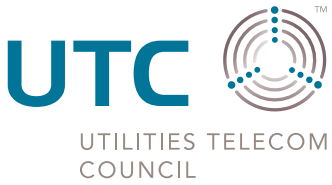
CYBER SUPPLY CHAIN RISK MANAGEMENT FOR UTILITIES— ROADMAP FOR IMPLEMENTATION



April 2015

Nadya Bartol, CISSP, CGEIT

Utilities Telecom Council

1129 20th Street NW

Suite 350

Washington, DC 20036

(202) 872-0030

www.utc.org

AUTHOR

Nadya Bartol, CISSP, CGEIT is UTC VP of Industry Affairs and Cybersecurity Strategist. She leads UTC cybersecurity initiatives world-wide. A dynamic leader, she works with UTC members and numerous industry partners to design, develop, and deliver practical solutions that help solve immediate utility cybersecurity challenges. She leads a number of industry initiatives driving strategic solutions to long term utility cybersecurity challenges including workforce development, utility modernization, and IT/OT convergence. An experienced convener of technical experts, Nadya moderates several peer-to-peer utility-focused cybersecurity forums, where utilities share their daily cybersecurity challenges and solutions for quick application to standing problems.

A leader in cybersecurity standardization, Nadya is responsible for driving the initiation, justification, development, and completion of the first global standard addressing security risks associated with supplier relationships, ISO/IEC 27036. She is an active contributor to US cybersecurity initiatives including the development and implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, development of Energy Delivery Systems Cybersecurity Procurement Language, and creation of cybersecurity framework implementation guidelines for the Energy and Communications Sectors, including CSRIC WG4.

Nadya is a consummate people leader and program manager. Before joining UTC, Nadya worked at global management and technology consulting company where she was responsible for leading multidisciplinary teams to capture, develop, and deliver cybersecurity services to US government and commercial clients. Nadya is a frequent speaker at premier industry events including RSA conference and SANS ICS Security Summits. Additionally, Nadya reaches a significant social media audience as host of the monthly UTC cybersecurity informational webinar series and via the numerous educational webinars she produces/collaborates in creating.

ACKNOWLEDGMENTS

UTC would like to acknowledge Jennifer Bisceglie of Interos Solutions for her contribution to this paper.

ABOUT THE UTILITIES TELECOM COUNCIL

Created in 1948, the Utilities Telecom Council (UTC) is an international trade association for the telecom and IT interests of electric, gas and water utilities and other critical infrastructure industries (CII), such as oil and gas pipeline companies.

UTC's members include large investor-owned utilities that serve millions of customers, as well as smaller municipal and cooperatively organized utilities that serve only a few thousand customers. In addition to its members in the United States, UTC has members in Canada (UTC Canada), Europe (European UTC), South America (UTC America Latina) and Africa. UTC's members all own, manage, or operate extensive wireless and wireline communications networks that they use to support the safe, reliable and effective delivery of essential energy and water services to the public at large.

UTC advocates before federal, state and local government executive, legislative and judicial bodies to support the advancement and security of the telecom and IT networks of utilities and other CII. It provides education and information services through conferences, publications, and electronic media. It also provides networking and technical services, including frequency coordination, to its utility and CII members and their associated technology partners, such as equipment manufacturers, engineering firms, and consultants.

ROADMAP FOR IMPLEMENTATION

This paper provides a roadmap tailored to the utility space on how to successfully organize supplier management activities while addressing associated security risks. It is based on practical experience, numerous discussions with utilities and vendors, and recently published standards and best practice documents.

Utilities rely on extensive networks of business partners and suppliers to support critical enterprise capabilities: systems integration, engineering and building of substations, customer support, data analytics, a variety of electric power equipment and networking devices, training, financial services, and many others. To make matters more complex, utilities' business partners and suppliers also rely on extensive networks of suppliers. Meter manufacturers do not make all components of their meters in-house; rather, they assemble components provided by other manufacturers. Network equipment is similarly integrated by its manufacturers, rather than made in-house. Financial service providers rely on third parties for data processing. Engineering companies hire subcontractors. Software companies outsource certain parts of their development lifecycles. Everyone has a supply chain… most suppliers outsource their functions as well and so the end-customer ends up with webs and chains of suppliers that they do not have visibility into nor are they able to influence.

