

Assent

Real depth. Sustainable growth.™

eBook

Electronics

Navigating the Compliance Landscape

Table of Contents

Introduction 2

Chapter 01

Compliance & the Electronics Industry 3

Chapter 02

Product Compliance 5

The RoHS Directive 7

The REACH Regulation 9

Industry Challenges 11

Standardization & Product Compliance 12

Chapter 03

Corporate Social Responsibility 13

Conflict Minerals 15

Human Trafficking & Slavery 17

Chapter 04

Vendor Management 19

Tariffs & Trade Compliance 20

Country of Origin & Business Continuity 21

Information Security 22

ITAR Controls 23

Quality Assurance 24

Audits & Inspections 24

Chapter 05

Enforcement & Risk Mitigation 25

Enforcement 25

The Blueprint for Success 27



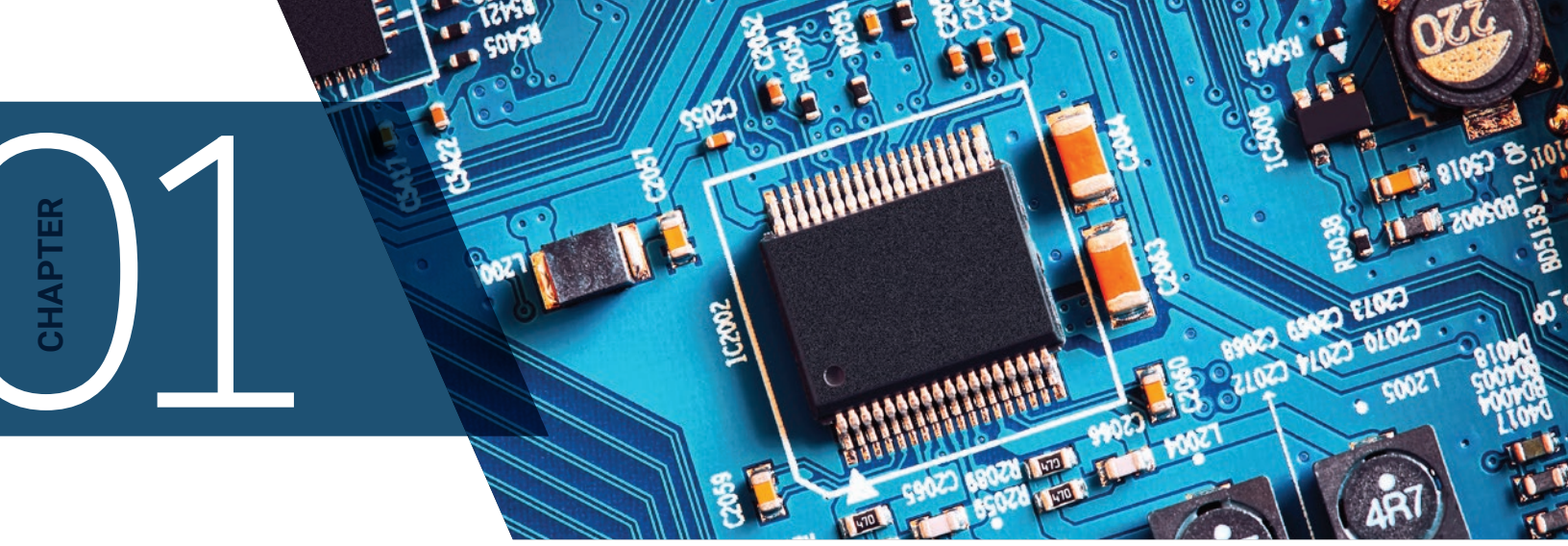
Introduction

Think back to the last time you exchanged pleasantries with a stranger. “Hello, how are you?” “Good, and you?” It’s essentially automatic. Now, would it be so automatic if the stranger spoke another language?

It’s not a matter of one form of communication being better than another — it’s about having a shared vocabulary. That’s what standardization is all about.

