

GOVERNANCE DOCS

PCI DSS v4.0.1

Gap Assessment Report

PCI DSS v4.0.1 Payment Card Industry Data Security Standard

Coastline Outdoor Retail (sample)

The cardholder data environment: the e-commerce checkout, 12 store tills and the payment integrations.

ASSESSED	25 September 2026
EDITION	June 2024
IN SCOPE	73 requirements, 71 applicable
PROFILE	Retail and e-commerce · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Coastline Outdoor Retail (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Coastline Outdoor Retail (sample) stands against PCI DSS 4.0

OVERALL READINESS

52.8%

Level 2 · Developing

The programme is under way, with material gaps an auditor would find.

Initial

Developing

Established

Audit-ready

APPLICABLE

71

EVIDENCED

14

OPEN GAPS

57

HIGH PRIORITY

23

STATUS OF EVERY REQUIREMENT

13

10

18

16

14

2

Not started

Planned

Partially implemented

Implemented, not evidenced

Implemented and evidenced

Not applicable

GAPS WITH AN OWNER

27 of 57

WITH A TARGET DATE

14 of 57

NOT ANSWERED

0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 52.8% against PCI DSS 4.0 across 71 applicable controls. 14 of them are implemented and evidenced.
- Most open gaps: Scope and validation, with 6 at 29%. Strongest area: Requirement 4 - Protecting data in transit at 100%.
- 16 controls are operating but not evidenced. Collecting their records alone lifts the score to 58.5% (+5.7 points), the cheapest gain available.
- 23 gaps are high priority (not started or only planned); 4 of them are in Requirement 9 - Physical access.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 4 high-priority gaps in Requirement 9 - Physical access	Risk Manager	Physical Security Policy
2	MEDIUM	Adopt and tailor the Roles and Responsibilities Matrix, which closes 7 open gaps	To assign	Roles and Responsibilities Matrix
3	LOW	Evidence the 16 controls that already operate (+5.7 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With an overall score of 52.8%, you must formalize scope validation and evidence existing controls to build measurable security.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

We currently stand at a readiness score of 52.8% at the Developing level, with 57 open gaps across 71 applicable requirements. Our primary exposure lies in 23 high priority gaps, especially within physical access, scoping, and network security controls. To address these vulnerabilities, we require leadership commitment to assign clear operational ownership across all unowned gaps. We must direct resource teams to finalize partially completed controls and document existing operational practices immediately.

WHERE YOU STAND

Your self-assessment places you at the Developing level with an overall score of 52.8%. Out of 71 applicable requirements, 57 open gaps remain, including 23 high priority gaps. Physical access stands lowest at 20%, followed by Scope and validation at 29.2%. Only 27 gaps have an assigned owner and only 14 have a target date. While Protecting data in transit reached 100%, the program has material gaps an auditor would find.

WHAT IT MEANS FOR THE ORGANIZATION

The distribution of statuses reveals clear operational momentum that lacks governance. While 14 requirements are implemented and evidenced, 16 are implemented without evidence and 18 are partially implemented. You are doing critical work in practice without the formal documentation necessary to demonstrate it. Operating with 13 unstarted controls and many unassigned gaps leaves foundational areas exposed. Evidencing what already runs would lift the score to 58.5%, while finishing partially implemented items would raise it to 71.1%.

