

ERISA Cybersecurity
What Plan Fiduciaries Should Know

November 2026

forvis mazars

Today’s Presenters



Ben Sady
Principal, IT Risk & Compliance
804.474.1267
ben.sady@us.forvismazars.com

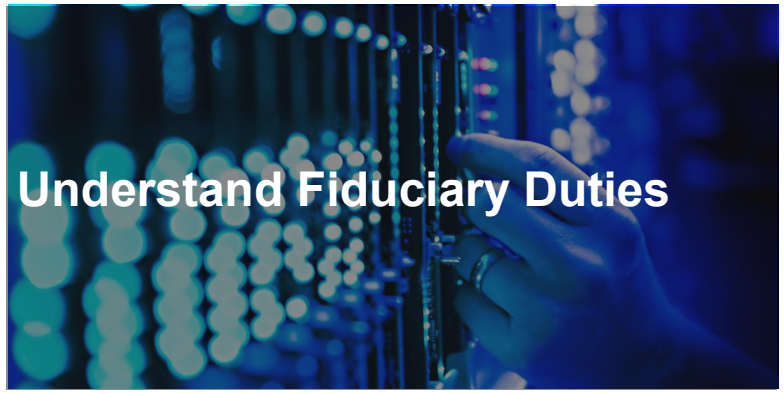


Nancy Ozuna
Partner, Professional Services Group – EBP Leader
210.268.1921
nancy.ozuna@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Learning Objectives

Our discussion today builds toward one of these three objectives.



Describe key fiduciary considerations related to Employee Retirement Income Security Act (ERISA) cybersecurity.



Identify information used to evaluate plan and service-provider cyber risk.



Recognize documentation that supports ongoing cybersecurity oversight.

© 2026 Forvis Mazars, LLP. All rights reserved.

Why This Matters Now

1. In 2024, the Department of Labor (DOL) clarified that its 2021 cybersecurity guidance **applies to all ERISA-covered plans**.
2. In 2026, the **DOL communicated that its EBSA investigations will prioritize cybersecurity**, including reviewing how plans and service providers protect their systems and data from cyber threats.
3. As a result, **plan fiduciaries are expected to prudently assess cybersecurity risk, oversee service providers, and maintain defensible documentation** – even where controls are largely operated by vendors.
4. **What we're seeing in practice**, is a shift from '*our vendor handles it*'… to '*we need to show how we oversee and document this in a defensible way.*'

Sources: "Compliance Assistance Release No. 2024-01," dol.gov; "US Department of Labor's Employee Benefits Security Administration updates national enforcement projects for employee benefit plans," dol.gov.

