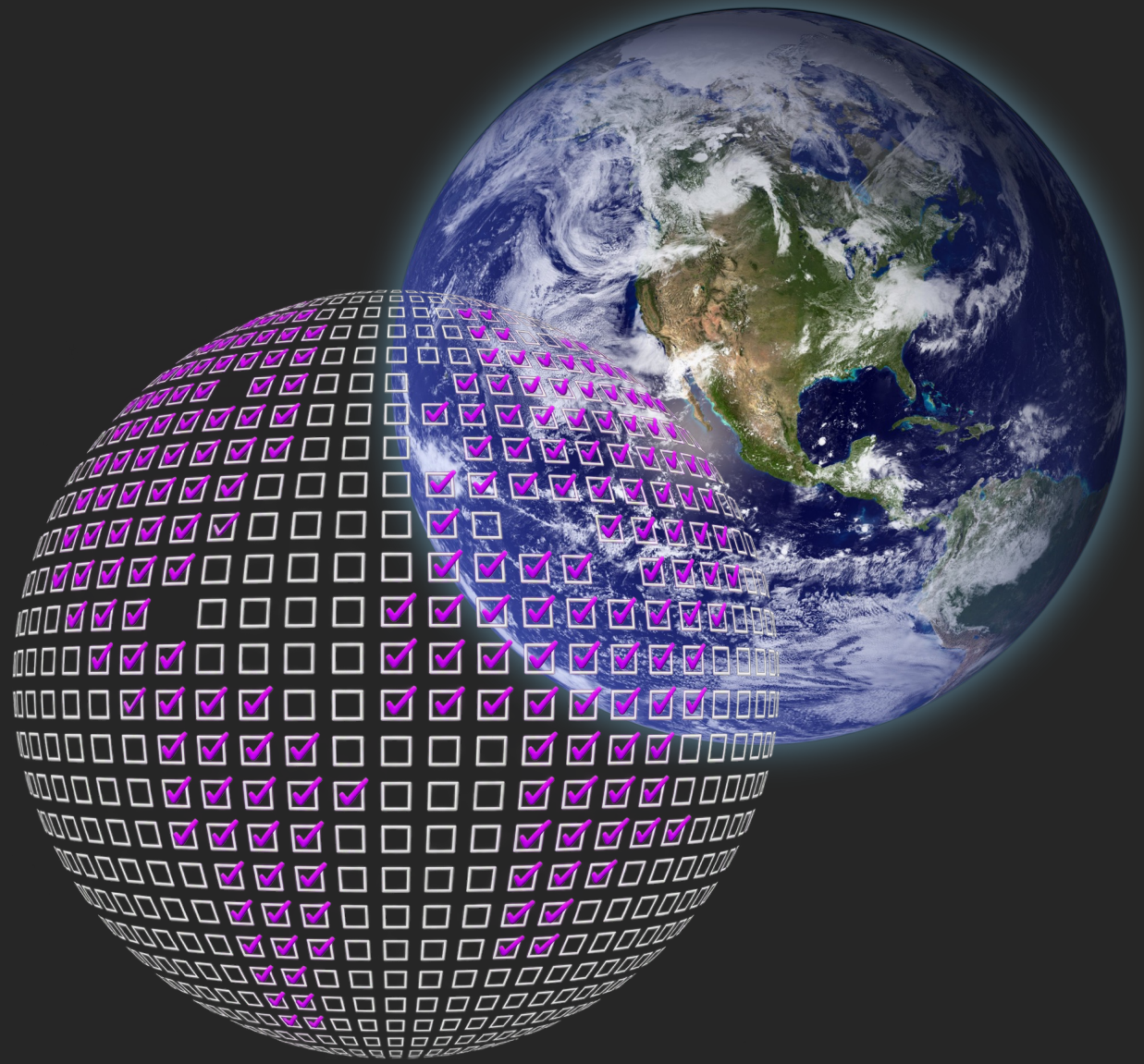
NetApp

BEYOND THE CHECKBOX

How certification can strengthen security and create market advantage



Lisa Rogers
Sr. Technical Program Manager
13 October 2026

© 2026 NetApp, Inc. All rights reserved.