Electronics are incredibly complex, heavily regulated, and sold into almost every vertical. To manage compliance requirements, companies need to speak the same language. This eBook will examine the requirements the electronics industry faces and how standardization can help companies meet them. We’ll also dive into best practices manufacturers and suppliers can use to deep map their supply chains and produce safer, more sustainable products, meet customer and investor expectations, and ultimately mitigate risk.

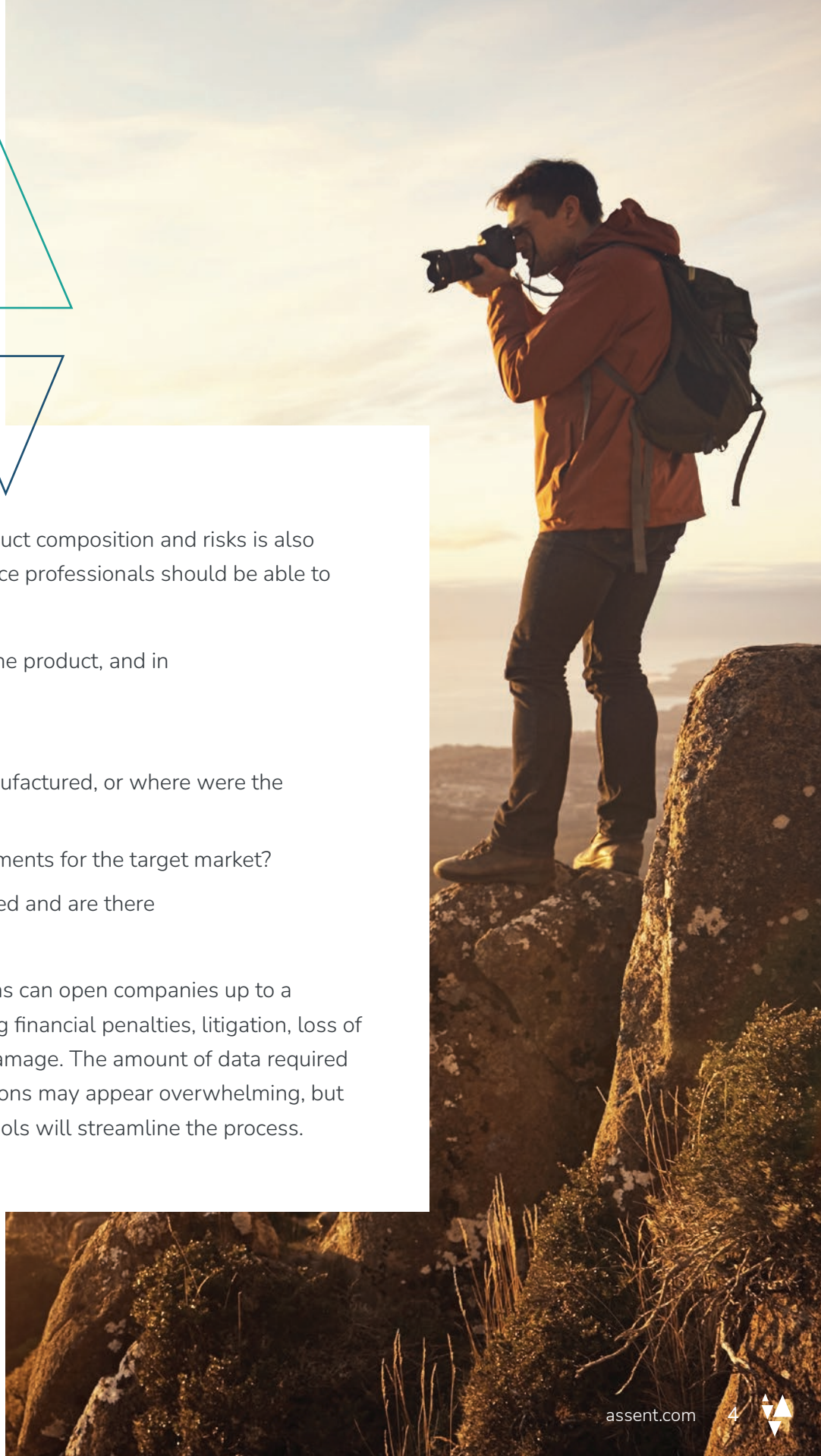
CHAPTER 01



Compliance & the Electronics Industry

Modern products are more digitally sophisticated than ever, and as products grow in complexity, so do regulatory requirements. As these regulations evolve, electronics manufacturers need to go back to their data again and again, searching for new substances of concern, supplier declarations, or country of origin information. When global supply chains span multiple continents that speak dozens of languages, there is greater risk of things getting lost in translation, potentially creating non-compliance penalties.

Scalable standardization and technology have proven to be the path to compliance success for electronics companies. For example, businesses that adopted tools such as IPC-1752A and IEC 62474 to address substance data required for product compliance regulations were better able to meet stringent requirements.