POV

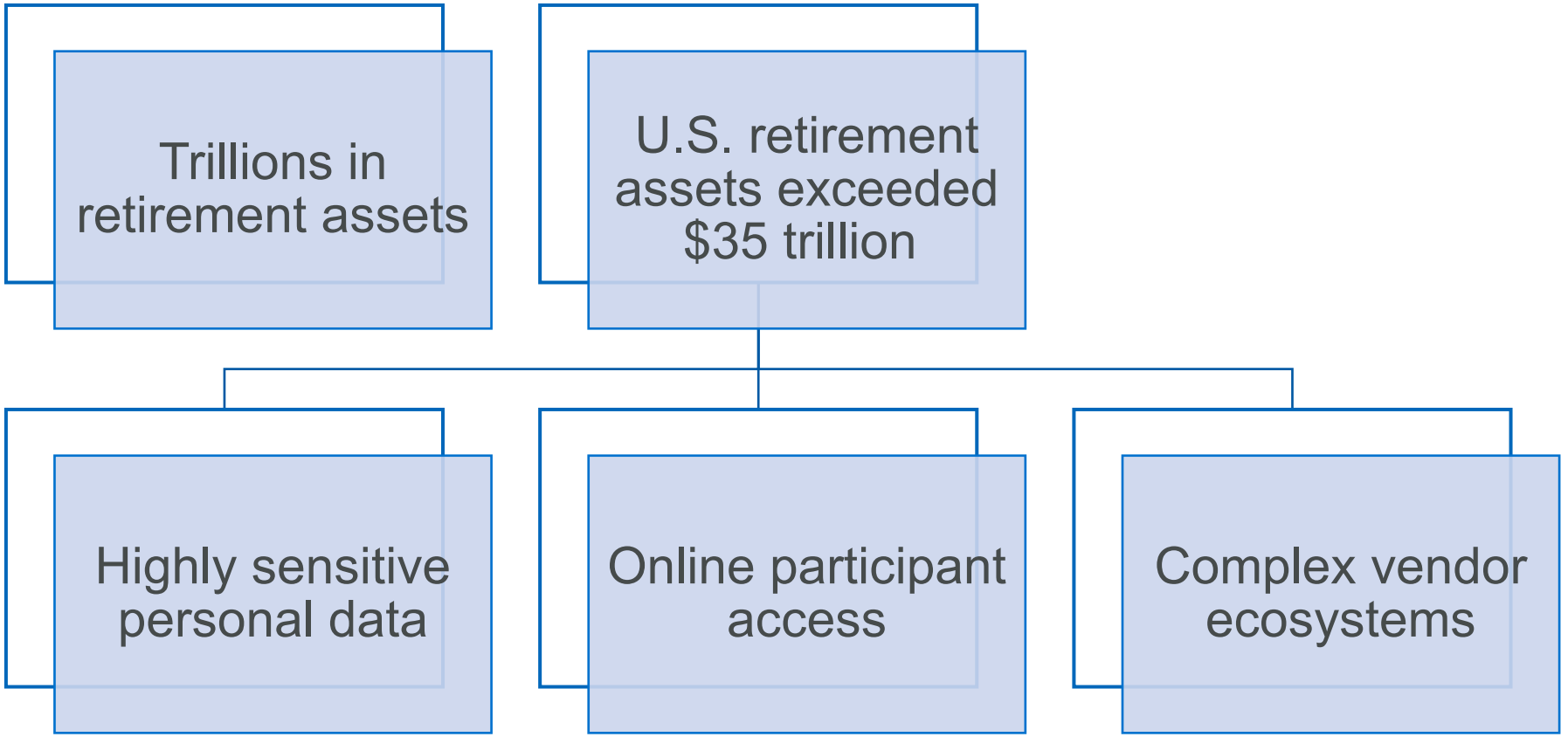
The DOL's cybersecurity guidance update (2024) and EBSA investigation priorities (2026) confirm that plan fiduciaries are expected to prudently assess cybersecurity risk, determine how the guidance applies to their plan environment, and implement controls commensurate with that risk.

While approaches may be right-sized based on plan complexity and reliance on service providers, fiduciaries should be prepared to demonstrate how their decisions were informed, documented, and aligned with the DOL's guidance.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Why Cybercriminals Target Benefit Plans



© 2026 Forvis Mazars, LLP. All rights reserved.

Plans & Cybersecurity

When something goes wrong, regulators will want to know:

Were the fiduciaries prepared?

Were there reasonable protections in place?

Was oversight of the plan documented?

Cybersecurity is not just an IT issue – it's a fiduciary oversight issue.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

