Secura

A BUREAU VERITAS COMPANY

RISK ASSESSMENT STANDARDS FOR ICS ENVIRONMENTS

Stash Kempinski
Secura, June 2021

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on

1. Introduction

The number of Internet connected Industrial Control System (ICS) environments is increasing, but their cyber security is still lacking. This lack of cyber security creates risks, and dealing with these risks is often treated as an IT task. However, using classical IT risk assessment methodologies can have adverse effects on ICS functionality and safety. This is why cyber security risks have to be assessed differently in ICS environments. This white paper discusses a selection of risk assessment standards and compares them to highlight their key differences. The following standards are chosen because of their generality, or their applicability to ICS environments:

- **ISO/IEC 31010:2009**: "Risk management - Risk assessment techniques"
- **IEC 62443-3-2:2020**: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design"
- **NIST SP 800-30r1**: Guide for Conducting Risk Assessments

ISO/IEC 31010 is used, instead of the more famous ISO 27005 standard, due to its generality. ISO 27005 is specifically written for IT and is derived from ISO 31000[1], hence it contains information not necessarily applicable to ICS environments.

The **IEC 62443** series of standards is probably most widely known and used in ICS. It is written specically for ICS, and contains standards for every step in the ICS design process. The IEC 62443-3-2 standard contains a step-by-step guide on how to conduct a risk assessment.

NIST has a standard that is focussed on ICS security (**NIST SP 800-82**) which contains helpful ICS specific information, but only little risk assessment information. The **NIST SP 800-30 standard** on the other hand is specifically written for risk assessments and provides clear, step by step guidance and tips. This makes NIST SP800-30 more suitable to discuss than NIST SP 800-82, even though it is not tailored to ICS.

Another well known standard series is **NERC CIP**. It contains a vulnerability assessment standard (NERC CIP 010-3) that states compliance requirements, but it does not provide real guidance. Hence, it is not considered for this white paper.

Table of Contents

[1] ISO 31000 is an accompanying standard for ISO/IEC 31010, it discusses risk management in total.

2. The Standards

This section describes each standard in their respective subsection. Each subsection contains a summary of the necessary tasks needed to perform a risk assessment, and explains the standard specific terminology. A mapping of the tasks between standards can be found in the Appendix. To capture the tone of the standards as accurately as possible, the same terminology is used wherever possible.

2.1. ISO/IEC 31010

ISO/IEC 31010 defines risk assessment as "**the overall process of risk identification, risk analysis, and risk evaluation**". Each step takes inputs from, and outputs to, other steps that are within the bigger risk management process. These inputs and outputs should be well documented, not only for reporting purposes but also for reviewing and improving the risk assessment process. ISO/IEC 31010 provides an elaborate list of existing risk assessment techniques, each with its pros and cons, and provides guidance on how to select the right techniques.

The **risk identification** process consists of documenting all possible risks in the organization before identifying the existing controls (countermeasures). In other words, even risks that are already mitigated should also be documented. All factors that make up a risk should be documented, so risks can be adjusted accordingly whenever a factor changes. These factors include, but are not limited to, the source, cause, and impact of events (note the word "event" being used instead of "threats"). ISO/IEC 31010 places emphasis on human and organizational aspects also being factors that can create risk. Hence, these aspects should be included in the risk identication process.

The most important part of the risk assessment process is **risk analysis**, ISO/IEC 31010 defines this process as "**developing an understanding of the risk**". This step uses the documented factors from the risk identification step to determine the likelihood and impact of events, and the effectiveness of existing controls. The outcome of this step is very dependent on the scope and context of the risk assessment, which are both defined in the risk management process developed in ISO 31000. These factors also determine which risk analysis methods are usable and how risk will be expressed/rated. Methods can be combined, but the rating of risks must be consistent to ensure that the derived ranking can be used to prioritize risks. The risk analysis process is split into five tasks: the first task, **controls assessment**, analyses the existing controls to determine their effectiveness. Next, **consequence analysis**, determines the impact of an identified event occurring. Using the controls assessment outcome, **likelihood analysis and probability estimation** can be performed to determine the likelihood of events. Using the determined impact and likelihood, **preliminary analysis** can be performed to determine risks, and to rank them so resources can be used efficiently. Lastly, the **uncertainties and sensitivities** of all factors that make up the risks must be documented. This helps organizations to evaluate each risk as complete and accurate as possible.