Today, many utilities are in the process of restructuring how they manage supplier relationships to address increased myriad security risks. The experience of these utilities demonstrates that the process is not easy and it requires stakeholders from across the organization to collaborate for success. Several standards and best practice documents emerged recently that provide useful information to guide this process.

To manage these risks, utilities need to articulate their expectations and institute appropriate monitoring regimes without putting undue burden on critical business relationships with suppliers that they depend on to deliver their own service. This means that those who acquire (acquirers) and those who supply (suppliers) need to engage in a productive, two-way conversation, with the explicit goal of arriving at a set of expectations and responsibilities that are balanced and achievable.

ISO/IEC 27036—Information Security in Supplier Relationships

Energy Delivery Systems Cybersecurity Procurement Language

Draft IEC 62443-2-4—Requirements for IACS Solution Suppliers

NIST SP 800-161—Supply Chain Risk Management Practices for Federal Information Systems and Organizations

DEFINING THE PROBLEM

When an enterprise buys or sells products and services from or to another enterprise, the two enterprises may gain access to information that may be sensitive, connect systems that may be critical, allow each other's employees access to facilities, or take components created by one organization and integrate those components into a product that will ultimately be sold by another organization to a consumer. Very few (if any) enterprises can say that they completely control everything they make, and that no individual or system belonging to another enterprise touches its products or services before these products and services are delivered to the consumer. Regardless of who does what, the enterprise that presents the final product or service to the customer remains the responsible party for the resulting product or service. That enterprise will also be held responsible if something goes wrong that impacts its customers or other stakeholders such as employees, shareholders, or regulators.

Managing what is not under your control is inherently more difficult than managing everything in-house. This requires a new approach to managing relationships with business partners and suppliers that is completely integrated into how an enterprise manages its systemic risks. In that new approach, agreements and contracts are not the beginning or the end of the relationship; rather, they document specific aspects of the relationship and are a piece in a comprehensive approach that both acquiring and supplying enterprises should deploy. It should be noted that this is not about putting all responsibility on the other party. Instead, this is about sharing a responsibility between the two parties by agreeing to protect each other's infrastructure. According to the 2014 Verizon Breach Report,[1] the number of breaches originating from business partners remained flat since 2007, while the number of breaches attributed to external parties has risen tenfold within the same time period. In the percentage terms, while breaches attributed to business partners declined to a very small number, the percentage of breaches attributed to an external threat increased from roughly 40% to 90%. Given these sets of threat facts, it is clear that supply chain risk management is becoming more and more important since, by establishing any supplier relationship, the acquirer (i.e., utility) exposes itself to that supplier's complete supply chain.

Utilities have hundreds to thousands of suppliers, each of which has its own frequently global supply chain. This distributed approach was facilitated by the advent of decentralized acquisition practices (responsible managers can buy what they need for their business lines) as well as by mergers and acquisitions. The result is that numerous companies out there, including utilities, do not know how many suppliers they have, who these suppliers are, and, most importantly, what risk these suppliers may represent to the utility.

Information and Communication Technology (ICT) presents an especially difficult version of this challenge because 1) ICT suppliers directly support critical capabilities in every utility; 2) ICT is present in the infrastructure and can have a negative impact on it long after the supplier is gone;

[1] http://www.verizonenterprise.com/DBIR/2014/

and 3), many aspects of the ICT supply chain involve ICT manufacturers' intellectual property and are therefore highly sensitive.

With respect to the second challenge (long-lasting security impact)—managing security risks associated with these relationships is especially challenging because vulnerabilities discovered in ICT are frequently not found until long after the relationship with an ICT vendor has ended. This may lead to compromise of reliability and safety of the services that utilities are delivering to their customers. Utilities that do not look into the risk that is associated with the ICT products and services that they bring in-house assume an unknown risk of reduced capability or malicious capability at an unknown point in the future which may result in reduced or unavailable service or compromised safety.

With respect to the third challenge (presence of intellectual property)—providing some sort of visibility for acquirers into its suppliers' proprietary development and acquisition processes requires a delicate balance for both acquirers and suppliers to protect everyone's sensitive data and critical infrastructure.

THE ELEMENTS OF A SOLUTION

As in any successful relationship, job one in overcoming a challenge is to recognize the problem exists. Job two is to develop a plan of attack on how to fix it. The last five years has seen the broad development and publication of best practices, standards, and guidelines to help provide a strategy for articulating 3rd-party supplier/acquirer risk expectations and monitoring conformance to those expectations.