A complete understanding of product composition and risks is also essential to compliance. Compliance professionals should be able to answer the following:

- What substances make up the product, and in what concentrations?
- Who made the product?
- Where was the product manufactured, or where were the raw materials extracted?
- What are the access requirements for the target market?
- How is the product being used and are there potential exemptions?

Ignoring any one of these questions can open companies up to a significant amount of risk, including financial penalties, litigation, loss of market access, and reputational damage. The amount of data required to comply with applicable regulations may appear overwhelming, but having the right knowledge and tools will streamline the process.

CHAPTER 02



Product Compliance

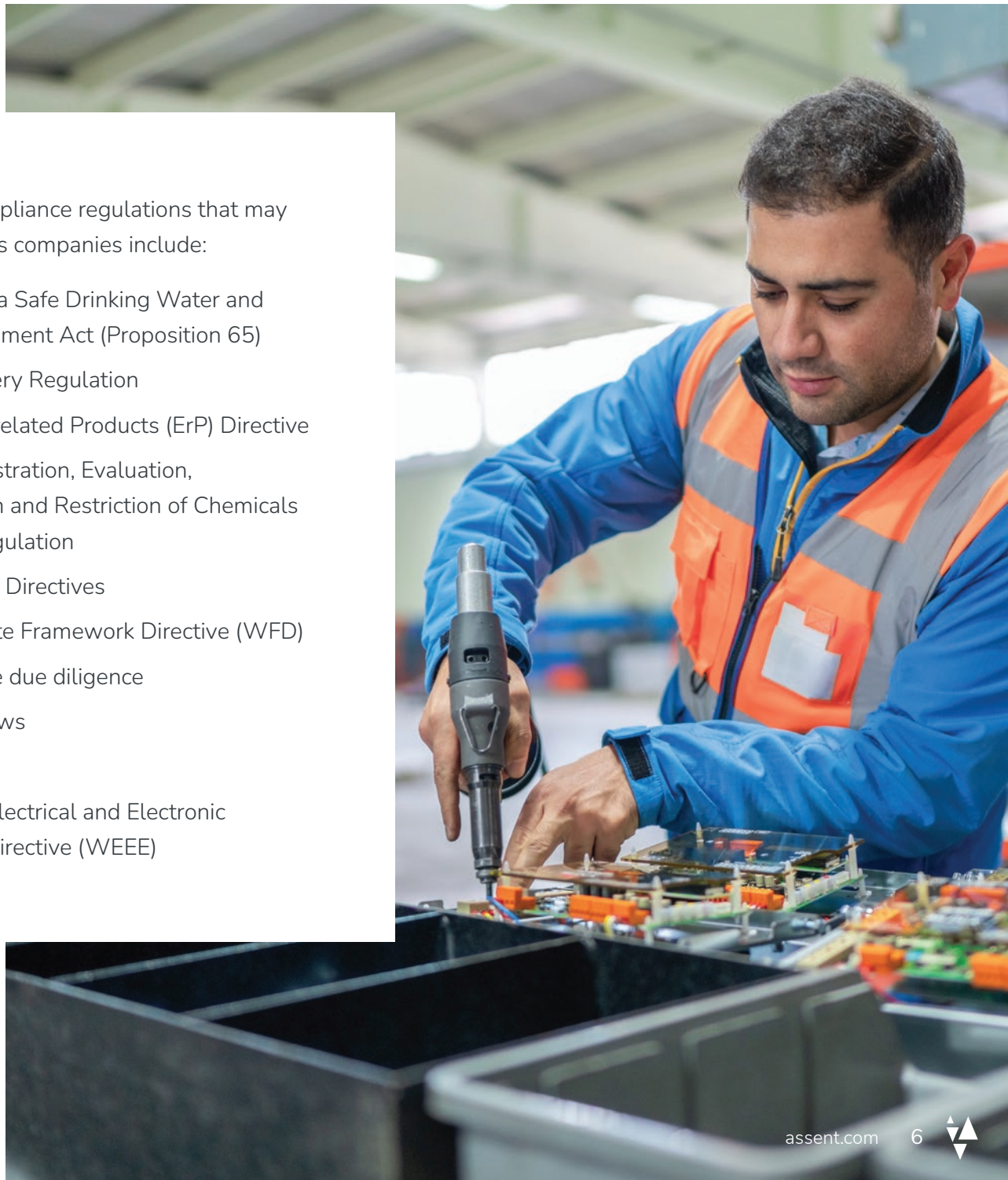
Today, even simple devices may need integrated circuits, microprocessors, power supplies, or display screens to function. The unprecedented demand for electrical and electronic equipment (EEE) components has been lucrative for companies, but creates an ever-expanding regulatory scope that compliance professionals must manage.

