

Q1

Does your enterprise place a priority on hardware and firmware lifecycle management?

Q1 MULTIPLIER Rate the level of importance the enterprise assigns to its approach: **HIGH:** 5 **MODERATE:** 4 **LOW:** 3 **NO:** 2

For the questions below, circle the number that best describes your enterprise:

YES: 3 **PLANNING TO IMPLEMENT** (in next 12-24 months): 2 **NO:** 1

- > Does your enterprise have an established firmware update policy?
3 2 1
- > Does your enterprise have formal patch management processes for firmware?
3 2 1
- > Does your enterprise consider the accessibility of device hardware interfaces or consoles (e.g., interfaces that are enabled/disabled or password protected)?
3 2 1
- > Does your enterprise consider information about device bootloader protections?
3 2 1
- > Does your enterprise ask device-manufacturers/partners for an auditable firmware update process?
3 2 1
- > When reviewing manufacturers (servers, network, storage, IoT), does your enterprise consider the ability to independently validate device integrity?
3 2 1

Q1 Score

_____ X _____ = _____
TOTAL FOR 6 QUESTIONS Q1 MULTIPLIER ANSWER

Q2

Does your enterprise's audit team provide feedback from regular compliance audits regarding firmware?

Q2 MULTIPLIER Rate the level of importance placed on audit team interaction and feedback: **HIGH:** 5 **MODERATE:** 4 **LOW:** 3 **NO:** 2

For the questions below, circle the number that best describes your enterprise:

YES: 3 **PLANNING TO IMPLEMENT** (in next 12-24 months): 2 **NO:** 1

- > Does your enterprise implement internal controls for firmware?
3 2 1
- > Has audit team feedback improved security outcomes for your enterprise?
3 1
- > Has your enterprise suffered a firmware-based malware attack in the last 12 months?
3 1
- > Has your enterprise suffered from exploitation of a firmware vulnerability in the last 12 months?
3 1

Q2 Score

_____ X _____ = _____
TOTAL FOR 4 QUESTIONS Q2 MULTIPLIER ANSWER

Q3

Does your enterprise employ governance frameworks or standards?

Q3 MULTIPLIER Rate the level of effectiveness for these programs in managing firmware governance: **HIGH:** 5 **MODERATE:** 4 **LOW:** 3 **NO:** 2

For the questions below, circle the number that best describes your enterprise:

YES: 3 **PLANNING TO IMPLEMENT** (in next 12-24 months): 2 **NO:** 1

> Does your enterprise segregate devices into trust zones that separate the operation of trusted devices from untrusted/untrustable devices?

3 2 1

> Does your enterprise monitor for changes in third-party firmware?

3 2 1

> Does your enterprise continuously monitor integrity of devices via the network through third-party systems and technologies (like TPM)?

3 2 1

> Do you feel your enterprise is prepared to handle a firmware attack?

3 2 1

Q3 Score

$$\text{TOTAL FOR 4 QUESTIONS} \times \text{Q3 MULTIPLIER ANSWER} = \text{_____}$$

Total Score

$$\text{_____} + \text{_____} + \text{_____} = \text{_____}$$

Q1 SCORE Q2 SCORE Q3 SCORE GRAND TOTAL

How resilient is your enterprise?

160+
HIGHLY RESILIENT

130-160
RESILIENT

100-130
INCREASED RISK

> 100
ENTERPRISE AT RISK:
REVIEW CONTROLS

NOTE: This assessment and your score are not guaranteed to indicate firmware security readiness in your organization. The assessment and results are for informational purposes and are not intended as professional guidance.

For more information on firmware security, how it affects your enterprise, and actions you can take, go to cybersecurity.isaca.org/firmware.