Risk evaluation is the last risk-related step of the ISO/IEC 31010 risk assessment process. In this step, the risks are evaluated using the criteria defined in the risk management process. These evaluations are used, in combination with other considerations (e.g. financial), as input to make risk treatment decisions. These decisions include what risks should be prioritized and if risks need treatment at all.

The final part of the risk assessment process consist of **documenting** the risk assessment results in a clear and consistent matter and **reflecting** on the process itself. Consistently documenting the outcomes of the risk assessment enables organizations to integrate the findings in their risk management process. The reflection on the process is needed to improve and update information (sources) where necessary.

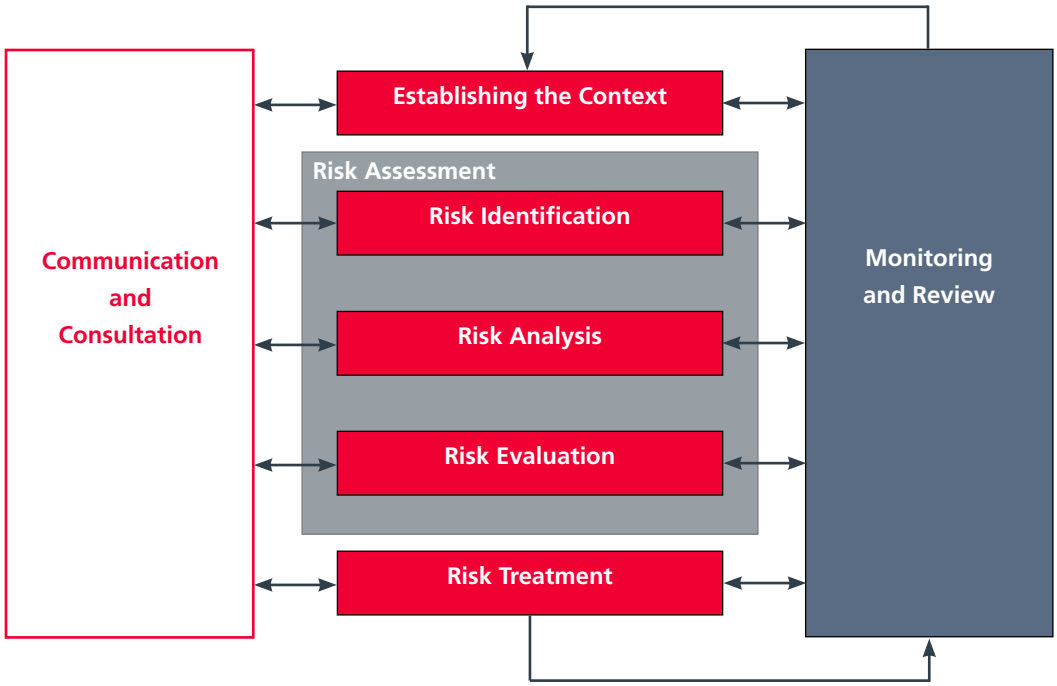


Figure 1: The Risk Management Process of ISO31000 and ISO/IEC31010

2.2. IEC 62443-3-2

IEC 62443-3-2 consists of a list of zone, conduit and risk assessment requirements that helps organizations systematically perform risk assessments. These requirements, called **zone and conduit requirements** (ZCR), must be fullled to correctly perform a risk assessment.