For example, if a product containing EEE components is sold into the EU, it is in scope of the EU Restriction of Hazardous Substances (RoHS) Directive. If sold in California, the same part would have different requirements under the Toxic Substances Control Act (TSCA).

For these reasons, companies that wish to sell globally into a range of industries must be prepared to provide compliance data for numerous regulations, and be equipped to respond to the information requests their customers will make.

Major product compliance regulations that may apply to electronics companies include:

- The California Safe Drinking Water and Toxic Enforcement Act (Proposition 65)
- The EU Battery Regulation
- The Energy-related Products (ErP) Directive
- The EU Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation
- Global RoHS Directives
- The EU Waste Framework Directive (WFD)
- Halogen-free due diligence
- Packaging laws
- TSCA
- The Waste Electrical and Electronic Equipment Directive (WEEE)



The RoHS Directive

The EU RoHS Directive came into effect in July 2006 and transformed the way electronics companies managed compliance. Many companies selling or manufacturing EEE in Europe were suddenly subject to restrictions on six chemicals at the homogeneous level:

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent chromium (Cr6+)
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ether (PBDE)



With four more being added years later on July 22, 2019.

- Bis(2-ethylhexyl) phthalate (DEHP)
- Benzyl butyl phthalate (BBP)
- Dibutyl phthalate (DBP)
- Diisobutyl phthalate (DIBP)

With these additional substance restrictions in effect, electronics companies that use these phthalates have had to reevaluate the materials they use when making products. For example, wire sheathing, wire harnesses, and power cords often use a flexible vinyl that may contain DEHP.

Non-compliance could result in reputational damage, loss of market access, recall of goods, loss of revenues, and/or fines.