DOL Cybersecurity Guidance – Key Themes

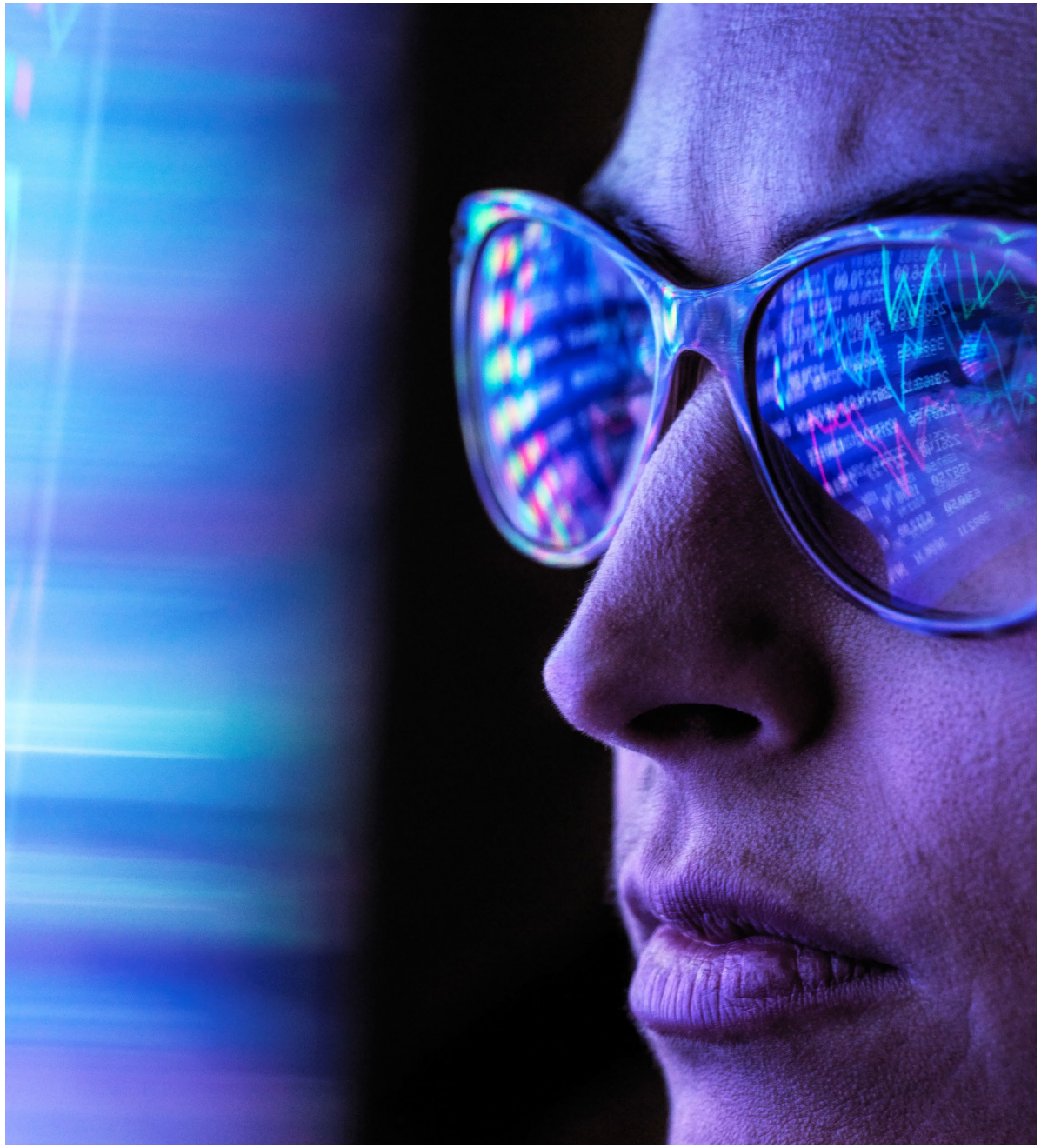
- Documentation matters
- Demonstrate vendor oversight
- Maintain an incident response plan
- Use multi-factor authentication and encryption
- Treat cybersecurity as tied to fiduciary duties

© 2026 Forvis Mazars, LLP. All rights reserved.

01

The DOL’s Cybersecurity Expectations

What the guidance says, who it applies to, and the 12 practices the DOL expects plans and their service providers to follow.

