

Risk Assessment

Dealership risk assessment template, covering what the FTC Safeguards Rule asks for in 16 CFR 314.4(b).

Dealership and rooftops covered

Owner (Qualified Individual)

People who took part

Assessment date

Next assessment due

How to use it. Fill it in at one sitting with your general manager, controller, F&I director, service director and IT. Walk the building before you score anything. Score each risk with the grid in section 4, list it in the register in section 6, sort by score, and put a name and a date, or a signature, on every row. Date it and keep every version.

1 Scope and owner 314.4(b), (b)(1)

Which stores, departments, systems, paper files and vendors this assessment covers, and who owns it. The Qualified Individual oversees the information security program.

Stores and departments covered

Systems, paper and vendors in scope

Owner (Qualified Individual)

Approved by (owner or general manager)

2 Where customer information lives 314.4(b), (c)(2)

Every system or place that holds customer information, or can reach it. Walk the building. Include paper and the phone system if it records calls.

System or place	Customer information it holds	Who can get in	Vendor
DMS			
CRM and BDC tools			
F&I menu and e-contracting			
Credit bureau and lender portals			
Email and Microsoft 365			
File server and scanned deal jackets			
Paper deal jackets and old deal files			
Backups			
Phone system and call recordings			
Website forms and chat			
Other			

3 Threats you can see coming 314.4(b)

Reasonably foreseeable risks to customer information, from inside the store and outside it. Add your own.

Threat	Inside or outside	Seen here or nearby?	Systems it touches
Phishing for email or DMS logins			
Ransomware			
Breach at a vendor that holds customer data			
Fake bank-detail change on an invoice			
Shared or never-removed logins			
Departing employee takes customer data			
Paper files left out or unlocked			
Lost or stolen laptop or phone			
Other			

4 Scoring criteria 314.4(b)(1)(i)

Decide what each level means before you score. Score = likelihood x impact, from 1 to 9. Suggested cut-offs: 6 or 9, fix with a name and a date. 3 or 4, fix or sign off. 1 or 2, accept in writing.

Level	Likelihood means, at this store	Impact means, at this store
1 Unlikely / Minor		
2 Possible / Serious		
3 Likely / Severe		

Likelihood / impact

Minor (1)

Serious (2)

Severe (3)

Likely (3)

3

6

9

Possible (2)

2

4

6

Unlikely (1)

1

2

3

5 Confidentiality, integrity and availability 314.4(b)(1)(ii)

For each system, rate 1 to 3 how much it matters that the data stays private, stays accurate and stays reachable. Then judge the controls already in place.

System	Confidentiality	Integrity	Availability	Existing controls	Enough? Y/N
DMS					
CRM					
F&I and e-contracting					
Email					
File server					
Backups					
Paper files					

Risk register

Section 6. One row per risk, sorted by score. L = likelihood, I = impact, score = L x I.

[illegible]

7 Mitigate or accept 314.4(b)(1)(iii)

Every risk gets a decision. Mitigate means a named person, a fix and a due date. Accept means an owner or general manager signs with a reason. Required safeguards such as multi-factor authentication and encryption cannot be accepted away unless the Qualified Individual approves an equivalent control in writing.

Risk #	Mitigate or accept	Fix, or reason for accepting	Owner, or signed by	Date

8 Vendors that hold your data 314.4(f)(3)

Assess each service provider on the risk it presents. Ask for evidence of its safeguards and check the contract for security terms.

Vendor	What it holds or can reach	Security terms in contract?	Last review
DMS provider			
CRM			
Credit bureau connection			
E-contracting or F&I platform			
IT and security provider			
Payroll			
Website and chat			
Other			

9 Where the results go 314.4(c), (d)(2), (e)(1), (i)

What changed because of this assessment: safeguards, the scope of penetration testing and vulnerability scans, training topics, and the written report to the board or owner.

Safeguards added or changed _____

Pen test scope this year _____

Vulnerability scan scope _____

Training topics updated _____

Report to board or owner, date _____

10 Reassess 314.4(b)(2), (g)

Reassess at least once a year, and again after a new store, an acquisition, a DMS conversion, a new vendor holding customer data, or a security event.

Reassessment owner _____

Changes that trigger an early one _____

Next assessment date _____

Signed (owner or general manager) and date _____

Want a second set of eyes on your register?

Bring it to a complimentary IT and cybersecurity assessment.

heliontechnologies.com/it-assessment/

Based on 16 CFR 314.4(b), Standards for Safeguarding Customer Information, as of October 2026. Dealerships with customer information on fewer than 5,000 consumers are exempt from the written assessment under 314.6, but the program must still be based on a risk assessment. This template is a planning aid, not legal advice. © 2026 Helion Technologies.