The solution boils down to articulating mutual expectations and responsibilities for managing the security risks of:

- Sharing information and resources among acquirers and suppliers: people, services, infrastructures, information, and facilities;
- Integrating information and communication technology (ICT) components provided by suppliers into existing infrastructures depending on products that will be operational for years to come;
- The increased use of outsourced services, such as cloud services.

Integrating security considerations into supplier relationships is a joint responsibility for acquirers and suppliers. It is critical that utilities organize their own processes and activities in such way that they are conducive to building productive and security-conscious relationships with suppliers. The remainder of this paper presents ten basic practices that will help utilities begin to organize relationships with their suppliers in a productive way.

It should be noted that many of the practices addressed here already exist in numerous acquirer and supplier organizations. However, these practices may not have been the subject of discussion among acquirers and suppliers up to this point.

1. **Identify critical assets, systems, and processes, and prioritize them**
2. **Identify critical data/information about your business and customers**
3. **Identify your suppliers**
4. **Assess supplier risk and prioritize suppliers**
5. **Establish general security requirements by priority**
6. **Establish how you will want to share information with suppliers on vulnerabilities and incidents**
7. **Establish how you will want to monitor supplier adherence to requirements**
8. **Get the people within your organization up to speed**
9. **Make arrangements for contingencies**
10. **Conclude supplier relationship in a risk-conscious way**

TEN BASIC PRACTICES

1. Identify critical assets, systems, processes and prioritize them.

Existing practices that help: **Asset Management, identifying Critical Cyber Assets (NERC) and Critical Digital Assets (NEI).**

It is impossible to protect everything equally well because nobody has infinite resources. Choices need to be made as to what is absolutely critical and thus requires greater protection. Knowing which assets are most critical and which suppliers support these assets is a first step towards gaining an understanding of the security risks associated with those supplier relationships.

Prioritize assets by criticality, for example which assets are highly critical, moderately critical, and somewhat critical. This will require a cross-organizational group of business owners, engineering, OT, telecom, sourcing/acquisitions, legal, physical security, cybersecurity, HR, and potentially other leaders to get in the room and talk about what is critical and why. While everything will be critical at first, clear priorities will emerge as the group has an opportunity to interact and explain different views to each other. NERC CIP critical assets and NEI Critical Digital Assets (CDA) will be naturally categorized as critical, but there will be other systems that are critical to a utility's business. Those may include customer or employee data. Assets will then need to be organized into understandable categories.

2. Identify critical data/information about your business and customers

Existing practices that help: **Data Classification, Information Protection (NERC)**

In any relationship between acquirer and supplier, data is exchanged or accessed by the other party which may be proprietary, sensitive, or somehow otherwise specific to one of the parties in the relationship. The acquirer and supplier should discuss what data will be shared and decide what is necessary to be shared and how this data should be protected. Examples of this data include customer records, electricity or water usage data, engineering drawings and network configurations, wiring maps, lists of executives and their salaries, security vulnerabilities, and numerous other types of business-specific information. The party which receives such data has a responsibility to protect it from unauthorized access and release, both intentional and unintentional. How the data is to be protected should be explicitly discussed and documented among the two parties. This question is especially critical because just as the acquirer is sharing its specifications, critical needs, and proprietary information with the supplier, the supplier may be in a similar situation with its own suppliers.

3. Identify your suppliers

Existing practices that help: **Supply chain/sourcing/acquisition processes.**

NOTE: This may be outside IT, OT, Telecom, or security processes.

Knowing who your suppliers are is critical for managing security risks associated with supplier relationships. If your organization is large and decentralized, this may be challenging. The same group that you created to identify your assets can help you identify your suppliers. Each of the assets that they identify will be supported by suppliers. Even though the members of the group may not know who the suppliers are, they will direct you to someone who does.

Utilities have hundreds to thousands of suppliers. Not all of them will be identified at the same time. But, you can't manage what you can't measure and certainly, you can't manage what you don't know. The most used suppliers will be known quickly, but it is also important to identify all other suppliers so that you can understand and manage the risk. Many of the publicized breaches in 2014 and 2015 targeted suppliers to breached organizations.

Ideally, acquirers would want to have their suppliers identified in the supply chain. This may not be practical, especially for ICT, given the distributed and global nature of supply chains. Depending on the criticality of the asset/supplier and the level of integration between utility and supplier staff and systems, utilities can ask these suppliers to identify primary sub-suppliers.

