NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Sampling Handbook

Revision 1.0

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Chapter 1 – Introduction

This document provides guidance when using sampling as a tool for compliance monitoring of registered entities (Entities). Regional Entity (Region) staff is responsible for identifying the sampling approach appropriate for the compliance monitoring method. This document is divided into the following sections: Overview, Sampling Approaches, Sampling Table A, and Sampling Glossary, with Appendices A, B, and C. These sections comprise the ERO *Sampling Handbook* (Sampling Handbook).

Background

The Compliance Monitoring and Oversight Process Working Group (CMPWG) developed a sampling methodology included in the *NERC Sampling Methodology Guidelines & Criteria*. During the creation of the ERO Enterprise Compliance Auditor Handbook in 2013, a need to update the *NERC Sampling Methodology Guidelines & Criteria* was identified. Similarly, the Key Reliability Standards Spot-Check (KRSSC); PRC-005-1 Key Reliability Standard Spot-Check, September 14, 2011 noted a need to update the *NERC Sampling Methodology Guidelines & Criteria*. With the approval of the ERO Compliance and Enforcement Group (ECEMG) and NERC, the ECEMG assigned the Manual Task Force (MTF) to create an updated Sampling Handbook that can be used by all Compliance Enforcement Authority (CEA). The MTF worked with the Compliance Monitoring Functional Group (CMFG) to create a Sampling Handbook and incorporate the new risk-based compliance monitoring and enforcement Program (CMEP) principles. The Sampling Handbook is the culmination of work and input from all eight Regions and various working groups.

Sampling Handbook

Chapter 2-Overview provides information about general sampling concepts and techniques. It also discusses documentation of the sampling process and the workpapers associated with the sampling process.

Chapter 3-Sampling Approaches offers two categories of sampling approaches: Statistical and Non-statistical. This is to generate consistent and confident sampling.

Chapter 4-Sample Table A and Appendix A-Sample Table A further establish a minimum set of guidelines for use with various compliance monitoring activities. These sampling approaches are also recognized by Generally Accepted Government Auditing Standards (GAGAS) and the Institute of Internal Auditors (IIA).

Additionally, Chapter 5-Sampling Glossary and the illustrative examples in Appendix B offer further guidance on different approaches to performing both Statistical and Non-statistical Sampling. Refer to the glossary in Chapter 5 for additional information on any of the technical or capitalized terms referenced in this document. Finally, Appendix C provides the Lead Sheet Template.