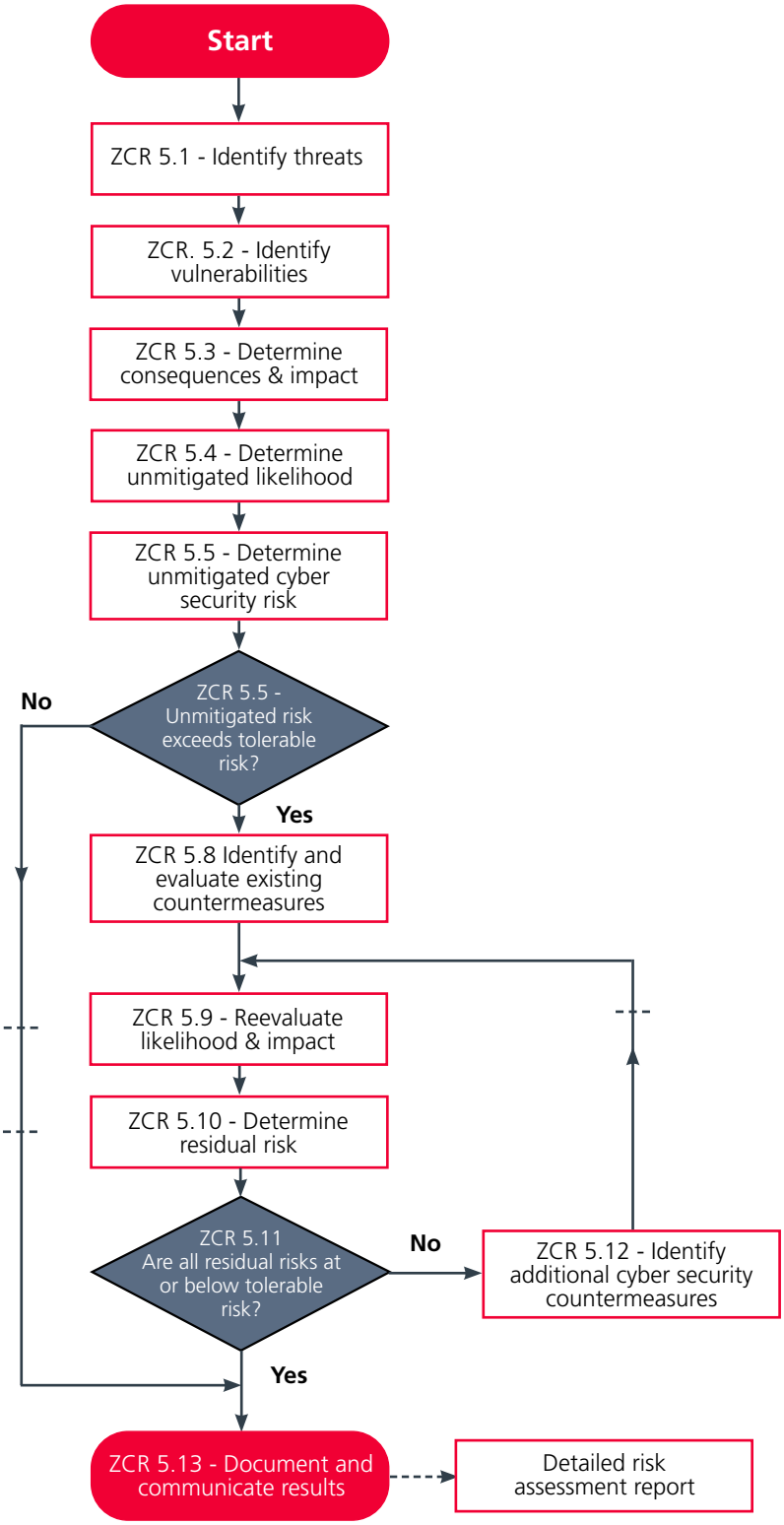
The first ZCRs consist of determining the System Under Consideration (SUC), and performing an initial risk assessment using existing documentation. The SUC is then divided into relevant zones & conduits and for each zone/conduit it must be determined if a "detailed" risk assessment should be performed. This must be determined using the target security level (SL-T) that must be defined for each zone/conduit. Note that zones and conduits are not required to have the same SL-T. The detailed risk assessment consists of multiple small steps, starting with identifying threats, vulnerabilities, and their consequences (impact). In the detailed risk assessment three types of risk are further specied: **unmitigated risk, tolerable risk,** and **residual risk**. These risks are determined in this order.

To find the **unmitigated risk**, the unmitigated likelihood of all identied threats and vulnerabilities must be determined. Using this unmitigated likelihood, the unmitigated risk can be calculated using the organization preferred risk calculation method.

Using the unmitigated risks and SL-Ts, the **tolerable risks** are determined. These risks are within the bounds that organizations deem acceptable, and thus do not need more resources or time allocated. For the non-tolerable risks, the existing countermeasures must be identified and evaluated. With these countermeasures in mind, the likelihood and impact can be re-evaluated. The residual risk is calculated using these re-evaluated attributes, which is then compared to the tolerable risk.