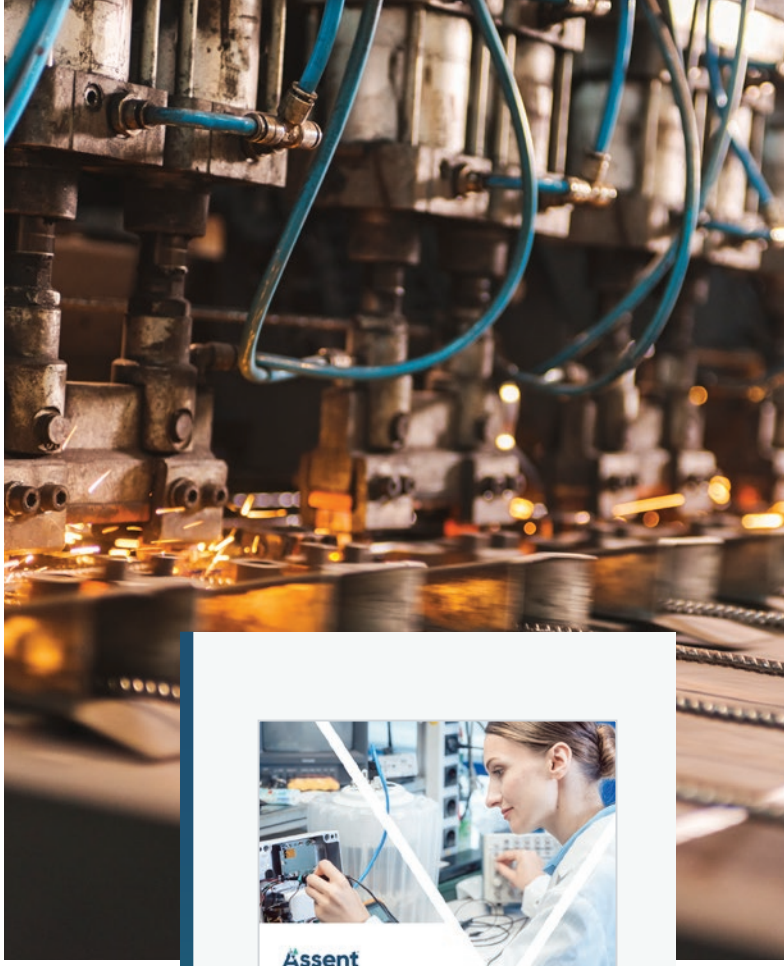
RoHS Exemptions

Exemptions are granted in situations where it is technically impossible to remove a substance from a product, or where manufacturers require time to find an alternative substance. Exemptions are typically granted for finite periods of time, so companies should closely monitor potential expiry dates.

RoHS Around the World

A part or product may be in scope of different regulations, depending on its final destination. Countries with RoHS-like legislation include Japan (2006), China (2007), Korea (2008), Taiwan (2012), and the United Arab Emirates (2017).[1] While these pieces of legislation have many similarities, there are subtle differences to consider when selling into the global market. Generally, customs agents will be the first to check for RoHS compliance of imported goods, and will use the specific guidelines provided by the destination country.

Global RoHS directives are most likely to differ from EU RoHS with regard to exemptions. Many of the global RoHS directives do not have expiration dates for exemptions, meaning expired EU exemptions may still be active in other parts of the world. Additionally, they may use unique numbering systems that do not align with the commonly-used RoHS numbering system.



To learn more about your obligations under the RoHS Directive, download our eBook, ***The RoHS Handbook: Your Guide to Compliance.***

Download eBook

1 National Institute of Standards and Technology. (2021, February). *Compliance FAQs: RoHS.* https://www.nist.gov/standardsgov/compliance-faqs-rohs



The REACH Regulation

The REACH Regulation safeguards human health and the environment from harmful substances. It places a host of requirements on companies manufacturing or importing into the European Economic Area (EEA), including communication obligations for substances of very high concern (SVHCs) and the outright restriction of certain substances.

Since the REACH Regulation came into effect, new SVHCs have been added to the Candidate List of SVHCs on a twice-annual basis. Suppliers of any article containing SVHCs above the threshold concentration of 0.1 percent weight over weight (w/w) must provide the recipient or consumer with safety information.