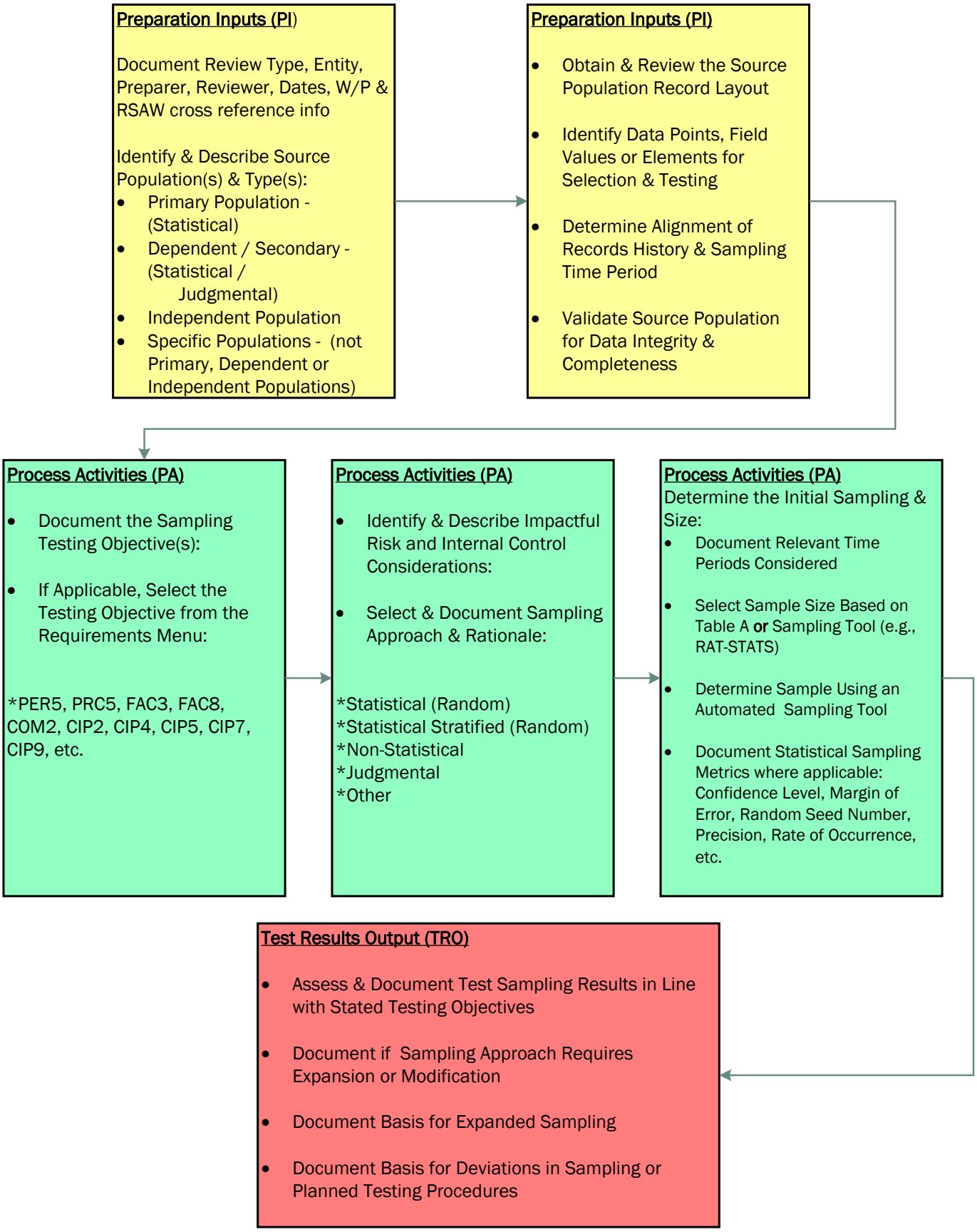
Chapter 2 – Overview

This chapter provides information about the use of general sampling approaches to sample evidence when performing various compliance monitoring activities. Sampling is essential for auditing and compliance monitoring because it is not always possible or practical to test 100% of either the equipment elements or documentation artifacts.

In the audit context, there are generally two primary approaches to sampling: Statistical and Non-statistical. Auditors may use a combination of the Statistical and Non-statistical approaches as well as other approaches to sampling. Regardless of the sampling approach, the CEA should determine the approach based on testing objectives. If the objective is to ensure a higher level of confidence concerning compliance that can be extrapolated to the whole population, for instance, the CEA should use Statistical Sampling. The CEA should appropriately document the chosen sampling approach, testing objective(s), supporting details, confidence level, and associated testing conclusions in the workpapers. Where Statistical Sampling is not practical, the CEA should establish criteria basis and context and document the justification of the value(s) and testing results of the Non-statistical sample selected.

Compliance Management or the Team Lead may determine, through the use of an Inherent Risk Assessment (IRA) and/or Internal Controls Evaluation (ICE) review, that the number of samples can be reduced for the engagement. If the number of items sampled is below those established in the Sampling Handbook, the CEA shall document in the workpapers the rationale for reducing the size of the sample population.

Overview of Sampling Process



Risk-based Approach

The risk-based approach includes the IRA performed by the Regions. This may also include an Internal Controls Evaluation (ICE) by the Regions. These activities (IRA, ICE, self-audit, self-spot check, data sampling, procedure updates, etc.) help the CEA determine the compliance monitoring process used. This enables the CEA to determine the risk-based scope to use in assessing whether the Entity meets the NERC and Regional Standards. The various risk, control, and compliance activities will support the idea of scoping or reducing the sampling to verify compliance. This will be determined by the CEA teams that review the activities performed by the Entity and Entity's risk to the Bulk Electric System (BES).

Additionally, Entity -performed sampling (as determined during an Entity's self-evaluation) may affect the sampling approach chosen. Before relying on the work of others, verify the sampling is unbiased, independent, complete, statistically-based, and well-documented. This can also be used if the CEA team reviews the Entity's samples and determines to expand the sample set. The CEA would then increase the sample set to the number in this document or greater depending on the testing, scope, and objectives of the tests. The determined sampling approach and rationale shall be documented in the workpapers.

Multi-Regional Registered Entities (MRRE)

Multi-Regional Registered Entities (MRRE) are Entities registered for functions in multiple Regions. Under the MRRE there will be at least one lead Region with the other Regions possibly participating or relying on the lead Region to perform the compliance monitoring for all the Regions involved. The MRRE process will require considerable coordination among the Regions as the IRA for the Entity may vary in each of the respective Regions depending on the identified risks, assets, locations, etc. All of the Regions involved should agree on the final scope of a compliance monitoring activity so that risks identified in each of the Regions can be addressed during the activity. Some sampling considerations that need to be decided to address Entity risk and BES reliability are as follows:

- Should the population include assets, devices, etc. from all Regions?
- Should the sample include more of the assets, devices, etc. from areas that pose the most risk? Note that the population should be chosen relative to the risk determined by each Region.
- Should the final sample list include (as an example) 33 samples from each Region or 33 samples across the Entity's entire population?
- Lead Region shall work with affected Regions to determine the sampling approach

The idea is to develop a sufficient sample of items to reach a level of confidence that the sample is accurate, complete, and meets the testing objectives. The sampling should not be an onerous task to show compliance. The determined sampling approach and the rationale shall be documented in the workpapers.

Requirements with Short Retention Periods

Some NERC Reliability Standards have requirements stating information shall be kept for a short retention period. These requirements usually have a 90-day retention period for very large quantities of data. For example IRO-001-1.1, CIP-005-3a, CIP-006-3c, and CIP-007-3a, among others, all have requirements with the 90-day retention period for data. For compliance monitoring, these requirements require sampling to collect and review a representative group of the total population, thus impacting data for the audit period identified in the monitoring process notification letter. Therefore these factors need to be considered when selecting samples for requirements with short retention periods.

Sampling from Multiple Versions of a Standard

There are several currently enforceable Reliability Standards that have implementation plans which overlap the different versions of the same standard. PRC-005 versions 1 and 2 are examples on the Operations and Planning list. CIP has several Reliability Standards where an Entity may cover two or more versions of the same standard. The CEA needs to ensure the testing meets the objectives for the versions in effect. The CIP version 3 to 5 transition introduces even more overlap.

