cyber awareness culture challenge is this: a lot of organisations think that the user is the biggest source of their security problems. If you see someone as a source of a problem, it's very different than if you think about empowering them to be an asset rather than a liability."**
>
> Andreas Wuchner, Field CISO at Panaseer

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
Phishing test coverage	How many employees are receiving phishing tests?	All employees tested **quarterly**	All employees tested **monthly**, except for repeat offenders who are targeted **weekly** until performance improves
Phishing test report rate	How many employees are successfully identifying and reporting phishing tests?	All employees reporting at least one test (frequency of reporting depends on how often employees are tested)	All employees reporting >20% of tests, where 20% is industry best (in finance, other industries lower)

2 Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/

Application security objectives

Application security is an integral part of any security measurement program. It's essential for security teams to ensure their applications are scanned for vulnerabilities with regularity, and that those vulnerabilities are remediated.

Security teams should identify critical applications and prioritize them because they pose a larger business risk, for example if they are internet-facing or house confidential data.

> **As a security professional, I'm always going to assume that threat actors are going to get past the first line of defence. And our applications act as a second line, so we need to ensure they are as secure as they can be.**
>
> Jim Doggett, CISO at Semperis

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
AppSec critical vulnerability detection SLA remediation	Are you remediating critical vulnerabilities in application security within the established threshold?	Remediate within **30 days**	Dependent on the application and its situation on the network. Remediate: ▪ Exploitable flaws on internet-facing applications – **2 days** ▪ Internet-facing applications – **14 days** ▪ Commonly targeted applications – **14 days** ▪ Other applications – **30 days**
Dynamic scan coverage	Are you dynamically scanning all applications for vulnerabilities?	Scan every **180 days**	Integrate into software development lifecycle - dependent on how quickly you develop and how critical the application is: ▪ All business-critical and internet-facing applications to be scanned every day where development is occurring
Static scan coverage	Are you statically scanning all applications for vulnerabilities?	Scan every **90 days**	Integrate into software development lifecycle - dependent on how quickly you develop and how critical the application is: ▪ All business-critical and internet-facing applications to be scanned every day, with subcomponent scanning in sprint for immediate feedback.
Penetration testing coverage	Are you running penetration tests on all applications?	Test every **365 days**, or when a major change occurs	Shorten test cycles for high-risk applications: for example, based on business-criticality of application or if application is internet-facing. Additional ad hoc scanning for major security-relevant development changes.

Identity & Access Management objectives

IDAM (Identity and Access Management) helps combat both initial breaches and lateral movement from threat actors that have already breached the organization.

Every employee will have multiple accounts for multiple applications, and all of those will have a password. Each poses a risk to the business.

Control objective	What are you measuring?	Initial measurement standard	Mature measurement standard
Account logon frequency	How often are employees logging in?	All accounts login to an asset every **90 days**	Based on account type and employee status. Logins: ▪ Active employees (I.e. not on extended leave) and standard user accounts – **30 days** ▪ Non-active employees and standard user accounts – **90 days** ▪ Service accounts – **90 days** ▪ Vaulted accounts – **365 days**
Password reset frequency	How often do employees change their passwords?	All accounts update passwords every **365 days**	Based on account type and employee status. Passwords reset: ▪ Active employees (I.e. not on extended leave) and standard user accounts – **90 days** ▪ Non-active employees and standard user accounts – **180 days** ▪ Service accounts – **365 days** ▪ Vaulted accounts – managed by vault
Active leaver	Are there active accounts that belong to an employee that has left the organization?	All accounts of terminated employees should be disabled within **3 days**	All accounts of terminated employees should be disabled the same day, unless date of termination occurs on a weekend/holiday then disablement should occur previous working day

How Panaseer can help improve your security posture

At Panaseer, we work with some of the most complex and advanced cybersecurity measurement programs in the world. We provide both the technology and the guidance they need to improve their security posture management.

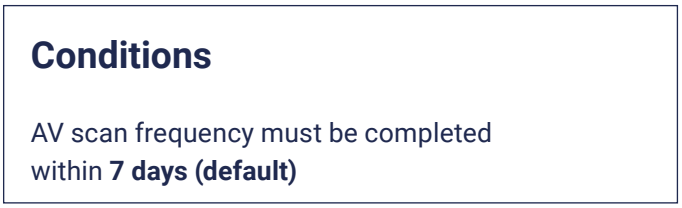
Our platform automates cybersecurity measurement, allowing organizations to continuously understand the effectiveness of their cybersecurity controls. It allows them to codify **control objectives** and automatically measure against **standards**. Organizations with advanced measurement programs can get detailed insight on things like control risk ownership, business risk, and historic trends.

Our team supports our customers to mature their security programs with guidance, best practices and actionable recommendations. We help by sharing our learnings in security measurement and posture management – how and what to measure, and what good looks like compared to industry peers.

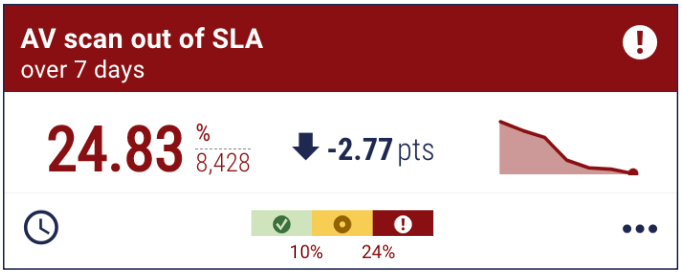
This helps organizations to stop preventable breaches by optimizing their security controls and proactively improving their security posture.