If that is not practical, utilities can ask their suppliers to ascertain or demonstrate that they have robust supplier management program themselves and that they are managing supply chain risks as required. Examples of such practices include explicit processes to purchase parts from authorized resellers, having standardized contractual language that addresses security concerns, and propagating those security requirements down the supply chain. It is recommended that utilities engage in a dialog with their suppliers about what is practical and appropriate to arrive at the best solution.

4. Assess supplier risk and prioritize suppliers

Existing practices that help: **Enterprise risk management processes.**

NOTE: This is outside IT, OT, Telecom, or security processes

Not all suppliers are created equal. That is why several standards and best practices use different terms for different types of suppliers. Some suppliers will serve in the role of system integrators, which means they will have access to acquirers' detailed requirements, configurations, plans, engineering drawings, facilities, and other assets or resources. This relationship is highly integrated and includes providing access to highly sensitive information to individuals who are not employed by the acquirer. It also includes providing access to acquirer systems for these individuals, and to potentially establishing a system-to-system access between the two organizations. Finally, it is expected to be a long-term relationship. These suppliers are high-value and high-risk at the same time. They are high-value because the supplier is supporting substantial acquirer functions and capabilities. They are high-risk because of the level of integration between acquirer and supplier people and systems. That level of integration is inherently difficult for the acquirer to control and monitor. Also, a lengthy relationship means that the exposure is spread over a long time. The acquirer has to establish a substantial level of trust with the supplier to address this risk. Please note that this goes in both directions. The supplier also needs to establish a substantial level of trust with the acquirer because the supplier's systems and people are integrated with the acquirers' systems and people. If the supplier is sharing their trade secrets with the acquirer, they may be as concerned as the acquirer about risks involved. This means that organizing this relationship will benefit both parties.

Other suppliers will just be providing commodity components that can be acquired from several different suppliers. That is a more discrete relationship that has limited access for both systems and people on both sides. However, these commodity components may be supporting highly critical functions in the acquirer systems and therefore the risk of those components being somehow compromised is nevertheless high.

These are just some of the criteria that the enterprise should consider when assessing risks associated with their suppliers. At a minimum, utilities should look at the following dimensions of their supplier relationships to understand associated risks:

1. Will/are your and suppliers systems accessing each other?
2. Will/are suppliers' people have access to your facilities? To your systems?
3. How long do you expect this relationship to last (one-time, short-term, mid-term, long term)?
4. How important/critical is the function/system/capability provided by the supplier to you?

Once you have assessed your supplier relationships from the point of view of potential risk, it is time to bring together your understanding of your supplier base and your understanding of your assets inventory. The next step is to identify which suppliers support or supply the assets in your asset inventory. For example, which company provides maintenance and upgrades for a critical customer management or billing system; which manufacturer supplies critical network components; what company delivers critical hardware components; or what company provides data analytics that are used for critical decision making.

Suppliers that support your most critical assets and that present the highest risk exposure are your critical suppliers. Suppliers that support your least critical assets and that present the lowest risk exposure are your least critical suppliers. This assessment and ranking can be done using a simple spreadsheet or a more sophisticated prioritization tool.

5. Establish general security requirements by priority

> **Existing practices that help:** **Existing security requirements.**

Security requirements provide a language for utilities to communicate their expectations to suppliers. The level of rigor in these requirements should depend on the criticality of suppliers to utilities operations. These should be high-level requirements that articulate the outcome rather than specific ways to do things or specific technologies. Getting into too much detail may limit innovation and potentially security. What if a supplier has a better way of getting to the acquirer's desired outcome than the way the acquirer specifies?

Any supplier relationship should set a high-level of security requirements that apply to that relationship. But these high-level security requirements should be different based on supplier criticality. Several sets of security requirements may be necessary with differing levels of rigor

depending on supplier/asset criticality. Establish high-level security requirements that apply to critical assets and corresponding supplier relationships, and customize them as necessary to individual supplier relationships or groups of similar supplier relationships.

There are numerous sources to come up with such requirements, both internally and externally. These include utility security policies and standards (e.g., NERC CIP), frameworks (e.g., NIST Cybersecurity Framework), and best practice documents (e.g., Energy Delivery Systems Cybersecurity Procurement Language).