The last part of the risk assessment consists of defining extra countermeasures for the remaining **residual risks**, recalculating the residual risks, and repeating this process until no more risks exceed the SL-T of the zone/conduct each risk belongs to. These suggested extra countermeasures should be documented and communicated to the stakeholders together with all the identified risks.

Figure 2: The Risk Assessment Process of IEC 62443-3-2



2.3. NIST SP 800-30

NIST SP 800-30 divides the risk assessment process in four steps: **prepare, conduct, communicate, and maintain**. Each step consists of multiple tasks that have to be completed, at a minimum, to effectively conduct a risk assessment. Organizations are free to implement other procedures in the risk assessment process if they want to, NIST SP 800-30 only intends "to provide a common expression of the essential elements of an effective risk assessment". NIST SP 800-30 provides templates for most tasks to help organizations in the risk assessment process.

The first step, **preparing**, is about collecting the information needed for a risk assessment. The purpose and scope should be defined first and are in turn used to identify assumptions and constraints. Explicitly defining these aspects is necessary to identify the information sources that must be consulted during the risk assessment. For example, legislations that are relevant for the organization its business. Lastly, **the risk model** and **analytic approaches** used in the risk assessment must be determined in this step.

Conducting the risk assessment consists of identifying threat sources, the events possibly caused by these sources, and vulnerabilities within the organization.

For these three aspects the likelihood and impact must be determined. The likelihood and impact are used to calculate the risks using the **analytic approach** defined in the previous step. The performed tasks should adhere to the used risk model to ensure that the risks are comparable. It is not necessary to perform the tasks in order, although most tasks rely on each other.

The findings of the risk assessment have to be **communicated** to the stakeholders. Risk-related information should be shared with the whole organization, to make employees aware of the existing risks. Communicating and sharing of information should be done constantly throughout the risk assessment process to ensure every relevant party has the most updated information at any time. This ensures that the risk assessment is conducted as accurately as possible.

The last step is **maintaining** the risk assessment. Risk-related information should be shared whenever possible, and existing risks and information sources should be monitored for new threats, vulnerabilities, or changes. This step also includes determining the effectiveness of the risk responses and verify compliance.

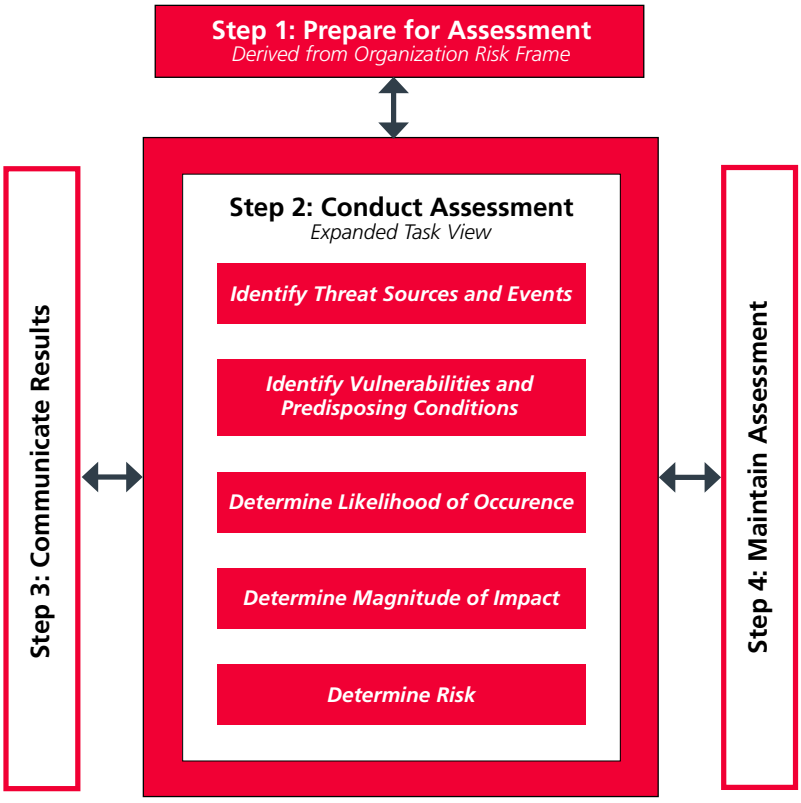


Figure 3: The Risk Assessment Process of NIST SP 800-30

3. Key Differences

This section highlights the key differences between the standards as objectively as possible. The complete standards are used for comparison, hence the differences mentioned here are not necessarily derivable from the previous section.