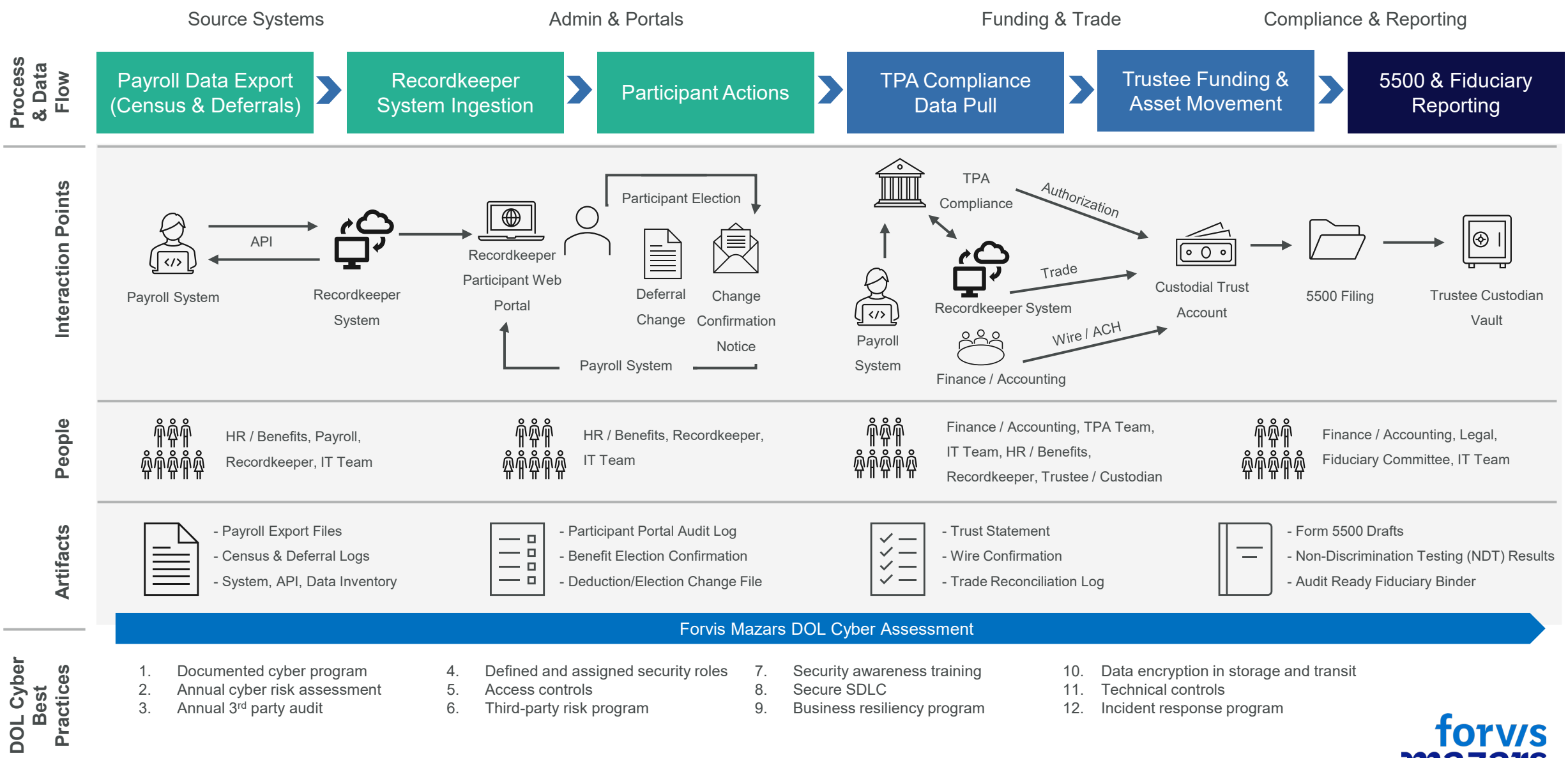


The DOL's 12 Cybersecurity Program Best Practices

- Documented cyber program
- Annual cyber risk assessment
- Annual third-party audit
- Defined and assigned security roles
- Access controls
- Third-party risk program
- Security awareness training
- Secure SDLC
- Business resiliency program
- Data encryption in storage and transit
- Technical controls
- Incident response program

© 2026 Forvis Mazars, LLP. All rights reserved.