These high-level security requirements will need to be tailored for each individual acquisition or existing supplier relationship. The benefit of starting with high-level security requirements is consistency of risk management across the organization and efficiencies resulting from saving time. When you have something to start from, coming up with a variant is generally a faster process.

6. Establish how you will want to share information with suppliers on vulnerabilities and incidents

Existing practices that help: **Legal, Public Relations, Incident Reporting and Response.**

NOTE: PR and Legal are outside IT, OT, Telecom, or security processes

Incidents happen in even the best-managed environments. Developing vulnerability-free code, for example, is impossible, so vulnerabilities will be discovered after installation in the acquirer's environment. When an event happens, how will the utility and supplier communicate with each other and with the outside world? Whose responsibility will it be to address the problem? How will the two parties continue after the problem is addressed? Discussion about common communication strategies and shared responsibilities in addressing incidents and vulnerabilities is critical. Both the utility and supplier will need to think about what they will do, including when and how to share information and how to collaborate in incident response, as well as in fixing the vulnerabilities or implementing compensating controls. Additionally, when bad things happen, it is extremely helpful to have a direct line to the person who can make a difference. Unfortunately, in the case of security incidents and vulnerabilities, the individual who acquires or sells the product may not be the individual charged with fixing it. Both acquirers and suppliers should designate points of contact for handling security-related issues to accelerate remediation and action.

7. Establish how you will want to monitor supplier adherence to requirements

Existing practices that help: Supply chain/sourcing/acquisition processes

NOTE: Supply chain/sourcing/acquisition processes are outside IT, OT, Telecom, or security processes

The work you have just completed to figure out what is important and to develop security requirements for that set of important assets and relationships will not be productive unless the results are monitored. However, this monitoring cannot be decided in a vacuum. While utilities may want to ask all kinds of questions and see all kinds of information, they need to be productive and efficient in their monitoring approaches. Utilities will need to figure out how they would like to monitor whether their suppliers are implementing security as defined, discuss those methods with suppliers, and negotiate a monitoring approach that makes sense for both organizations.

Utilities will need to balance the need for more rigorous testing against the cost to them and their suppliers of carrying out such testing—and against the expected risk associated with failing to do rigorous testing. On the less rigorous end of the scale, utilities can request that suppliers self-attest to implementing utility security requirements, having a secure development lifecycle, training developers on good coding practices, conducting appropriate testing, using secure packaging techniques, verifying origins of delivery, and continuing to deliver ICT products and services to the acquirer as those products and services were defined. A step up from self-attestation is acquirer site visits and acquirer tests of supplier's ICT products and services. Finally, the acquirer can request third-party testing or certification of the ICT products and services that the supplier provides.

The level of testing the acquirer chooses will depend, in part, on the quality of process control it finds already present in the supplier organization. For example, if the supplier can demonstrate it uses secure development lifecycle, it has gone a long way towards demonstrating its ability to continuously deliver on the acquirer's security requirements. Some of the ways to ascertain or demonstrate the existence of secure lifecycle include conducting security reviews throughout the lifecycle, training developers in secure coding practices, use of secure code repositories, knowledge of critical component origins by the supplier, fixing critical weaknesses during (rather than after) the lifecycle, and supplier awareness of industry best practices such as Open Web Application Security Project (OWASP) Top 10 vulnerabilities.

Please note that, many of the practices that may be the subject of monitoring may be proprietary for both acquirers and suppliers, and any consideration of sharing this information between the two parties should be done with great care. For example, the supplier may be very careful about

sharing the details of their secure lifecycle implementation with the acquirer. Special care should be taken requesting and storing any detailed information. For example, while an acquirer may be invited to review supplier procedures, the meeting may be held in the supplier's space with no note-taking allowed. As a rule, acquirers should not be asking for information that they may not be able to consume, act upon, or securely store.

Consider if the acquirer requests that a software supplier submit their detailed specifications or source code for inspection by the acquirer or their designated third party. These detailed specifications and source code are the intellectual property of the supplier and require strict protection. Suppliers are right to not trust acquirers with their source code in terms of appropriately protecting it from accidental release. Furthermore, having access to the source code is not required to ascertain that the supplier is following good practices. There are numerous alternative measures that will accomplish the same purpose.