3.1. Risk Assessment Tasks

ISO/IEC 31010 does not consider the defining of **scope, context** and **criteria** part of the risk assessment. Defining these aspects is part of the risk management process defined in ISO 31000. This makes ISO/IEC 31010 unsuitable to be used on its own, and thus should be used in combination with the risk management process described in ISO 31000.

IEC 62443-3-2 does not consider reflecting a task in the risk assessment itself. There could be multiple reasons for this; the first is that monitoring and improving is a different category of the IEC-defined risk management framework[2], so also doing this in the risk assessment process itself would be redundant. Another reason is that IEC 62443-3-2 states that "risk assessments are often facilitated by third-parties...", hence reflecting is less relevant for the organization that is being assessed, but more important for the assessors.

All three standards disagree on target risk levels: if there should be a target, and where in the risk assessment process this target should be determined. ISO/IEC 31010 and IEC 62443-3-2 agree that a target risk level should be determined; ISO/IEC 31010 does this before the start of the risk assessment, IEC 62443-3-2 only after the unmitigated risk is determined. NIST SP 800-30 does not consider a target level explicitly, but leaves this implicit when determining the significance of risk.

3.2. Trust and Organizational Culture

The NIST dedicates a sizeable part of its SP 800-39[3] standard to **organizational culture, trust (and trustworthiness), and how this impacts risk management**. This standard states that both organizational culture and trustworthiness are essential in how organizations are willing to address risk. It gives definitions of these concepts, how they influence risks, and why this might differ per organization (or even within an organization).

NIST SP 800-39 does this, among other things, by providing multiple trust models, how they are established, and how they influence organizational behaviour. It also describes the relationship between these concepts and different risk-related concepts. The NIST SP 800-30 standard further describes the effects of these concepts on the risk assessment process itself, for example if organizations prefer quantitative or qualitative risk assessments.

The risk management standards of ISO and IEC (ISO 31000 and IEC 62443-2-1) state that an organizational culture should be taken into account in risk management/assessment, but does not provide any rationale for why and how this should be taken into account. ISO/IEC 31010 mentions culture once, and IEC 62443-3-2 does not mention culture at all. The influence of trust is not mentioned in any of these standards.

3.3. Unmitigated Risk

As explained in Section 2.2, the **unmitigated risk** is the risk that is calculated using the likelihood of a threat occurring/vulnerability being exploited without taking into account the existing countermeasures (the unmitigated likelihood). The purpose of this unmitigated risk, when considered at all, differs between the three standards.

ISO/IEC 31010 mentions in the risk identification process that "once a risk is identified, the organization should identify any existing [countermeasures] such as design features, people, processes and systems", but it does not explicitly name this risk (like IEC 62443-3-2 does). The "controls assessment" step in ISO 31010 evaluates the existing controls (countermeasures), for this evaluation the unmitigated risk should be known. Hence, even though ISO 31010 does not explicitly use the term unmitigated risk, it uses the concept.

[2] This framework is called the "Cyber Security Management System" and is defined in IEC 62443-2-1.
[3] This is the NIST risk management standard, which describes the impact of trust and organizational culture more elaborately than NIST SP 800-30.

IEC 62443-3-2 uses unmitigated risk to determine the risks that do not meet their SL-T, and thus need countermeasures. It also uses the unmitigated risk to evaluate the existing countermeasures. The unmitigated risks that do meet the SL-T requirements are not further considered in the risk assessment process. This is a big difference with the other two standards, which both consider all identified risks throughout the complete risk assessment process.

NIST SP 800-30 does not consider unmitigated risks at all, the "determine likelihood" step takes countermeasures into account from the start. This is in line with NIST SP 800-30 not determining a target risk level either, hence it does not need specially identified risks for comparison purposes.

3.4. Assessment Step Order

IEC 63442-3-2 its risk assessment process is quite linear and leaves little space for reordering. Although tasks like "**identify**" and "**evaluate existing countermeasures**" could be done earlier in the process, this can be redundant as it is not needed for risks that are at a tolerable level already.

The same sort of linearity can be found in ISO/IEC 31010. Both ISO 31000 and IEC/ISO 31010 are needed to complete a risk assessment as tasks defined in ISO 31000 have to be completed to do an effective risk assessment.