The Benefit Plan Ecosystem



© 2026 Forvis Mazars, LLP. All rights reserved.

Gaps We Typically See

Organizations can build on existing strengths through documentation, assessment, and demonstrated controls.

What Organizations Have Today



Enterprise Cyber Controls



SOC Reports & Vendor Managed Controls

What They May Be Missing



A plan-specific view: assessment, vendor oversight, & evidence tied to the 12 DOL areas

© 2026 Forvis Mazars, LLP. All rights reserved.

Potential Gaps & How to Close Them

Plan Scope

Plan systems, data, and vendors never defined as in scope

Define the plan environment and bring it into scope

Risk Assessment

No plan-specific cybersecurity risk assessment

Assess annually and document it

Data Inventory

Plan systems and data flows undocumented

Inventory systems, data, and vendors

Coordination

IT owns cyber; HR and finance own the plan relationships

Name a coordinator; record decisions in committee minutes

Vendor Oversight

SOC reports (usually) collected but not always reviewed

Review, document exceptions, track them

Shared Duties

Unclear split between sponsor and vendors

Agree in a documented responsibility matrix

Contracts

Vendor agreements not catalogued or reconciled

Catalog agreements and reconcile them with the responsibility matrix

Evidence

Documentation, decisions, and assumptions are not organized

Keep documentation in an audit-ready file

© 2026 Forvis Mazars, LLP. All rights reserved.

A Right-Sized Approach to DOL Cybersecurity Expectations

Aligned to DOL expectations for documenting, assessing, and demonstrating cybersecurity risk.

1. Document

- Document benefit plan IT environment
- Identify systems, data, & vendors
- Clarify roles & responsibilities

Common starting point

2. Assess

- Evaluate cybersecurity risk
- Align to DOL expectations
- Identify key risk themes & gaps

Typical assessment approach

3. Demonstrate

- Benefit plan program documents
- Demonstrate vendor oversight
- Maintain defensible documentation

Bringing it together

Our approach is flexible and right-sized, allowing organizations to start where appropriate and scale based on plan complexity, risk, and fiduciary needs.

© 2026 Forvis Mazars, LLP. All rights reserved.

Connecting the Pieces
A Complete DOL Cybersecurity Program

Common answers – “we have an enterprise security program,” “we get vendor SOC reports,” “we completed a vendor questionnaire” – are each valuable yet only one piece of a complete program.

Document	Assess	Demonstrate
Enterprise security program & policies	Benefit-plan-specific cyber risk assessment mapped to DOL	Documentation showing how the org is addressing applicable DOL cybersecurity program areas
Benefit plan IT environment, systems & data inventory	Vendor SOC report review	
Defined internal security roles & responsibilities	Vendor security questionnaires	
Shared responsibility matrix with vendors	DOL cyber applicability scoping	

- Documented cyber program
- Annual cyber risk assessment
- Annual 3rd party audit
- Defined and assigned security roles
- Access controls
- Third-party risk program
- Security awareness training
- Secure SDLC
- Business resiliency program
- Data encryption in storage and transit
- Technical controls
- Incident response program