WHERE TO FOCUS FIRST

Focus first on establishing boundary definitions and ownership across open findings. Addressing Scope and validation alongside Network security controls will establish a reliable baseline for cardholder data environments. Core documents such as the Roles and Responsibilities Matrix and the Network Security Policy address multiple high priority gaps simultaneously. Assigning owners and realistic target dates to all unassigned gaps will establish accountability and ensure steady execution across the 23 high priority gaps.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Define scope boundaries and segmentation validation SC.1 Merchant level or service provider level · SC.5 Segmentation	Unvalidated scope and missing segmentation leave cardholder data environments vulnerable to wider network breaches. This undermines all downstream technical safeguards.	Review network architecture diagrams against the segmentation criteria.	Network Security Policy PCI-DSS Toolkit - Comprehensive 180+ Templates	30 DAYS
2 Establish identity verification and access control standards 7.2 Access defined and assigned appropriately · 8.1 Identification and authentication processes documented · 8.3 Strong authentication	Gaps in authentication and access restriction expose critical systems to unauthorized entry. Restricting access by business need protects cardholder data from internal and external threats.	Draft baseline access requirements using the access control policy template.	Access Control Policy PCI-DSS Toolkit - Comprehensive 180+ Templates	60 DAYS
3 Deploy malware protection and anti-phishing safeguards 5.2 Preventing, detecting and addressing malware · 5.4 Anti-phishing mechanisms	Malicious software and phishing attacks represent immediate operational threats to payment data. Without formal policies and detection controls, systems remain exposed to automated attacks.	Inventory existing anti-malware tools and evaluate coverage against current policies.	Anti Malware Policy PCI-DSS Toolkit - Comprehensive 180+ Templates	60 DAYS
4 Formalize physical access and media handling controls 9.1 Physical access processes documented · 9.3 Personnel and visitor authorisation · 9.4 Media storage, distribution and destruction	Physical access scored lowest at 20% and presents tangible exposure to device tampering and media theft. Securing facilities prevents unauthorized physical interaction with cardholder assets.	Document visitor authorization procedures and secure area entry rules.	Physical Security Policy PCI-DSS Toolkit - Comprehensive 180+ Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS - Define scope boundaries and evaluate network segmentation using the Network Security Policy. - Assign accountable owners and completion deadlines to all unowned high priority gaps. - Gather and archive evidence for the 16 controls already operating in daily practice.	DAYS 31 TO 60 - Enforce access authorization rules and authentication procedures using the Access Control Policy. - Implement anti-malware and anti-phishing standards to protect endpoints and payment systems. - Complete documentation and testing for the 18 partially implemented security requirements.	DAYS 61 TO 90 - Implement physical access guidelines, visitor authorization rules, and secure media handling procedures. - Execute targeted risk analyses across customized controls and entity-defined review frequencies. - Standardize system component baselines and initiate required technical vulnerability scanning schedules.
--	--	---