8. Get the people within your organization up to speed

Existing practices that help: **HR and training, security training**

NOTE: HR and training are outside IT, OT, Telecom, or security processes

Lots of people touch products and services as they traverse an enterprise throughout the lifecycle of a supplier relationship. The roles of these people span the entire lifecycle of the acquired (or supplied) product and service and include acquisition/procurement, legal, information technology, supply chain, engineering, software and system development, delivery, shipping and receiving, human resources, information/cyber security, physical security, network operations, facilities, and potentially many others. All these people need to understand their role in managing security risks associated with supplier relationships. While each of these individuals may have a small piece of the overall puzzle, their collective behavior is critical for managing the risks. For example: Human Resources defines and implements background checks and training policies. Acquisition and procurement defines the process for soliciting and bringing in suppliers. Legal keeps organizations out of legal trouble. Engineering designs products. Shipping and receiving makes sure that boxes that contain critical components have not been tampered with enrooted or at the warehouse. Software developers ensure that the code is tested and fixed. The list goes on and on. Acquirers and suppliers need to train their personnel on how to address and mitigate the risks that are deemed critical.

Individuals and functions that have a key role in cyber supply chain risk management should receive tailored supply chain risk management training that helps them understand what they are being asked to do, and why they are being asked to do it. For general users, utilities can integrate cyber supply chain concerns into their security awareness training.

It should be noted that when acquirers establish supplier relationships, the individual and business unit responsible for the relationship may not be the unit responsible for security aspects of it. To avoid confusion during critical times, as when breaches happen, utilities can designate security points of contact for critical supplier relationships. That way if a supplier experiences a breach, this supplier can contact the right utility staff who can immediately initiate actions on behalf of the utility.

9. Make arrangements for contingencies

Existing practices that help: **Supply chain/sourcing/acquisition processes**

NOTE: Supply chain/sourcing/acquisition processes are outside IT, OT, Telecom, or security processes

The life of a system does not end when it goes into production. Generally, utilities keep their OT systems for a long time, a lot longer than IT systems. Suppliers who put those systems together may experience changes during the system's lifetime that will impact a utility who acquired that system. Suppliers may experience any of the following, resulting in security risks to utilities.

What May Happen to Supplier	Risk to Utility
Stop supporting operating systems or applications (e.g., Microsoft is no longer supporting Windows 95 operating systems)	Operating systems or applications are no longer patched and are therefore increasingly more vulnerable and obsolete.
Stop making the specific device, device component, or entire system.	When hardware and software is no longer supported or available, authorized resellers may still be able to provide those components. If that is not possible, utilities may have to go to the utility equivalent of a junk yard to find those spare parts and components. Purchasing hardware or software from anyone but an authorized reseller is risky because it is impossible to tell whether the hardware is as it was produced by the original manufacturer. Downloading software from unapproved third party sites risks introduction of malicious and unwanted code. This may mean that the replacement components are at higher risk of having unintentional flaws (which may impact performance) or intentional malicious functionality.
Go out of business	
Experience a drastic change in direction caused by change of management, acquisition, or another strategic imperative resulting in removal of support for software or hardware.	

Utilities need to plan for any of these eventualities when they are acquiring (especially) critical systems. The following list of considerations can help reduce the risks from such events to utility systems:

- Include provisions for hardware and software to be available in the future for maintenance and sustainment. Example provision: software escrow or buying parts ahead of time for future use
- Identifying approved resellers (for critical devices and components) that are likely to be in business as long as needed.

One very fruitful source of information about an organization is its equipment. Authorized disposers provide an important service that mitigates the risks of accidental data release through disposed computers that may still contain sensitive information. Utilities should consider using authorized disposers for their devices as much as possible.

10. Conclude supplier relationship in a risk-conscious way

Existing practices that help: **Supply chain/sourcing/acquisition processes**

NOTE: Supply chain/sourcing/acquisition processes are outside IT, OT, Telecom, or security processes

Supplier relationships sometimes end and utilities need to protect their operations, systems, and information in the process of terminating such relationships. The extent of what needs to be done depends on the same risk factors as assessing potential risks associated with supplier relationships:

1. Did supplier's people have access to your systems? Were your systems connected to supplier's systems?
2. Did suppliers' people have access to your facilities?
3. Did this relationship last for a long time?
4. How important/critical is the function/system/capability provided by supplier to you?