To find out how Panaseer can help your organization automate security measurement and improve the effectiveness of your controls, *request a demo* or get in touch with our Head of Security Performance Management, Charlotte Jupp.

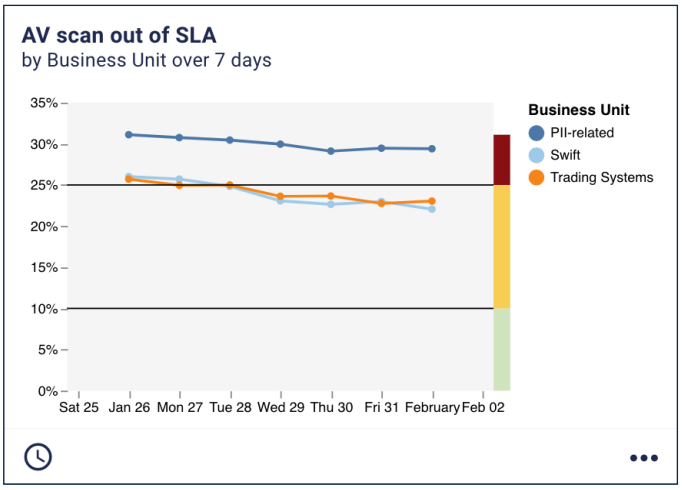
1. Set your conditions



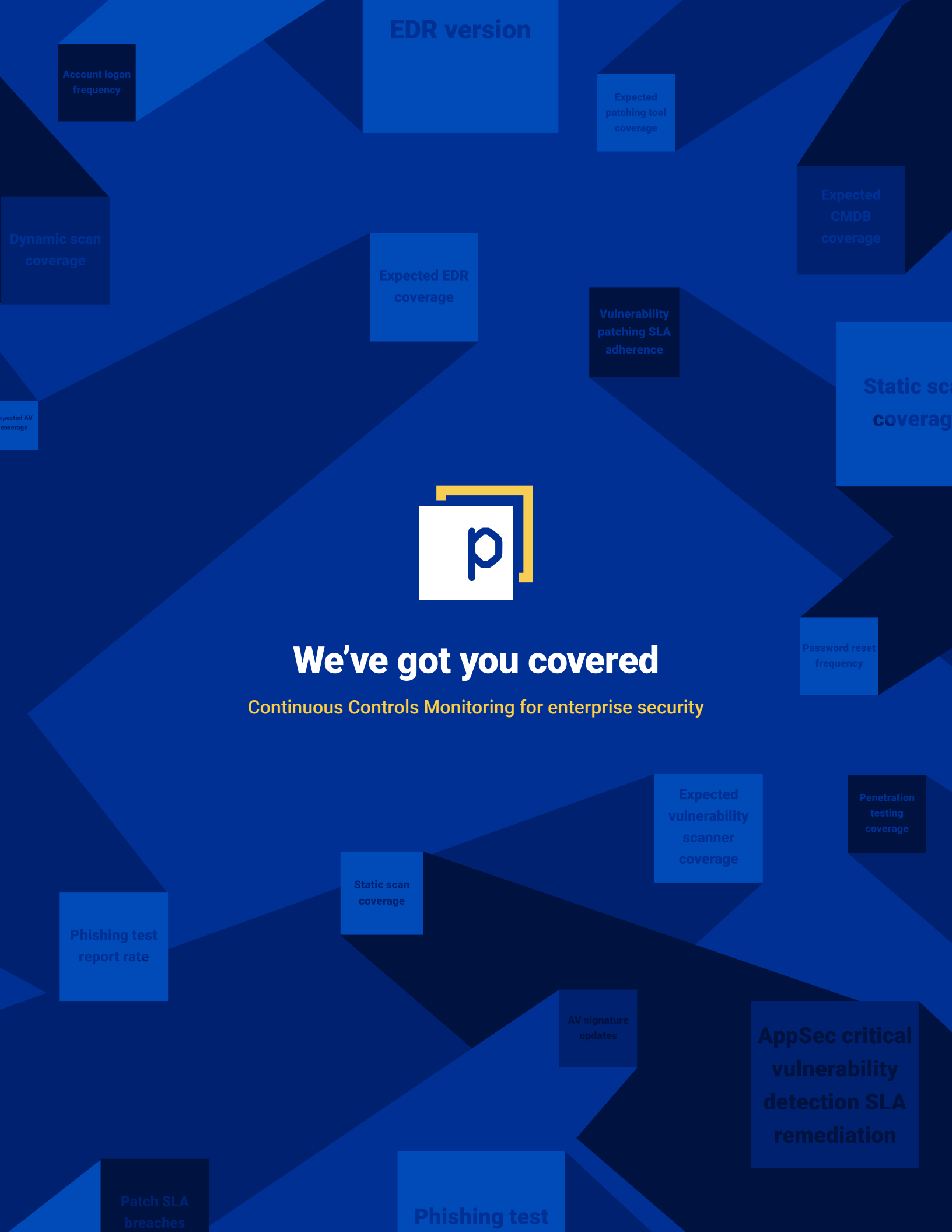
2. Monitor your adherence



3. Add business context



Charlotte Jupp
Panaseer's Head of Security Performance Management
charlotte.jupp@panaseer.com



We've got you covered

Continuous Controls Monitoring for enterprise security