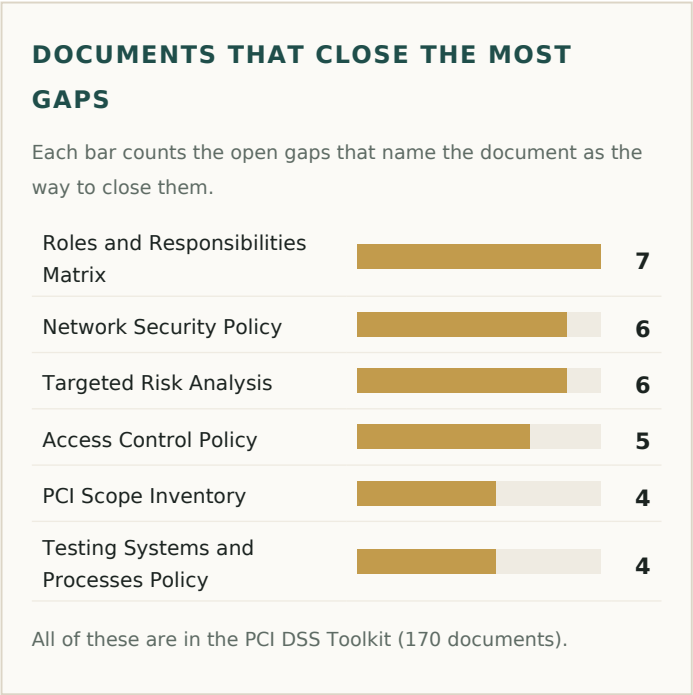
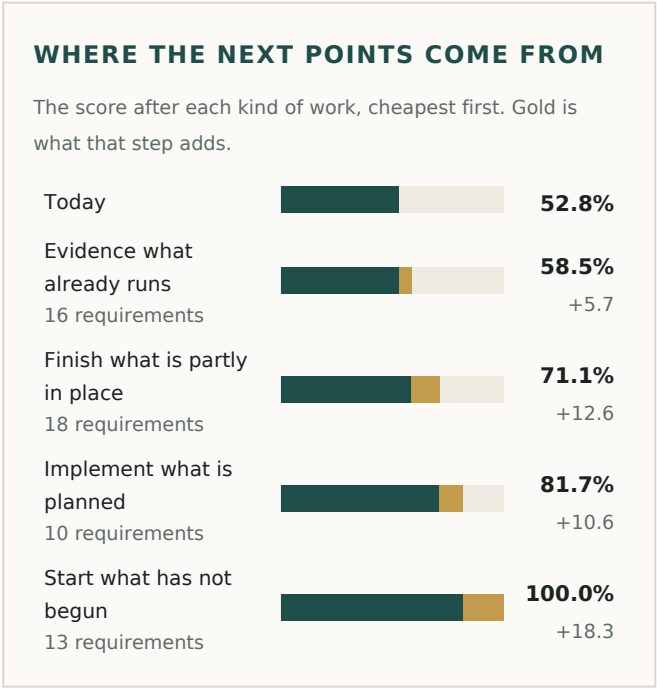
Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and validation	2 1 3	29%	3 3 0
Requirement 1 - Network security controls	1 2 1 1	45%	3 0 1
Requirement 2 - Secure configuration	2 1	58%	0 2 1
Requirement 3 - Protecting stored account data	2 2 1 2	61%	2 2 1
Requirement 4 - Protecting data in transit	2	100%	0 0 0
Requirement 5 - Malicious software	2 1 1	31%	2 1 1
Requirement 6 - Secure systems and software	3 1 1	45%	3 1 0
Requirement 7 - Access by business need to know	1 1 1	38%	1 0 1
Requirement 8 - Identity and authentication	2 1 2 1	35%	3 0 2
Requirement 9 - Physical access	3 1 1	20%	4 0 1
Requirement 10 - Logging and monitoring	3 2 2	71%	0 3 2
Requirement 11 - Testing security	2 2 2	75%	0 2 2
Requirement 12 - Policies and programmes	3 3 4	78%	0 3 3
Approach and risk analysis	2 1 1	31%	2 1 1

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

Where the next points come from



Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 13

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.1	Merchant level or service provider level	Scope and validation	To assign	PCI DSS Compliance Programme · PCI DSS Charter
SC.5	Segmentation	Scope and validation	Operations Manager	Network Security Policy · Penetration Testing Methodology
1.2	Network security control configuration	Requirement 1 - Network security controls	Risk Manager	Firewall and Router Policy · Change Management Policy +1 more
5.2	Preventing, detecting and addressing malware	Requirement 5 - Malicious software	To assign	Anti Malware Policy · Handling of Virus Attacks +1 more
5.4	Anti-phishing mechanisms	Requirement 5 - Malicious software	To assign	Email Policy · Safe Browsing and Web Filtering Policy +1 more
7.2	Access defined and assigned appropriately	Requirement 7 - Access by business need to know	Compliance Lead 4 Feb 2027	Access Control Policy · Access Review Procedure +1 more
8.1	Identification and authentication processes documented	Requirement 8 - Identity and authentication	Operations Manager 21 Jan 2027	Password Policy Statement · Roles and Responsibilities Matrix
8.3	Strong authentication	Requirement 8 - Identity and authentication	Compliance Lead	Password Policy Statement · Procedure for Reset of User Passwords
9.1	Physical access processes documented	Requirement 9 - Physical access	Risk Manager	Physical Security Policy · Roles and Responsibilities Matrix
9.3	Personnel and visitor authorisation	Requirement 9 - Physical access	Operations Manager 24 Dec 2026	Physical Security Policy · Guidelines for Working in Secure Areas +1 more
9.4	Media storage, distribution and destruction	Requirement 9 - Physical access	IT Manager 29 Oct 2026	Procedure for Management of Removable Media · Physical Media Transfer Procedure +1 more
AP.2	Targeted risk analysis for customized controls	Approach and risk analysis	To assign	Customized Approach Targeted Risk Analysis · Customized Approach Matrix
AP.3	Targeted risk analysis for entity-defined frequencies	Approach and risk analysis	To assign	Targeted Risk Analysis · Risk Assessment and Treatment Process