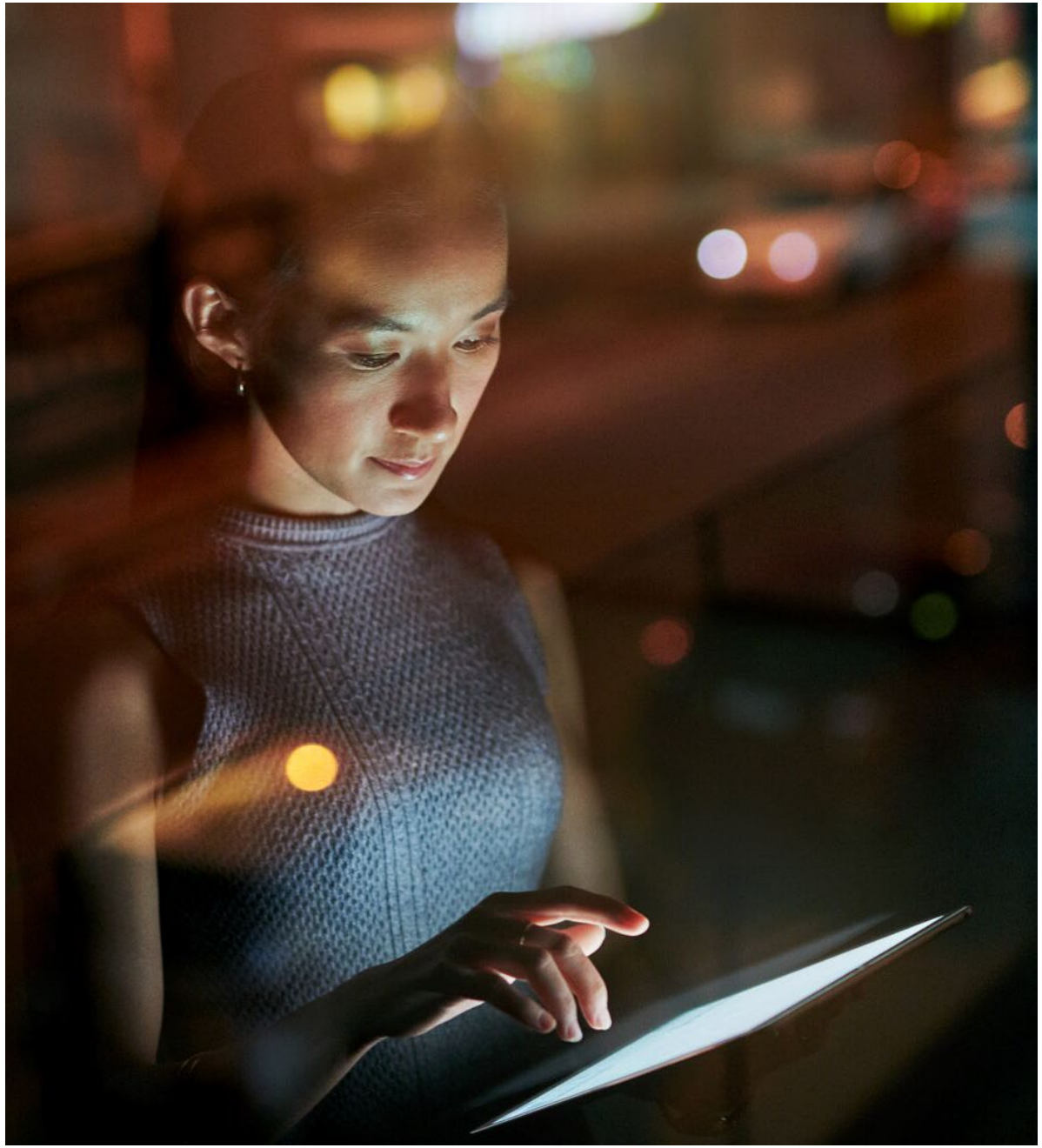
Key takeaway: the three phases should work together—and the risk assessment is the single step that sets all three in motion. That’s where we go next.

© 2026 Forvis Mazars, LLP. All rights reserved.

02

Evaluating Risk & Oversight

A discussion of how a risk assessment can help organizations address the DOL’s 12 cybersecurity program areas.



It Starts With a Risk Assessment
Your Highest-Value First Step

Scope	**Assess**	**Map to the 12**	**Remediate**
Confirm which plans the DOL guidance applies to and which systems, data, and providers sit inside each plan's boundary.	Evaluate the inventoried processes, systems, data flows, access, and third parties against the threats that actually face benefit plans.	Identify which of the DOL's 12 cybersecurity program best practices are met, partially met, or missing.	Prioritize the gaps by risk, assign an owner and a date to each, and record what the committee reviewed and decided.
Output: a documented scope statement per plan	**Output: a plan-specific cyber risk assessment**	**Output: a gap analysis across the 12 areas**	**Output: a remediation plan & an audit-ready file**

The assessment is the second best practice. To perform it you must document vendors, data flows, owners, and contracts, and score yourself against the 12 areas. One exercise, many birds.