These version changes can cause confusion for the CEA, as well as the Entity. When compliance monitoring needs to sample for a Requirement over a period of time where there is more than one version of the Reliability Standard in effect, the chosen sampling approach needs to reflect the objectives of the compliance monitoring activity.

Questions to consider include the following: "Are we more concerned with how the Entity supports the newer Requirement" or "How well did the Entity manage the prior versions of the standard?" These questions can lead to a different sampling approach.

The sample set should not be overly burdensome, and the CEA should have some rationale behind the number of samples requested for each version of the standard. However, CEA may choose not review data from the period when the older version of the standard was active because associated Requirements are covered in the newer version of the Requirement, or vice versa. Alternatively, the testing may include multiple samples from the different versions of the Standard. No matter the sampling approach chosen, the approach needs to tie to the overarching monitoring objective, and the CEA must document the approach in the workpapers.

Data Retention

If current Reliability Standards are silent as to a data retention period, sampling of data should focus on the most recent two years, unless the data sample would be statistically too small or irregularities are identified in the initial samples. This would not apply to the following:

- Voice and audio recordings should focus on a 90-day rolling retention period.
- Standards requiring a current program or procedure should focus on the currently effective version, with a revision history specifying changes and dates of review.
- Standards requiring testing intervals (e.g., PRC-005), should focus on the most recent full testing records with evidence of previous testing intervals.
- For standards supported by evidence records that extend beyond the audit period, the most recent record should be tested. For example, PER-005-1 Requirement R2 requires validation of the most recent competence records for a system operator, even if the date of the record is outside the audit period.

The data retention section is based on the *NERC Final Data Retention Whitepaper*, September 12, 2014, posted on the NERC Website.

Documentation in Workpapers

In general, compliance monitoring workpapers should reflect the statistical or non-statistical testing approach used and sampling results achieved when performing specific compliance monitoring testing. The workpapers should capture the testing approach in sufficient detail so a reviewer can understand the testing approach used.

The testing or sampling process typically starts with profiling and documenting the type of sampling source population(s) and defining the compliance or other testing objective(s). CEA also determine the sampling approach (i.e., statistical or non-statistical), statistical metrics setting (e.g., Confidence Level, Margin of Error, Precision, etc.), sizing of the sample(s), or choosing an alternative sampling method when applicable.

The CEA should document its results of the test sample output and its determinations. The CEA must also substantiate its rationale for any deviations from either the Sampling Handbook guidelines or planned testing procedures within the workpapers. Additionally, the CEA should clearly annotate and provide references for the sample testing outputs or results to aid in analysis and compliance monitoring. Sample output testing records and results should also be retained and secured in a fashion similar to other workpapers, including supporting evidence and fieldwork evaluations.

The overall workpaper documentation should be of sufficient quality and substance to support management's or an independent third parties review.

The Sampling Handbook also references a Sampling Lead Sheet, included as Appendix C, which can be used by the CEA when performing various compliance tests where sampling is used. The Sampling Lead Sheet can be used to capture and catalog the various sampling activities encountered in any given compliance monitoring or other sampling testing. Refer to the Sampling Lead Sheet to reference and catalog sequencing of the various sampling activities.

Chapter 3 – Sampling Approaches

Considerations for Professional Judgment When Sampling

Professional judgment has to be exercised throughout the compliance monitoring processes. There are times where the sample population may require a mix of sampling techniques to create the final sample population. This may occur due to the type of data available, timing, logistics, etc., that affect the compliance monitoring process. The team should be able to justify why a particular method is used during an engagement. The reasoning and variations shall be documented in the workpapers. The Sampling Handbook does not dictate how a population is sampled but provides guidance on common practices used by the ERO to perform sampling. The CEA always has the flexibility to sample a population as it sees fit to meet the objectives.

Statistical Sampling

Statistical Sampling is employed when testing the entire population is impractical but one wants to extrapolate the results of the test over the entire population. Statistical Sampling provides assurance that the attributes of the selected sample represent the entire population. Using RAT-STATS or other Statistical Sampling tools together with the Sampling Handbook further supports this approach to compliance monitoring testing. The CEA may also use information gathered during the engagement to increase or lessen the sample size for Statistical Sampling. This information may come from the IRA, ICE, or other documentation already reviewed to justify modifying the sample size. When the sample size is reduced, the confidence level is also reduced for that population. If the sample size is increased, the confidence level is also increased for that population.

The Sampling Handbook and its predecessor, the *NERC Sampling Methodology Guidelines and Criteria*, are based on the use of a 95% confidence level, which is represented in Sample Table A. Should a different confidence level be employed, the CEA will have to use a Statistical tool (such as RAT-STATS) to determine the sample size. The ideology behind the 95% confidence level is to sample a representative portion of the total population with a low margin of error (MOE).

It is recommended that CEA opt for the 95% confidence level as opposed to selecting a higher confidence level (e.g., 98% or 99%). This is because as the confidence level increases, the number of standard errors also increases along with the MOE. If you wish to be more than 95% confident about your results, you will need to add and subtract more than two standard errors. For example, 99% confidence requires the addition and subtraction of 2.58 standard errors (i.e., critical value or z*-value) to derive the MOE. Therefore, the higher the confidence level, the larger the z*-value, the larger the MOE, and the wider the confidence interval. Hence, there is an added price for seeking the additional confidence. It should be noted the wider confidence interval and increased margin of error can both be offset and reduced, respectively, by increasing the sample size. Refer to the glossary in Chapter 5 for additional information on any of the technical terms referenced in this section.