HIGH Planned · 10

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.3	Cardholder data discovery	Scope and validation	Operations Manager 21 Jan 2027	PCI Scope Inventory · Documentation Analysis Tool
1.4	Connections between trusted and untrusted networks	Requirement 1 - Network security controls	IT Manager 26 Nov 2026	Firewall and Router Policy · Network Security Policy
1.5	Dual-homed and remote computing devices	Requirement 1 - Network security controls	To assign	Mobile Computing Policy · Bring Your Own Device Policy +1 more
3.2	Minimising stored account data	Requirement 3 - Protecting stored account data	HR Manager 26 Nov 2026	Data Retention and Disposal Policy · Records Retention and Protection Policy
3.5	Rendering PAN unreadable at rest	Requirement 3 - Protecting stored account data	IT Manager	Cryptographic Policy · Encryption Key Management Guidance
6.2	Secure development of bespoke and custom software	Requirement 6 - Secure systems and software	Compliance Lead	Secure Coding Policy · Secure Development Policy +1 more
6.3	Identifying and addressing vulnerabilities	Requirement 6 - Secure systems and software	HR Manager	Technical Vulnerability Management Policy · Vulnerability Management Policy
6.5	Change management for system components	Requirement 6 - Secure systems and software	HR Manager 21 Jan 2027	Change Management Policy · Release and Deployment Management Process +1 more
8.6	Application and system account credentials	Requirement 8 - Identity and authentication	To assign	Access Control Policy · Targeted Risk Analysis +1 more
9.5	Point of interaction device protection	Requirement 9 - Physical access	HR Manager 12 Nov 2026	Card Reader Policy · Targeted Risk Analysis

MEDIUM Partially implemented · 18

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.2	Payment channels	Scope and validation	To assign	PCI Scope Inventory · Cardholder Data Policy Statement
SC.4	Cardholder data environment definition	Scope and validation	IT Manager	PCI Scope Inventory · Network Security Policy
SC.6	Third party service providers	Scope and validation	To assign	List of Service Providers · Shared Responsibility Matrix Version 4.0 +1 more
2.2	System component configuration standards	Requirement 2 - Secure configuration	To assign	System Hardening and Baseline Configuration Procedure · System Configuration Policy