Especially when system and facility access are involved, utilities need to be very conscious of organizing supplier relationship termination processes that minimize security risks after the relationship is completed. Specifically, utilities should ensure that the ending of a relationship with a supplier that involves a transition between different suppliers or from a supplier to the utility involves an organized transition plan where the current supplier's responsibilities and activities are assumed by the receiving party. Specific activities that reduce security risks include

debriefing supplier staff, removing their access privileges immediately upon termination, and using reputable and approved component disposers (or returning used components to their original manufacturers).

PUTTING IT ALL TOGETHER

It is not easy to begin addressing utility cyber supply chain risk management challenges due to the diversity and number of suppliers, the numerous contracts in place, and the multidisciplinary nature of this challenge. While categorizing suppliers helps, this is not the only technique that helps organize and streamline supplier risk management activities. Every utility will have three categories of supplier relationships:

1. Existing supplier relationships that are expected to continue
2. Existing supplier relationships that are expected to conclude
3. New supplier relationships that are expected to be initiated

Each of these categories will also include suppliers of different criticality to a utility.

These categories are useful for organizing utility cyber supply chain risk management activities, because the level of control that a utility can exercise in addressing potential security risk differs for these three categories. Existing supplier relationships that are in progress and not coming up for renewal for some time are the most difficult to address immediately. Existing supplier relationships that are expected to conclude may not be worth the effort, although that would depend on how critical those suppliers and supported systems are. New supplier relationships that are expected to be initiated are the best candidate for utilities to make immediate impact and to try out their security requirements. To further focus the efforts, new supplier relationships that are critical for a utility are the best candidate for beginning this process.

As utilities work with their potential suppliers they can establish a productive dialog to discuss, negotiate, and tailor the baseline security requirements which the utility has developed (that are also applicable to the specific supplier relationship). Tailoring is important to ensure that the requirements genuinely fit the specific supplier relationship. Some of the baseline security requirements may remain unchanged, some may be revised, some may need to be dropped, and new requirements may need to be added. For those supplier relationships that are expected to conclude, it may be most efficient to mitigate security risks associated with these relationships by applying mitigating controls and waiting until those relationships conclude. Ongoing supplier relationships that are expected to continue are the most challenging to change. However, utilities can still initiate discussions with those suppliers to further its new security objectives:

1. Inform the supplier that the next contract renewal will involve a newly developed set of security requirements
2. Work with the supplier to determine what mitigating measures the utility and supplier can deploy between now and the next contract renewal
3. If the supplier is unwilling to engage in dialog explore other suppliers of similar solutions

This approach can be described as peeling the onion—where the most critical new supplier relationships are addressed first; then, in order of risk priority: less critical new supplier relationships, critical existing supplier relationships, less critical existing supplier relationships, and supplier relationships that are expected to conclude.

Another essential aspect of setting this new security process in place is gaining active support from all relevant participants in the process. Putting together the right set of cyber supply chain risk management activities will require participation of a variety of leaders and practitioners throughout the organization.

Engage players across your own utility to get the right perspectives early.

HOW TO PROGRESS

The 10 practices in this paper provide a good start for any utility to begin addressing their cyber supply chain risk management challenges in a methodical and organized way. These practices are squarely based on practitioner experience and grow directly out of several key standards and guidelines that have been developed over the past five years to address various aspects and perspectives of cyber supply chain risk management. But they only go so far. Beyond these foundational activities, it is strongly recommended that utilities and utility suppliers consult applicable standards and best practices to guide their cyber supply chain risk management programs. The table below lists such useful standards and best practices and summarizes how they can be used. Utilities can pick and choose their guiding source or sources from this table based on what they are trying to accomplish.

To Be Used For	Standards and Best Practices	Primary Audience
Establishing supply chain risk management implementation practices	ISO/IEC 27036—Information Security in Supplier Relationships	Acquirers and suppliers, including utilities
Source of supplier requirements language to tailor based on requirements, applicable risks, and other environmental factors	Energy Delivery Systems Cybersecurity Procurement Language Draft IEC 62443-2-4—Requirements for IACS Solution Suppliers	Energy systems acquirers ICS Acquirers
COTS products third party certification approaches	The Open Trusted Technology Provider™ Standard (O-TTPS)	Utilities
Examples of cyber supply chain controls	NIST SP 800-161—Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Federal agencies
Source of software Integrity practices	SAFECode Framework for Supply Chain Integrity SAFECode Overview of Software Integrity Controls	Organizations engaged in software development

1129 20th Street NW

Suite 350

Washington, DC 20036

(202) 872-0030

www.utc.org