The CEA needs to document the use of Sample Table A or the use of a different confidence level or sample size and note the other materials used to justify this decision in the workpapers.

Considerations for Statistical Sampling (Single Random)

It should be noted that in a simple random sample of a given size, all subsets of the population frame are given an equal probability. Any given element from a set of selected elements (pairs, triples, and so on) has the same chance of selection as any other. This minimizes bias and simplifies analysis of results. Statistical Sampling (Simple Random) may be vulnerable to sampling error when the randomness of the selection sample does not reflect the population composition. In this case, the CEA may wish to consider using the stratified or systematic sampling techniques, which use information about the population to choose a more representative sample.

Considerations for Statistical Sampling (Stratified)

Where source populations can be differentiated by unique categories, the population frame can be organized by these categories into homogenous "strata." Each stratum can be sampled as an independent sub-population from which individual elements can also be randomly selected. This approach typically allows for greater specificity of the sampled results. Additionally, because each stratum is treated as an independent population, different sampling approaches can be applied to different strata.

As an example, if there are ten substations in the total population, with three at 345kV and seven at 230kV, then this would be a population with two different strata.

An example of homogenous strata would be the five different Protection System Device types. Sampling all the relays and the integrated components associated with the relay (CT/PT, DC circuitry, communications, and DC sources) would create a homogenous set of data. This type of sampling can be accomplished in two ways: first you could sample the five separate component populations, or second you can sample the relays and request all associated components for each relay selected.

Considerations for Statistical Sampling (Systematic)

Systematic sampling relies on arranging the study population according to an ordering scheme and then selecting elements at regular intervals through the ordered list. Systematic sampling requires a random start and then proceeds with the selection of every kth element [(k=population size / sample size] from then onwards. The starting point is chosen randomly from within the 1st to the kth element in the list. For example, sampling every 5th item is also known as an every 5th sample or as a "sampling skip of 5." This approach can be especially efficient for sampling from databases. With a randomized starting point, this approach represents a type of probability sampling. The practitioner should also be aware that the Statistical Sampling (Systematic) approach can be vulnerable to periodicities in the list. If list periodicity is present and the period is a multiple or factor of the systematic interval used, then the sample is likely to be unrepresentative of the overall population.

Non-statistical Sampling

There may be cases where Statistical Sampling is inappropriate for obtaining the desired or stated testing objective. For example, consideration of Events Analysis or an IRA further requires the evaluation of a particular subset of the population. In this case, a Non-statistical approach (Judgmental, etc.) is used to augment the initial Statistical sample.

Considerations for Judgmental Sampling

Some situations and populations do not fit the statistical models. This demonstrates the need for the CEA to add items to the selected sample list for compliance monitoring activities. Therefore, the population of samples may need to be selected using a Judgmental Sampling process. The Judgmental Sampling process is a useful alternative to Statistical Sampling. This may be due to items being at more risk to the BES or there is a history of issues with the items selected. The workpapers shall document the reasoning for the selected items, the actual items selected, and the determinations.

Considerations for Attribute-based Sampling

Attribute-based sampling is an alternative approach centered on the concept of control frequency. As an example, this methodology rationalizes that if an attribute executes on a daily basis, then it occurs about 30 times a month. As a result, the CEA selects a sample of 30. If the attribute is an automated one, such as a password configuration, then a sample of one may be obtained. Additionally, if the population is under 10, the CEA would test the entire population. If the audit population is under 30, the CEA would test one for each 24-hour day. Additionally, it should be noted that attributes that are regularly exercised (e.g., daily) result in a high confidence rating.

Chapter 4 – Sample Table A

The Sample Table in Appendix A is designed to provide the CEA more guidance after the sampling approach (Statistical and Non-statistical) is determined. The table includes three sections, each with a range of numerical spreads that support a confidence factor of 95% with a +/- 10% MOE. The sample selection value is based upon the minimum value of the population size.

When the population sample to be reviewed consists of documentation records, a Statistical approach using RAT-STATS or other Statistical tools is expected. The Statistical Sampling process is divided into two applications:

- The first application is where the population needs to be reduced in steps consisting of a Primary and Dependent sampling group to select the final sample set. A Statistical sample is selected from the Primary population to create a Dependent population for sampling. From the Dependent population, the final sample set is selected. The selection of Dependent samples may be repeated to refine the population until a final sample set is selected.
- The second application is where the population is independent and can be statistically sampled from the original population. The population size determines the number of samples selected.

Non-statistical Sampling is addressed in Chapter 3. Non-statistical Sampling is performed when the population to be reviewed is physical, restricted by travel and time constraints, or other instances where a Judgmental sampling process would better address the sampling of the population and meet the objectives. From the selected sample set, the CEA can then use Statistical Sampling to select the final items to review. As an example, Non-statistical Sampling is used to select substations to visit. Then from the list of substations, a Statistical Sampling method is used to select the items reviewed at the selected substations.