© 2026 Forvis Mazars, LLP. All rights reserved.

Document Your Environment
The Assessment Drives This Inventory

1 **Plans in Scope**
Each ERISA-covered plan, including health & welfare
Artifact: a named list of plans & who sponsors each

2 **Processes**
Enrollment, payroll feeds, contributions, distributions, claims
Artifact: a process map with owners at each step

3 **Systems**
Payroll, HRIS, recordkeeper, TPA, trustee, & participant portals
Artifact: a system inventory tied to each process

4 **Data**
Participant PII, census files, elections, balances, & bank details
Artifact: a data inventory showing what moves & where it rests

5 **Third Parties**
Each provider & subcontractor that touches plan data
Artifact: a vendor register with the data each one holds

6 **Data Flows**
How files move between payroll, recordkeeper, TPA, & trustee
Artifact: documented interfaces, methods, & transfer controls

7 **Security**
Who can view or change plan data, internally & at providers
Artifact: an access list covering privileged and vendor accounts

8 **Ownership**
Who is accountable across HR, IT, finance, & the committee
Artifact: named owners documented for each area

© 2026 Forvis Mazars, LLP. All rights reserved.

A Practical Framework

Each element here is either an input to or an output of the risk assessment.

- Plan Scope & Applicability
- Systems, Data & Vendor Inventory
- Roles & Ownership
- Plan-Specific Risk Assessment
- Mapping to the 12 DOL Areas

ERISA Plan Cyber Program

Right-sized to plan complexity & provider reliance

- Vendor Due Diligence & SOC Review
- Contracts & Shared Responsibility
- Incident Response & Resiliency
- Committee Minutes & Evidence

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

What the Risk Assessment Can Deliver
One Assessment, Three Returns

What We Did

- Scoped which plans and providers the DOL guidance applies to
- Inventoried plan systems, data, vendors, and data flows
- Evaluated controls against the threats facing benefit plans
- Mapped the results to each of the DOL's 12 best practices
- Prioritized gaps with named owners and target dates

Best Practices

- The DOL expects a prudent annual risk assessment of the plan environment
- This is a plan-specific assessment, not an enterprise-wide one
- It is documented, dated, and repeatable year over year
- The committee has a decision record showing what was reviewed and why

What You Also Get

- A documented overview of the benefit plan ecosystem
- A documented view of how you stand against all 12 areas, not just #2
- A vendor register and a shared responsibility view for contracts
- Named owners across HR, IT, finance, and the committee
- A remediation roadmap you can budget and schedule

