Entity Profile Questionnaire (EPQ) Frequently Asked Questions
Risk and Internal Controls

This document was updated on January 25, 2021.

RF has received the following EPQ-related questions regarding risk and internal controls. If you need clarification on a topic not addressed in this document, please contact us at entityprofile@rfirst.org.

Please note, we appreciate that it may be a difficult task to complete your EPQ by the Feb. 19, 2021 timeframe. If you feel your organization will not be able to meet the deadline, please email the aforementioned address and provide us with an estimated date of completion.

How does participating in the EPQ benefit Entities?

Going forward, Entities can expect conversations about internal controls to occur consistently because they relate to every aspect of maintaining a reliable, resilient secure grid. If an Entity is scheduled for an oversight engagement this year, then the controls conversation and review will be part of the assessment. The benefit of participating outside of the oversight schedule is receiving feedback on your controls, which provides the opportunity to consult with RF about your controls and provide improved mitigation of your risk.

How would an Entity in the beginning stages of their program answer more mature program questions?

We appreciate that some of the questions may be applicable to a more mature program, but that was by design. For those questions that address a program area you have not designed yet, it is acceptable to leave it blank. That said, it can be extremely beneficial to use those questions to help mature your process. These questions mirror some of the information you will be asked about during any oversight conversations, so we felt that including them (even though some programs are not ”quite there”) would provide some guidance and information on steps to strengthen your internal control system.

Is there any guidance on how an Entity is expected to determine their risk score as they apply to the Risk Elements? Can Entities use the document “ERO Enterprise Guide for Compliance Monitoring - Appx B ERO Risk Factors”?

This open-ended question was designed to allow those Entities that have already performed a risk assessment of their organization to utilize their Entity-specific risk assessment. That said, **Appx B ERO Risk Factors** would be an excellent tool to assist in performing your risk determination.

When using the “ERO Enterprise Guide for Compliance Monitoring - Appx B ERO Risk Factors” document, if a standard is applicable to your risk and internal controls submission but is not identified as a current risk in the 2021 NERC CMEP, would the response be a low rating?

If an Entity determines that their risk to the reliability and resilience of the Bulk Power System (BPS) lies outside the ERO Risk Elements (i.e., an area not identified within the 2021 NERC

CMEP), then we would expect the Entity to focus their resources on those areas. In other words, if a standard is not included in the 2021 NERC CMEP, the Entity would still respond with a rating commensurate with their risk.

Are Entities required to submit controls, their associated monitoring processes and previous two monitoring process results, even if they responded "No" to submitting their controls for review? (This question is based on the last request in the EPQ template.)

No, Entities are not required to provide any control documentation for controls they do not want considered for scoping. However, we will be asking about your control documentation during oversight engagements.

Are Entities required to submit all controls, their associated monitoring processes and previous two monitoring process results if they responded "Yes" to submitting their controls for review?

No, you simply need to supply those that you would like reviewed in order to be considered during scoping. Please remember, in order for scoping to be affected, the documentation would need to evidence the risk raised by the standard/requirement has been appropriately mitigated, monitored and represented by the controls submitted.

Are Entities required to respond to every question following the "Applicable Standards and Requirements" selection box if they are not submitting the controls for scoping consideration?

We are requiring the risk determination for each Risk Element. If the Entity's risk determination for that Risk Element is greater than zero, we would like to receive that information, even if the control is not being submitted for scoping consideration. However, if that information is not supplied at this time, these questions will come up during any oversight engagement.

Please describe RF's need for and intended use of the internal controls and monitoring information potentially provided.

The goal for receiving this data outside an engagement is to benefit both the Entity and RF by providing an opportunity for review and feedback. By reviewing the design of the controls, RF is able to determine where Entities may be struggling with a specific area or consistently missing a needed control. This allows us to address the topic through outreach activities, such as a workshop, monthly Technical Talk with RF call, newsletter article, etc., which benefits our entire industry. Additionally, the Entity benefits from getting their controls reviewed outside of an oversight engagement, allowing them the opportunity to make corrections prior to the timing of any engagement activity.

The EPQ requests that Entities submit their documented internal control and evidence of the last two monitoring processes. What constitutes a monitoring process?

Any time someone performs a systematic quality review of something like a process, procedure or protocol over a period of time, it can be considered a monitoring process. Documentation of the monitoring process should be maintained, but it does not have to be extensive.

When does the initial notification period start for internal controls to be considered for scoping?

Per the RF Engagement Timeline (available here on the RF website) the Inherent Risk Assessment (IRA) notification is sent out 115 days prior to the beginning (i.e., onsite date) of the audit.

Is this EPQ request a replacement of the Internal Controls Evaluation (ICE) program?

Internal controls are the foundation of sustainability in a risk-based environment. Compliance is the result of an appropriately designed and implemented program. The ICE program was designed as a standalone process used in conjunction with a compliance audit. This EPQ process is designed to address risks and their mitigating controls.

What is the intent of the Risk and Internal Control Evaluation process and how will the information provided be used?

The information will be used in the IRA process during the creation of the Compliance Oversight Plan (COP). This process reviews eight Performance Considerations during the creation of the COP, and this would be one of those considerations. Additionally, the audit team will be reviewing the internal controls to assist in the determination of scope.

When compiling the risk rankings, what is the viewpoint of the impact to the BPS? Is this the inherent or mitigated risk?

The Risk determination response would be the unmitigated risk. The internal controls provided in the lower section of the template would evidence how the risk is mitigated.

Who should I contact if I have questions?

Please email entityprofile@rfirst.org with any additional questions.