Use of the Sampling Table

Use the first column to identify the description of the population to be sampled. There are three types of populations listed in the table:

1. Statistical Primary and Dependent Populations: used when a large population (substations, ESPs) includes even larger subpopulations (relays, CCAs)
2. Statistical Independent Populations: used when elements are not interdependent with other elements that need to be sampled
3. Non-statistical

Statistical Primary and Dependent Populations

For large populations, identify the Primary population size listed in the first column (example: substations, etc.). Once the population is identified, use the second column to determine the sample size to sample from the Primary population. Next use the Primary samples to request the list of items that are relevant to the Primary samples. From the materials received, the Dependent Population has been identified. From the Dependent population, use the first column to select the size of the population and the second column to determine the number of samples to request. This creates a list of sample items identified that will be included in the final data request for that requirement.

1. **First**: Identify primary population (substations, etc.)
    a. If the total number of the primary population of substations owned by the Entity is 1-8, sample the entire population.
    b. If the total number of the primary population of substations owned by the Entity is greater than or equal to 9, sample 8 of the substations.

2. **Second**: Identify the total number of secondary-dependent population elements (relays) from the primary population (substations, etc.)

    a. If the total number of the dependent population of relays owned by the Entity is 1-9, sample all elements.

    b. If the total number of the dependent population of relays owned by the Entity is 10-19, sample 9 elements.

Statistical Independent Populations

Identify the Primary population size listed in the first column. Once the population is identified, use the second column to determine the sample size to sample from the population. This creates a list of sample items identified that will be included in the final data request for that requirement.

Non-statistical Populations

Identify the Primary population size that meets the documented criteria for the compliance monitoring (example, substations within a 60-mile radius). Once the population is identified, use the second column to determine the sample size to sample from the Primary population. Note there may be reasons not to sample four items. The CEA will document the criteria and reasoning for its selection of samples. Once the Primary population has been identified, the team will request the list of items that are relevant to the Primary samples. It is preferred that Statistical Sampling is used at this point to refine the final sample list. But there are times where Judgmental sampling would better meet the objectives. The CEA will document the process used and the outcome of the sampling review.

Examples of the sampling process are provided in Appendix B, Sampling Process Flows.

Chapter 5 – Sampling Glossary

The terms included in this section define different methods and concepts associated with the Sampling Handbook:

- **Attribute:** A quality, property, or characteristic.
- **Compliance Monitoring and Enforcement Program (CMEP):** The program used by the North American Electric Reliability Corporation ("NERC") and the Regional Entities to monitor, assess, and enforce compliance with Reliability Standards within the United States.
- **Compliance Enforcement Authority (CEA):** NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.
- **Compliance Monitoring and Oversight Process Working Group (CMPWG):** A retired ERO working group with auditing representatives from all eight Regional Entities and NERC. The group worked to build consistency among the eight Regions. The group was migrated to the CMFG.
- **Compliance Monitoring Functional Group (CMFG):** ERO working group with representatives from all eight Regional Entities and NERC. The group works to build consistency with the compliance monitoring activities for the ERO. The group reports to the ECEMG.
- **Compliance Monitoring Sampling:** The selection and evaluation of a sample of items from a population of relevant information. The CEA expects the sample to be representative of the population and thus likely to provide a reasonable basis for conclusions about the population. In this context, representative means the sample will result in conclusions that, subject to the limitations of sampling risk, are similar to those that would be drawn if the same procedures were applied to the entire population.
- **Confidence Interval:** The single number sample statistic describing a sample (e.g., sample median) plus or minus a margin of error (MOE). The lower end of the interval is the sample statistic minus the margin of error, and the upper end is the sample statistic plus the margin of error.
- **Confidence Level:** A number that marks a level of confidence for which a sample provides a reasonable level of assurance the information reviewed is correct and accurate. The confidence level also represents the confidence interval expressed as a percentage or how confident you are the results will capture the true population parameter depending on the luck of the draw with your sample. The current ERO default is 95%. For more information, see the RAT-STATS user guide.
- **Dependent Sampling:** A sample is chosen from reducing a primary sample population so that a new subset population is created and the dependent samples are selected from it. Example: primary population is "cars", the subset is chosen as "blue cars." Once the list of blue cars is identified, then a final sample set of blue cars can be chosen from the list. This process can be repeated several times to reduce the original population down to a manageable and representative population.
- **Desired Precision Range (Precision):** The range of error, such as plus or minus (+/-) five (5) percent for a 10% precision band. As the range of allowable errors narrows, the required sample size increases. For RAT-STATS, this is the desired width of the confidence interval, with a range of 1-99%. The current ERO default is 10%. For more information, see the RAT-STATS user guide.
- **Entity:** When singularly used and capitalized in this document, refers to a Registered Entity as defined in the NERC Rules of Procedure (ROP).
- **ERO Compliance and Enforcement Management Group (ECEMG):** ERO Regional Entity management representing all eight Regions and NERC. The group is comprised of the NERC and Regional compliance operations and enforcement management formed to achieve coordination and collaboration across the

ERO Enterprise in the implementation of the CMEP to improve transparency, consistency, efficiency, cost effectiveness, quality, and timeliness of results of compliance monitoring activities.

