Road to PCI DSS Compliance

Globomantics Gap Analysis Assessment

Department/Area: Customer Service, IT

Date of Assessment: 7/7/2025

Prepared By: J. Fluker

Reviewed By: C. M. Burns

OBJECTIVES

Goal of the assessment: To ensure compliance with the Payment Card Industry Data Security Standard across all departments.

CRITERIA & METRICS

List the criteria or standards being evaluated: Compliancy with PCI DSS requirements 8.3.5, 8.3.6, and 8.3.8.

Note: *Globomantics is in compliance with the other requirements except where determined not applicable.*

PCI DSS Requirement: 8.3.5

Defined: If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:

- Set to a unique value for first-time use and upon reset.
- Forced to be changed immediately after the first use.

Current State: Helpdesk analysts frequently reuse the same passwords.

Desired State: Helpdesk analysts use new and unique passwords for logging in and resetting user accounts.

Identified Gap: Helpdesk analysts don’t know or adhere to the requirement.

Priority: **Medium**

Gap Cause [Lack of Knowledge, Skill, and/or Practice]: Knowledge -- Helpdesk analysts are unaware of requirement. Practice -- Helpdesk analysts haven't adopted the requirement.

Method used to Identify Gap: Direct observation of screen logs during assessment.

Action Plan/Next Steps: Restrict the procedure for selecting a unique password to one effective method to reduce severity of brute force attacks. Ban the re-use of temporary passwords to protect against certain cyber attacks such as phishing and to avoid multiple security breaches.

Implementation Status [Fully/Partially/None]: Fully

Resources: Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 © 2006 - 2022, page 173

PCI DSS Requirement: 8.3.6

Defined: If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

Current State: Globomantics' policy 14.2 only requires a minimum password length of 8 characters, resulting in a weaker security strategy.

Desired State: Globomantics adopts the PCI DSS standard of a minimum password length of 12 characters.

Identified Gap: The minimum password length is below standard, allowing a greater chance for the success of brute force and dictionary attacks.

Priority: **Medium**

Gap Cause [Lack of Knowledge, Skill, and/or Practice]: Knowledge: Globomantics may be unaware of the standard.

Method used to Identify Gap: Interviews with key personnel and direct observation of screen logs.

Action Plan/Next Steps: Increase the minimum password length from 8 to 12, not just to meet compliance, but to defend against dictionary and brute force attacks.

Implementation Status [Fully/Partially/None]: Fully

Resources: Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 © 2006 - 2022, page 174

PCI DSS Requirement: 8.3.8

Defined: Authentication policies and procedures are documented and communicated to all users including:

- Guidance on selecting strong authentication factors.
- Guidance for how users should protect their authentication factors.
- Instructions not to reuse previously used passwords/passphrases.
- Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

Current State: Globomantics' Acceptable User Policy (AUP) as well as the training course it provides does not advise its employees to not reuse passwords. It also doesn't provide any instructions for employees to change passwords/passphrases if there is any suspicious activity or knowledge that the password/passphrases have been compromised, and how to report an incident.

Desired State: Globomantics provides training and advises its employees to not reuse passwords, provides instructions for employees to change compromised passwords/passphrases and how to report an incident.

Identified Gap: No clear policy or training concerning changing passwords or who to report a suspicious incident to.

Priority: **High**

Gap Cause [Lack of Knowledge, Skill, and/or Practice]: Knowledge -- Inadequate training; no clear policy.

Method used to Identify Gap: Interview with Head of Learning and Development, company policy and other documentation.

Action Plan/Next Steps: Update the Acceptable User Policy and training material to instruct employees to change passwords/passphrases if they notice any suspicious activity or know of any password/passphrases that have been compromised. Employees should also have clear instructions/documentation on how to report suspicious activity, ensuring everyone remains informed should an incident occur.

Implementation Status [Fully/Partially/None]: Fully

Resources: Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 © 2006 - 2022, page 176

For more information about the requirements: www.pcisecuritystandards.org/