2.3	Wireless environment configuration	Requirement 2 - Secure configuration	Compliance Lead 12 Nov 2026	Network Security Policy · System Hardening and Baseline Configuration Procedure
3.1	Stored account data processes documented	Requirement 3 - Protecting stored account data	Compliance Lead	Cardholder Data Policy Statement · Roles and Responsibilities Matrix
3.3	Sensitive authentication data not stored after authorisation	Requirement 3 - Protecting stored account data	Compliance Lead 12 Nov 2026	Cardholder Data Policy Statement · Documentation Analysis Tool
5.1	Malicious software processes documented	Requirement 5 - Malicious software	To assign	Anti Malware Policy · Roles and Responsibilities Matrix
6.4	Protecting public-facing web applications	Requirement 6 - Secure systems and software	Compliance Lead 7 Jan 2027	Web and Mobile Applications Security Standard · Testing Systems and Processes Policy
10.2	Audit logs implemented	Requirement 10 - Logging and monitoring	Compliance Lead 10 Dec 2026	Event Logging and Monitoring Policy · Systems Monitoring Policy
10.3	Audit logs protected	Requirement 10 - Logging and monitoring	To assign	Event Logging and Monitoring Policy · Access Control Policy
10.5	Log retention	Requirement 10 - Logging and monitoring	To assign	Event Logging and Monitoring Policy · Records Retention and Protection Policy
11.1	Security testing processes documented	Requirement 11 - Testing security	Operations Manager	Testing Systems and Processes Policy · Roles and Responsibilities Matrix
11.3	Vulnerability scanning	Requirement 11 - Testing security	IT Manager	Technical Vulnerability Assessment Procedure · Technical Vulnerability Management Policy
12.3	Risk management for the CDE	Requirement 12 - Policies and programmes	To assign	Targeted Risk Analysis · Customized Approach Targeted Risk Analysis +1 more
12.4	Compliance management	Requirement 12 - Policies and programmes	HR Manager	PCI DSS Compliance Programme · PCI DSS Charter +1 more
12.10	Incident response	Requirement 12 - Policies and programmes	Risk Manager 29 Oct 2026	Incident Response Procedure · Major Incident Management Process +1 more
AP.1	Defined or customized approach	Approach and risk analysis	HR Manager	Customized Approach Matrix · PCI DSS Guidelines and Implementation

LOW Implemented, not evidenced · 16

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
1.1	Network security control processes documented	Requirement 1 - Network security controls	To assign	Network Security Policy · Roles and Responsibilities Matrix

2.1	Secure configuration processes documented	Requirement 2 - Secure configuration	To assign	System Configuration Policy · Roles and Responsibilities Matrix
3.6	Cryptographic key protection	Requirement 3 - Protecting stored account data	To assign	Cryptographic Key Management Policy · Cryptographic Key Custodian Acceptance Form
5.3	Anti-malware kept active and current	Requirement 5 - Malicious software	To assign	Anti Malware Policy · Removable Media Assessment Guidelines
7.3	Access enforced through an access control system	Requirement 7 - Access by business need to know	To assign	Access Control Policy · User Access Management
8.4	Multi-factor authentication for CDE access	Requirement 8 - Identity and authentication	To assign	Password Policy Statement · Procedure for Remote Supplier Access to Systems
8.5	MFA system configuration	Requirement 8 - Identity and authentication	To assign	Password Policy Statement · Access Control Policy
9.2	Physical entry controls	Requirement 9 - Physical access	To assign	Physical Security Policy · Data Centre Access +1 more
10.4	Audit log review	Requirement 10 - Logging and monitoring	To assign	Procedure for Monitoring the Use of IT Systems · Systems Monitoring Policy +1 more
10.6	Time synchronisation	Requirement 10 - Logging and monitoring	To assign	System Configuration Policy · Systems Monitoring Policy
11.2	Wireless access point detection	Requirement 11 - Testing security	To assign	Testing Systems and Processes Policy · Network Security Policy
11.6	Payment page change detection	Requirement 11 - Testing security	To assign	Web and Mobile Applications Security Standard · Testing Systems and Processes Policy
12.5	Scope documentation and validation	Requirement 12 - Policies and programmes	To assign	PCI Scope Inventory · Inventory and Ownership of Assets
12.6	Security awareness education	Requirement 12 - Policies and programmes	To assign	Staff Training Programme · Information Security Communication Plan +1 more
12.8	Third party service provider risk management	Requirement 12 - Policies and programmes	To assign	Managing Service Providers · Supplier Management Policy +2 more
AP.4	Evidence and attestation readiness	Approach and risk analysis	To assign	Documentation Analysis Tool · PCI DSS Document Dashboard Version 4.0 +1 more

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com