- **Generally Accepted Government Auditing Standards (GAGAS):** Also referred to as the Yellow Book. This is the professional standards and guidance framework for conducting high quality audits with competence, integrity, objectivity, and independence. This is one of the reference documents used in ERO Compliance Monitoring.
- **Institute of Internal Auditors (IIA):** Is the authoritative guidance as the standard-setting body for the internal audit profession globally. The International Professional Practices Framework (IPPF) is one of the reference documents used in ERO Compliance Monitoring.
- **Independent Sampling:** A sample is chosen from a population that does not need to be sorted or reduced to select a representative sample set.
- **Inherent Risk Assessment (IRA):** IRA of Registered Entities is to identify areas of focus and the level of effort needed to monitor compliance with enforceable NERC Reliability Standards (Reliability Standards). The IRA is a review of potential risks posed by an individual registered entity to the reliability of the Bulk Power System (BPS). An assessment of BPS reliability impact due to inherent risk requires identification and aggregation of individual risk factors related to each registered entity, and the consideration of the significance of BPS reliability impact for identified risks. An IRA considers risk factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition when determining the compliance oversight plan for a Registered Entity.
- **Judgmental Sampling (Non-statistical):** When an auditor selects sample items based on some type of methodology in an attempt to select items that exhibit some type feature. This method purposefully biases the sample, and, thus, the results of the testing cannot be extrapolated to the larger population.
- **Manual Task Force (MTF):** ERO working group tasked with managing the ERO Compliance Auditor Manual. The group consists of four Regional Entity members and a NERC representative. They report to the ECEMG.
- **Margin of Error (MOE):** The number added to a statistic (estimate) of how much the sample results could change if you took another sample. The MOE also equates to the number of standard errors you need to get the confidence level you want. For example, 1.645 standard errors (i.e., critical value) correspond to a 90% confidence level, 1.96 to 95%, 2.33 to 98% and 2.58 standard errors to 99% confidence levels, respectively. Note: Examples based on typical Z-distribution for the critical value (z*-value) and common confidence levels.
- **Multi-Regional Registered Entities (MRRE):** Are registered entities registered for functions in multiple Regions. Under the MRRE there will be one or more lead Regions with the other affected Regions participating or relying on the lead Region to perform the compliance monitoring.
- **Non-statistical Sampling:** A sampling approach that does not include both the random selection of the sample items and the use of an appropriate statistical technique to evaluate sample results, including the measurement of sampling risk.
- **Parameter:** A single number that describes a population, such as the median of the population.
- **Population:** The entire set of data from which a sample is selected and about which the compliance monitor wishes to draw conclusions.
- **Random Sampling (Statistical):** See Statistical Sampling.
- **RAT-STATS:** A statistical audit tool used by the U.S. Department of Health and Human Services' Office of Audit Services and developed by the Regional Advanced Techniques Staff (RATS) in San Francisco. The statistical software tool assists the user in selecting random samples. The goal behind RAT-STATS was to develop valuable analytical tools that could be easily used by auditors.

- **Rate of Occurrence:** The expected rate of occurrence for the characteristic within a population. For RAT-STATS, the rate of occurrence is 0.5-98%. The current ERO default is 0.5%. For more information, see the RAT-STATS user guide.
- **Regional Entities (Regions):** The eight regions that make up the North American Electrical Grid. Southwest Power Pool (SPP RE), SERC Reliability Corporation (SERC), Texas Reliability Entity (TRE), Florida Reliability Coordinating Council (FRCC), Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), Western Electricity Coordinating Council (WECC), and Reliability First (RF).
- **Seed:** A random number selected by a user of RATS-STATS software to produce a sequence of sample results. Confidential selection of a different seed number prohibits Entities from identifying what items might be selected from a sample population.
- **Sampling:** The act, process, or technique of selecting a suitable sample; specifically, the act, process, or technique of selecting a representative part of a population for the purpose of determining parameters or characteristics of the whole population.
- **Sampling Errors & Biases: I**nduced by the sample design. Selection Bias – condition where true selection probabilities differ from those assumed in calculating the results.
- **Random Sampling Error:** Random variation in the results due to elements in the sample being selected at random.
- **Sampling Risk:** The risk the analyst reaches an incorrect conclusion because the sample is not representative of the population or from the correct time period. To correct, adjust the audit procedure (i.e., selection method / test objective / audit sample size).
- **Standard Deviation:** Measures variability (or spread) among the numbers in a data set or distance from the average or mean. It also describes where most of the data should fall (assuming a bell-shaped normal distribution); approximately 95% of the data will lie within two standard deviations of the mean.
- **Standard Error**: Measures variability in sample results in terms of a number of standard errors. Similar to standard deviation of a data set - but applies to sample "means" or sample "percentages" that you could have gotten if different samples were taken.
- **Statistic:** A single number that describes a sample, such as the median of the sample. The statistic is typically expressed as a range of possible values for the population parameter. The number that is added to and subtracted from the statistic is called the margin error (MOE) and is denoted by a (+/-).
- **Statistical Sampling:** An approach to sampling that has the following characteristics: a) Random selection of the sample items; and b) The use of an appropriate statistical approach to evaluate sample results, including measurement of the sampling risk.
- **Test/Testing:** The process or approach for evaluating evidence from a registered entity

.