The NIST standard provides more freedom, the order of the tasks in each step is in most cases not important, as long as they are completed before continuing to the next step. This opens up the possibility to parallelize the tasks in different steps.

3.5. Uncertainties of Identified Risk Factors

Both NIST SP 800-30 and ISO/IEC 31010 emphasize the uncertainties of factors that make up risk, and the importance that these should be documented. Both standards also agree that documenting these uncertainties is essential for the accuracy and interpretation of the risk assessment outcome. ISO/IEC 31010 has a dedicated task for this, uncertainties and sensitivities analysis, and NIST SP 800-30 mentions this throughout the different tasks. The IEC 62443-3-2 standard does not consider uncertainties at all.

3.6. Level of Detail

Not necessarily a key difference, but still noteworthy is the level of detail and the grouping of steps and tasks. Although most of them are trivial (like how the IEC combines "re-evaluate likelihood and impact" in one step), two are worth mentioning.

The first is the **identification of risk**. As can be seen in table of Appendix A, ISO/IEC 31010 generalizes this to one step, IEC 62443-3-2 divides the identification over multiple steps, and NIST SP 800-30 has the "conduct" step explicitly divided over multiple tasks. The more detailed steps of IEC 62443-3-2 can be explained by the different forms of risk that get determined in this standard.

The second difference is the **level of detail, the description, and explanation of steps**. Where NIST SP 800-30 provides elaborate "supplemental guidance" for each task, IEC 62443-3-2 only gives short descriptions per step (sometimes just one or two sentences). The level of detail of the ISO/IEC 31010 step description is somewhere in between, but where NIST SP 800-30 provides examples of task outcomes, ISO/IEC 31010 provides information of applicable risk assessment techniques.

4. What Standard is the Most Applicable for You?

The applicability of each standard differs per organization. This section summarizes several factors that can be taken into account when deciding which standard is best applicable to your situation. All three standards allow adjustments in their processes, hence standards can be combined when needed. The following table summarizes these decision factors per standard.

Factor	ISO/IEC 31010	IEC 62443-3-2	NIST SP 800-30
Audience	Written with ISO 31000 in mind, hence most applicable for an organization that wants to do the risk assessment using an **internal team.**	Risk assessment from start to finish, hence an **external organization.**	The generality makes it useful for **all organizations involved** in the risk assessment.
Scope	Focused on what happens **within an organization.**	Written specifically to assess **systems**.	**Takes everything into account**, from organizational factors to business processes, systems, and external relations.
Risk Managment Maturity needed	**A risk management system has to be in place already** when using ISO/IEC 31010.	**Can start from zero**, but having existing previous risk assessments is preferred.	**Can be used to start and setup a risk management strategy.**
Duration of the Risk Assessment	**Medium**, in between IEC 62443-3-2 and NIST SP 800-30 based on the times risk is assessed.	**Longest** due to amount of risk evaluations.	**Shortest**, due single evaluation of risk.
When to not use this Standard	When **no risk management framework is in place.**	When continuity **is preferred.**	In **very dynamic environments** (organization structural wise).
Number of Risk Evaluations	**Two**, once without taking controls into account and once while taking controls into account.	**At least twice**, until enough countermeasures are in place.	**Once**, everything is taken into account.
Continuity	**Strongly present**, risk assessment is a part of the continuous risk management process.	**None**, after delivery the process ends.	**Present** through the maintaining step of the risk assessment process.
Recognition	**Internationally** recognized.	**European** recognized.	**American** recognized.

Secura
A BUREAU VERITAS COMPANY

5. Conclusion

Although all standards cover the necessary steps to effectively conduct a risk assessment, their approaches and audience differ. **The risk assessment of ISO/IEC 31010 and the ISO 31000 risk management processes are very intertwined.** The best example for this is that there are essential tasks missing from ISO/IEC 31010 (which are done in ISO 31000). This can create very effective continuous risk assessments when all risk-related tasks (both assessment and management wise) are done by entities within the assessed organization. However, when the risk assessment is done by an external organization it can slow the process down due to both organizations having to adjust their methods to fit within the assessment or management framework of the other.