How closely do you work with product certifications?

Raise your hand for the one option that best describes you.



Directly involved



Support certification work



Familiar, but not involved



New to the topic

© 2026 NetApp, Inc. All rights reserved.



“Blue Ridge Mountains Panorama,” Cowee Mountain Overlook — © Joshua T. Moore (jtm71), via Shutterbug

The assumption gap

What we know

What the evidence establishes and within what limits.

What we assume to be true

The beliefs and assumptions we rely on when deciding what to do.

Which assumptions are shaping our decisions?

“As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves.”

Ross Anderson, Security Engineering, 2nd edition, Chapter 1, §1.1

© 2026 NetApp, Inc. All rights reserved.

APRIL 2014

Anyone remember what happened?

© 2020 NetApp, Inc. All rights reserved.

Heartbleed

A missing bounds check in the TLS heartbeat implementation exposed process memory.

APRIL 2014



FIPS validation covers a defined cryptographic module, not the whole application.

© 2026 NetApp, Inc. All rights reserved.

What are we assuming after validation?

We may assume…	We need to check…
Patches will be applied promptly.	Who owns patch deployment, and how will we confirm it?
Private keys will stay protected.	What evidence shows keys remain protected in deployment?
The environment will stay the same.	Which changes require us to reassess?

Which assumption will you check next?

© 2026 NetApp, Inc. All rights reserved.

DISCIPLINED CERTIFICATIONS

An ongoing practice of using certification requirements and evidence to improve security throughout the product lifecycle.

Certification is a milestone. Security discipline is ongoing.

© 2026 NetApp, Inc. All rights reserved.

DISCIPLINED CERTIFICATIONS

Four questions to make disciplined certification practical

GOALS

What are we protecting, and do our controls work in practice?

Identify assets and threats beyond the certification boundary. Check that controls work as intended.

MINDSET

How could the system fail?

Examine dependencies, interfaces, and operating conditions.

INCENTIVES

Who does the work, who benefits, and who bears the consequences?

Examine how ownership, funding, and accountability shape security decisions.

EXPECTATIONS

What could change our assumptions?

Monitor shifts in attacker focus, product changes, and operating conditions.

Use each defect or vulnerability to test assumptions about the whole system.

© 2026 NetApp, Inc. All rights reserved.

DISCIPLINED CERTIFICATIONS

Applying the four questions across the system

RISK

Code quality is not enough.

Changing code doesn't always fix the risk.

RESPONSIBILITY

Security depends on shared ownership.

Release, operations, procurement – the entire ecosystem.

COMPATIBILITY

Compatibility decisions affect security.

Downgrades and legacy paths are attack surface.

CONTEXT

Security must be judged in context.

Same code, different environment, different outcome.

Closing the gap takes attention to the whole system and shared ownership.

© 2026 NetApp, Inc. All rights reserved.

If certifications don’t eliminate all security risk, why do them?

The value depends on customer requirements and how the certification is used.

MARKET ACCESS	**Required for some federal, defense, and regulated markets.**
FASTER REVIEWS	**Creates evidence for review without starting from scratch.**
CUSTOMER CONFIDENCE	**Provides independent assurance within the evaluated scope.**
REVENUE	**15 to 40% of revenue.** (*Based on my observations across certification programs I led at NetApp, Cisco, and ScienceLogic.)*
COMPETITIVE ADVANTAGE	**Can differentiate a product when alternatives lack required certifications.**

Certification creates business value when it meets a customer requirement.

© 2026 NetApp, Inc. All rights reserved.


NetApp
The most secure storage on the planet

How can you add rigor and still be agile?

Build certification work into the existing development and release cadences.

Planning	Identify certification needs before design begins.
At design review	Identify applicable requirements and evidence owners.
During development	Capture evidence alongside implementation and testing.
Before release	Review changes for certification impact and plan any required reassessment.

Start with one recurring checkpoint in your existing release process.

© 2026 NetApp, Inc. All rights reserved.

Where should you focus first?

Choose the improvement that addresses your program's biggest constraint.

GOVERNANCE

Map overlapping requirements across certification schemes.