Appendix A – Sample Table A

Sample Table A	
Population Description	**Sample Selection**
Statistical Sampling	
Primary Population (Examples: Substations, Generating Stations, ESPs, PSPs, CCAs)	**Using Statistical Sampling**
1-8	Entire population
9 +	8 Samples
Dependent Population of Elements: (Examples: Relays, CCAs, Routers, Firewalls & Other)	**Using Statistical Sampling**
1-9	All Elements
10-19	9 Samples
20-40	16 Samples
41-100	23 Samples
101-1000	29 Samples
1001 +	33 Samples
Independent Population of Elements: (Examples: Transmission Segments, Blackstart units, Outages, Mis-operations, Daily Operations reports, Line Ratings, others)	**Using Statistical or Judgmental Sampling**
1-9	All Elements
10-19	9 Samples
20-40	16 Samples
41-100	23 Samples
101-1000	29 Samples
1001 +	33 Samples
Non-Statistical Sampling	
Physical Visits : Due to geographic limitations and/or time constraints, the team may choose to sample less than 4 physical sites. (Examples: Control Centers, Substations, Generating Stations)	**Non-Statistical**
1-4	Entire population
5+	4 Samples

The confidence factor is 95% +/- 10% error. Confidence factor is based upon the minimum value of the population span, i.e. for a population range of 10-19; the 95%+/-10% reflects the confidence factor for a population of 10.

Appendix B – Sampling Process Flows

Contents

CIP Standards:

- CIP-007-3
- Additional future examples are being developed

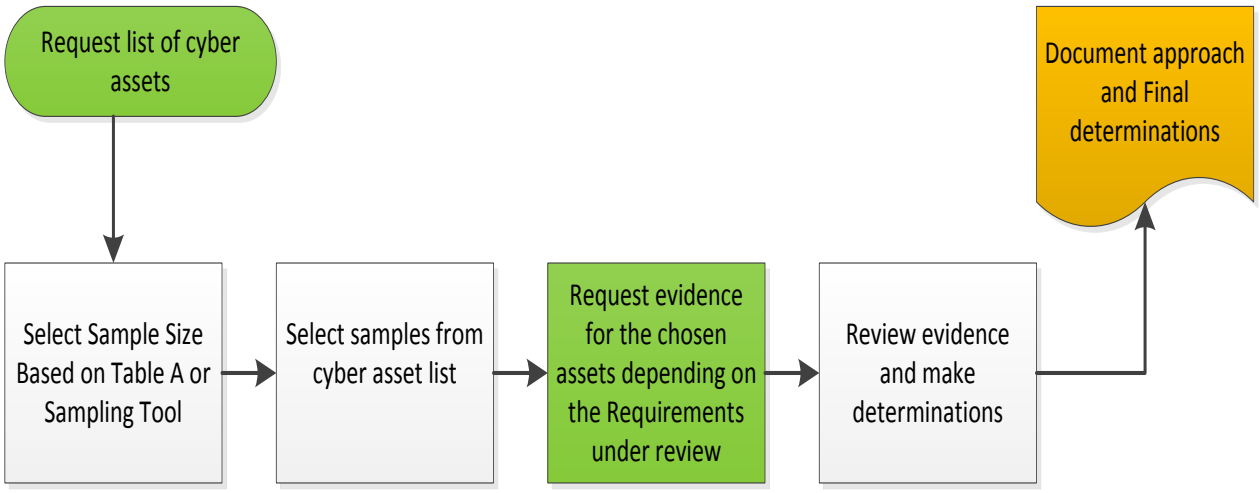
Operations and Planning Standards:

- FAC-008-3
- Additional future examples are being developed

CIP-007-3

This may be used for several Requirements

Flow Chart:



Process:

- Request the cyber assets inventory list from the Entity
- Determine the size of the sample set from the Entity approved cyber assets inventory listing by referencing Table A. Then perform the sampling process using a random number generator such as RAT-STATS.
- The resulting sample set of cyber asset inventory is then used as the basis for evidence requests relating to the various requirements of CIP-007-3. Typical examples of CIP-007-3 Entity data requests may include:
  - R1.3 - Testing records and results for each selected cyber asset;
  - R2 - Documentation records of enabled ports and services for each cyber asset;
  - R3 - Patch management records for each cyber asset or a complete inventory listing with sampled cyber assets (highlighted);
  - R4 - Evidence that supports up-to-date anti-virus and anti-malware signatures or an approved TFE request for each selected cyber asset;
  - R5.1.2 - Logs of user account access for each cyber asset;
  - R5.2.3- Provide audit trail records of shared / generic account usage for the cyber asset sample set during the audit period (MM/DD/YY);
  - R5.3 – Provide screenshots or other supporting evidence demonstrating enforcement of password complexity technical requirements, or else provide approved TFE request evidence;
  - R6.4 - Provide security event logs from the audit period (MM/DD/YY) for each cyber asset;
  - R6.5 – Provide supporting evidence that the system event logs generated during the audit period (MM/DD/YY) were reviewed for each cyber asset.

Comments:

A preliminary meeting between the Compliance Monitoring staff and Entity is often required to gain an understanding of the size and complexity of the Entity organization including telecommunications networking, ESP's, PSP'S, access points, and the number and type of cyber assets. These factors are ultimately considered in determining an effective

and suitable approach to sampling. Additionally, as a contingency, RAT-STATS can generate a random number of spares that can be used. Selecting spares provides for additional sample set cyber assets to be tested in place of the initially selected assets where actual results / supporting evidence may not be applicable or available to the initial asset selection.

Availability, format, and size of the data to be sampled during the audit period (or agreed upon alternative time period) should be vetted with the Entity. Also, considerations for preserving historical records should be discussed where applicable. Additionally, issues of privacy, confidentiality, or CEII handling should be reconciled with the Entity to ensure the availability of information and records for testing / sampling.