IEC 62443-3-2 is aimed towards external organizations doing the risk assessment. The explicit documenting of the SUC and its zones and conduits is something that should be available within the organization already. More importantly, the lack of continuity makes IEC 62443-3-2 unsuitable for internal organizational use. This continuity is present in NIST SP 800-30 (through the maintaining step), and to some extend in ISO/IEC 31010 through the reflecting step in the risk assessment. The length of IEC 62443-3-2 might be another reason to choose a different risk assessment standard. Risks are at least evaluated twice, opposed to NIST SP 800-30 where risks are evaluated once. But this is not the only reason to choose NIST SP 800-30 over IEC 62443-3-2 (and ISO/IEC 31010).

NIST SP 800-30 covers more than just the technical aspects of risk evaluation, like how organizational culture and trust influence risks. As NIST SP 800-30 is the only standard that covers these aspects, and it is free of charge, there is no downside to incorporating NIST SP 800-30 in a risk assessment methodology. NIST SP 800-30 elaborately explains all steps and tasks of a risk assessment, giving a clear idea on what should be done and also why it should be done. These elaborate explanations are not just helpful for organizations specializing in risk assessments, but also for organizations that are being assessed. By reading this standard, the organization that is being assessed can help the assessing organization greatly, especially in the preparing step. For example, can the right information sources already be identified, saving valuable time for the assessing organization.

The uncertainties and sensitivities analysis of ISO/IEC 31010 can complement IEC 62443-3-2 greatly. As all risks, their controls, and security target level are explicitly documented, this analysis creates very effcient consecutive risk assessments. Given that no risks are left undocumented during the initial risk assessment, only the changes within the organization between assessments have to be collected. The risk factors that have changed can now easily be adjusted and be re-evaluated according to their security target level. Only when new zones or conduits are added, or when major organizational changes have occurred, a more elaborate risk assessment is needed.

In conclusion, while the standard(s) of a single standard organization are sufficient, combining them creates a more robust risk assessment. Which standards, and how to combine them, greatly depends on the **risk management maturity** of an organization and the **scope of the risk assessment.**

About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: **secura.com.**

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: secura.com/subscribe.

Follow us on

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Appendix: Risk Assessment Task Mapping

This table shows, where possible, a mapping between the different steps of each standard. If there are steps that are not present in one guideline, the row of that standard is empty. If multiple steps in one standard are grouped into one step in another it is represented as a cell spanning a set of cells. Steps that span multiple non-consecutive steps are mentioned on the same row with just their step number in bold. The step and task numbers are kept line with the respective standards. Note that the tasks within step 3 of ISO/IEC 31010 are not part of ISO/IEC 31010 but are part of ISO 31000.

ISO/IEC 31010	NIST SP 800-30	IEC 62443-3-2
3.2 Defining the scope	1-1 Identify purpose	1 Identify the System under Consideration (SUC)
	1-5 Identify risk model and analytic approach	Implied that this is already done
		2 Perform an initial cyber security RA
3.3 External and internal context	1-2 Identify scope	3 Partition the SUC into zones and conduits
	1-4 Identify information sources	
3.4 Defining risk criteria	1-3 Identify assumptions and constraints	4 Check if initial risk exceeds tolerable risk
5.2 Identify Risks	2-1 Identify threat sources	5.1 Identify threats
	2-2 Identify threat events	
	2-3 Identify vulnerabilities and predisposing conditions	5.2 Identify vulnerabilities
	2-5	5.3 Determine consequence and impact
		5.4 Determine unmitigated likelihood
		5.5 Determine unmitigated (cyber security) risk
3.4		5.6 Determine SL-T
		5.7 Compare unmitigated risk with tolerable risk
5.3.1 Controls assessment	**2-3**	5.8 Identify and evaluate existing countermeasures
5.3.2 Consequence analysis	2-5 Determine impact	5.9 Reevaluate likelihood and impact
5.3.3 Likelihood analysis and probability estimation	2-4 Determine likelihood	
5.3.4 Preliminary analysis		5.10 Determine residual risk
5.3.5 Uncertainties and sensitivities analysis	2-6 Determine risk	
5.4 Risk evaluation		5.11 Compare residual risk with tolerable risks
		5.12 Identify additional cyber security countermeasures
5.5 Document results	3-1 Communicate risk assessment results	5.13 Document and communicate results
	3-2 Share risk-related information	
5.6 Monitoring and reviewing RA	4-1 Monitor risk factors	
	4-2 Update risk assessment	

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS

Shaping a World of Trust