Prioritize when you need several certifications for your target markets.

PEOPLE

Engage your lab early and learn from the community.

Prioritize when expertise or team capacity is limited.

PROCESS

Align certification work with each product's release cycle.

Prioritize when product changes repeatedly disrupt assessments.

TOOLS

Automate repeatable evidence and testing tasks.

Prioritize when manual work consumes engineering time.

Start with the bottleneck that causes the most rework or delay.

NetApp

© 2026 NetApp, Inc. All rights reserved.

How is NetApp improving certification work

We are integrating certification into everyday work, one improvement at a time.

GOVERNANCE

Threat-model new cryptographic features before coding.

100% of new crypto features are threat-modeled at design review, before code is written.

PEOPLE

Notify cross-functional teams when PSIRT flags a vulnerability.

PSIRT alerts trigger JIRA notifications to the cross-functional team.

PROCESS

Plan the transition to post-quantum cryptography.

Planning covers algorithm choices, platform dependencies, and implementation scope.

TOOLS

Automate algorithm and entropy workflows.

Reduce manual effort in repeatable testing and evidence collection.

Certification requirements now inform design decisions and ongoing security work.

© 2026 NetApp, Inc. All rights reserved.

How can you leverage certifications across markets?

Plan for each market's requirements and check what evidence you can reuse.

UNITED STATES

FIPS 140-3, Common Criteria (CC), and Commercial Solutions for Classified (CSfC).

EUROPEAN UNION (EU)

EUCC: Common Criteria-based certification.

CRA: Mandatory product cybersecurity requirements.

OTHER MARKETS

Check national requirements in each target market.

RECOGNITION LIMITS

Recognition depends on the scheme, scope, and target market.

Map requirements by market, reuse evidence where accepted, and plan for the gaps.

© 2026 NetApp, Inc. All rights reserved.

How many pages do you have to read alone?

Find the guidance and the people who can help.

Communities and events

FIPS 140-3
FIPS and Chips, ICMC, CMUF

Common Criteria
ICCC, CCUF

CSfC
DIB Cybersecurity

DoDIN APL
TechNet Cyber

Official guidance

EU CRA (regulation)
Commission guidance

EU EUCC (certification)
ENISA guidance

India (certification)
STQC's IC3S

Find one person who can help with your certification question.

© 2026 NetApp, Inc. All rights reserved.

Select a resource name to open its website.

What should we automate, and who stays accountable?

Use automation for repeatable tasks and AI to support analysis. Keep people responsible for decisions.



AUTOMATION

Run repeatable tasks

Execute tests, collect evidence, and draft documentation.



AI

Support analysis

Suggest coverage gaps and possible root causes for human review.



PEOPLE

Own decisions and claims

Review evidence, challenge assumptions, and approve claims within the evaluated scope.

Automate the work. Never automate the accountability.

© 2026 NetApp, Inc. All rights reserved.

Could OpenSSL pursue a shared certification beyond FIPS 140?

We are exploring the feasibility of another certification path and seeking contributors.

FOUNDATION

OpenSSL 3.x provides the provider architecture.

PRECEDENT

FIPS 140 validation offers a model for a shared module within its validated scope.

FEASIBILITY

Explore a German certification path with BSI and a lab (Lightship Security).

NEXT STEP

Form a scoping group to assess requirements, effort, and funding.

Interested in sponsoring, contributing, or advising? Find me after the talk.

© 2026 NetApp, Inc. All rights reserved.

Next steps

Beyond the Checkbox

1. Test one assumption that shapes your security decisions.
2. Build one ongoing security check into how your team works.
3. Help scope the proposed BSI certification effort.

© 2026 NetApp, Inc. All rights reserved.

Certification is a milestone.
Security discipline is ongoing.

© 2026 NetApp, Inc. All rights reserved.

Did you get at least one idea?

You'll leave with practical ideas to make your certification program *(or other area)* more efficient, strategic, and valuable to the business.

© 2026 NetApp, Inc. All rights reserved.

THANK YOU

Lisa Rogers



NetApp

© 2026 NetApp, Inc. All rights reserved.