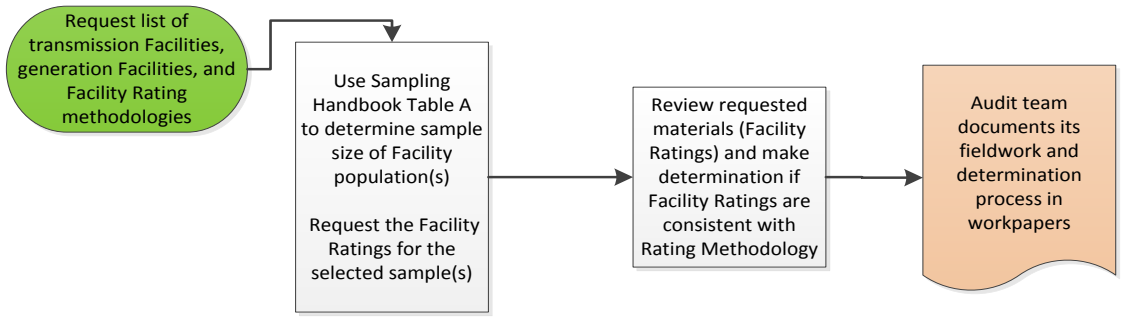
Applicability (Other Standards):
Both the process and sample set can also be utilized in supporting the CIP-009-3 and CIP-005-3 standards and requirements. The CIP-009-3 and CIP-005-3 compliance monitoring staff may also wish to alter the CIP-007-3 derived sample set based on professional judgment and the specific needs of their respective requirements. In the case of CIP-009-3, consideration should also be given to including and addressing the various cyber asset device types (e.g., routers, switches, workstations, firewalls, PLC's, etc.).

Questions for Data Request:
None at this time

FAC-008-3

Requirement 6

Flow Chart:



Process:

- Determine Population Size:
  - Request, if not already available, a list of BES transmission Facilities and generation Facilities along with the Facility Ratings methodology for each from the Entity. From the total population of BES transmission Facilities and/or generation Facilities, determine the total population(s) of elements to be sampled.
- Determine Sample Size:
  - This can be accomplished using the Sampling Handbook Table A or RAT-STATS (or other sampling software) to define the sample population size(s). Then select the samples using RAT-STATs (or equivalent tool) and request the rating data for those samples.
- Testing Results:
  - Review requested materials (Facility Ratings) and make determination if Facility Ratings are consistent with the Ratings Methodology.
- Documentation:
  - Use the Lead Sheet for guidance for various sampling checkpoints; document the sampling approach and audit team determination(s) in audit workpapers.

Comments:
This process applies to Generation Owners (GO) and Transmission Owners (TO). Requirement R6 states the Facility Rating of the generation and transmission Facilities are to be consistent with the Entity's Facility Ratings methodology. Additionally, Regions can further strengthen their evaluations by also performing physical inspections of the Entity Facilities to verify the list of BES transmission Facilities (generation and transmission) and equipment list (population validation).

Applicability (Other Standards):
None at this time

Questions for Data Request:

90-Day Notification Letter:

1. Provide a list of all XYZ Power Company (XYZ) BES Facilities.
2. Provide a system one-line diagram for the XYZ system.

Data Request #1:

1. Provide the Facility Ratings for the following Facilities … (provide XYZ list of facilities determined in the Random Sampling of all XYZ facilities/elements).
2. Provide a station one-line diagram for the following XYZ substations (determined from Random Sample of facilities)

Appendix C – Lead Sheet Template

Preparation Inputs (PI):	Auditor / Analyst Commentary
Engagement Data	
Registered Entity:	
Entity Acronym:	
Entity NCR Number:	
Audit Review Type:	
Review / Engagement Date:	
Preparer:	
Date:	
Workpaper - RSAW Cross-Reference:	
Reviewer/Approval:	
Date:	
Source Population Type:	
Primary	
Dependent / Secondary	
Independent	
Other	
Obtain & Review Source Population(s) Record Layout:	
Identify Data Points, Field Values & Elements for Selection & Testing:	
Determine Alignment of Records History & Sampling Time Period:	
Validate Source Population(s) for Data Integrity & Completeness:	
Process Activities (PA):	
Standard	
Document the Sampling Testing Objective(s): [If applicable, Select the Testing Objective from the Requirements Menu]	
[If Applicable] - **Other Testing Objective(s):**	

Identify & Describe any Impactful Risk [IRA] & Internal Control [ICE] Considerations that were used:	
Select & Document Sampling Approach & Rationale: [If applicable, select Sampling Approach from the Menu]	
Comments and Rationale	
Determine the Initial Sampling & Size:	
Document Relevant Time Periods Considered:	
Population Size	
Select Sample Size Based on Handbook Specifications [Table A] [or] Sampling Tool (e.g., RAT-STATS)	
Document Statistical Sampling Metrics:	
(Table A Default Values)	
Confidence Level (95%)	95%
Margin of Error (10%)	10%
Random Seed Number	
Desired Precision Range (10%)	10%
Rate of Occurrence (0.5%)	0.50%
Comments for changes from default values	
Test Results Output (TRO)	
Assess & Document Test Sampling Results in Line with Stated Testing Objectives:	
Document if Sampling Approach Requires Expansion or Modification	
Document Basis for Expanded Sampling	
Document Basis for Deviations in Sampling or Planned Testing Procedures	
Determination/ Findings	
Area of Concerns	
Recommendation	