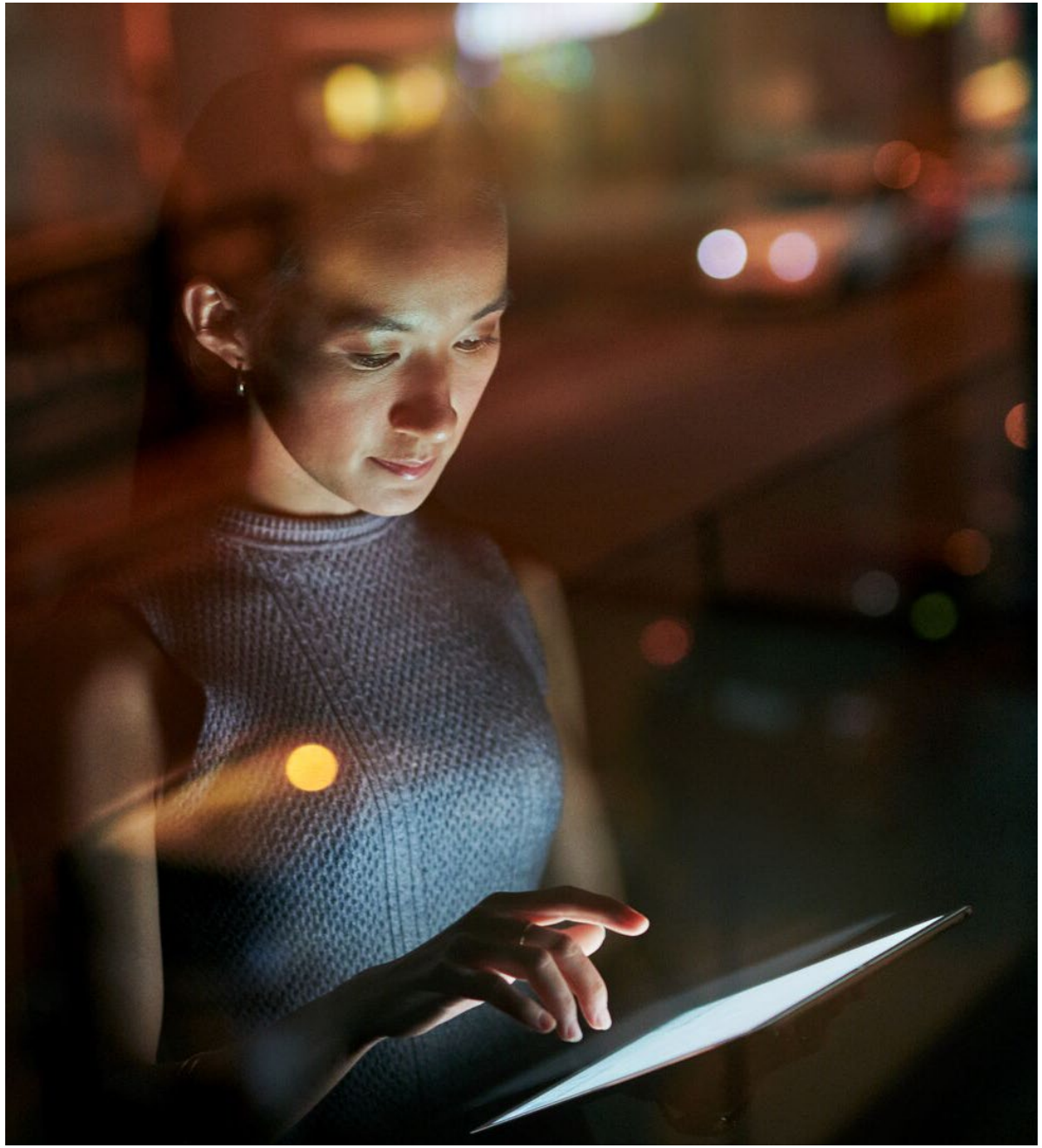
One assessment addresses best practice #2—and hands you the documentation, ownership, and evidence the other 11 depend on.

© 2026 Forvis Mazars, LLP. All rights reserved.

03

Takeaways

What to do first and what it may take to get moving.



Key Takeaways

If you do one thing after today, schedule the plan-specific risk assessment.

A Fiduciary Duty

- Cyber oversight follows from the ERISA duties of prudence and loyalty, whatever the size of the plan
- Outsourcing the service does not outsource the responsibility — or the need to document it

The Bar Has Moved

- The guidance applies to every ERISA-covered plan, including health and welfare
- EBSA confirmed that fiscal 2026 investigations will prioritize cybersecurity

Start With the Assessment

- It satisfies best practice #2 and forces documentation of the inventory, owners, and policies the other 11 rely on
- Your next step: scope a plan-specific risk assessment and put it on the committee calendar

© 2026 Forvis Mazars, LLP. All rights reserved.



EBP & Cybersecurity

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.

Contact >> Reach out with questions, to learn more, or to schedule a meeting.

Forvis Mazars

Ben Sady
Principal, IT Risk & Compliance
P: 804.474.1267
ben.sady@us.forvismazars.com

Nancy Ozuna
Partner, Professional Services Group – EBP Leader
P: 210.268.1921
nancy.ozuna@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.