After SVHCs are added to the Candidate List, they may then be put on the Authorisation List, also known as Annex XIV. Substances are added to the Authorisation List based on priority, as determined by the ECHA.[2] Once a substance is included on this list, it may only be placed on the EU market or used after its sunset date (typically 18 months later) if a manufacturer, importer, or downstream user is granted an authorization for a specific use.

There are now over 200 substances restricted under the REACH Regulation. While the RoHS Directive specifically governs electronic devices and their subcomponents, the REACH Regulation has a much broader scope. This may bring products such as packaging and some accessories into scope for electronics companies.

2 European Chemicals Agency. (n.d.). *Authorisation List*. https://echa.europa.eu/authorisation-list

Companies whose products are non-compliant can face disruptive penalties, including:

- Loss of access to EU markets
- Financial penalties
- Implementation of new auditing procedures dictated by enforcement authorities
- Criminal prosecution in cases where the safety of workers is at risk

The EU Waste Framework Directive

Companies that introduce products or articles that contain SVHCs over the 0.1 percent w/w threshold to the EEA now face additional obligations that go beyond the scope of REACH reporting. As of January 5, 2021, the EU WFD created additional data requirements for submissions to the Substances of Concern In articles, as such or in complex objects (Products) (SCIP) database that include:

- The article category
- Information on linked articles
- Substance concentration levels
- The material or mixture category



To learn more about your obligations under the REACH Regulation, download our eBook, ***The REACH Handbook: Your Guide to SVHC Compliance.***

Download eBook

Industry Challenges

In addition to identifying the regulations they are in scope of and collecting supplier data, companies may also be required to provide testing documentation to prove their products are compliant.

REACH & RoHS Overlap

While the RoHS Directive was written specifically for the electronics industry, the REACH Regulation impacts a wide range of industries. This has led to some overlap between the two, though they are intended to be complementary. When a substance that is already covered under the RoHS Directive is added to the REACH Candidate List, enforcement authorities make an effort to ensure there is no conflict between requirements, that controls are consistent and that one regulation is not more restrictive than the other.

In a paper published by the European Commission, EEE manufacturers are instructed that "as far as possible, RoHS should be given priority to regulate issues pertaining to the use of substances in EEE."[3]

Electronics companies will find certain products, such as some accessories and packaging, are out of scope of the RoHS Directive, but must be considered under the REACH Regulation.

Product Testing

In some cases, declaring compliance is not enough. Suppliers may be asked by their customers to prove their declarations for REACH and RoHS are accurate and provide supporting documentation, such as analytical testing reports.

Companies manufacturing EEE have quickly learned the meaning of "no data, no market." The European Commission uses this phrase in relation to REACH compliance to place responsibility on industries to manage risk from chemicals, and on manufacturers and importers to gather information on an ongoing basis.[4]

As restrictions increase, companies have implemented more rigorous processes for data collection and testing. Paperwork may be evaluated at the border to ensure imported products meet compliance requirements. Companies that cannot demonstrate compliance may find their products held in customs or turned away altogether. Compliance testing for the REACH Regulation and RoHS Directive can be layered on top of echnical files to show due diligence beyond what is legally required.

3 European Commission, Enterprise and Industry Directorate-General. (n.d.). *REACH and Directive 2011/65/EU (RoHS): A Common Understanding.* http://ec.europa.eu/DocsRoom/documents/5804/attachments/1/translations/en/renditions/native

4 European Commission. (2016, August 24). *REACH.* http://ec.europa.eu/environment/chemicals/reach/reach_en.htm



"Testing should be engaged when you have a debatable part in your product, such as wire harnessing that you're sourcing from China, and you're just not sure it's RoHS-compliant. After you've built up your technical file to show conformance, do the testing and layer it on top to show additional due diligence."

— **Bruce Jarnot, Senior Manager, Product Compliance, Assent, and a board-certified toxicologist**

Standardization & Product Compliance

In response to the challenges of data collection, the industry has developed a number of standards and templates that can help companies streamline the reporting process.

Full Material Disclosures

Many companies now request full material disclosures (FMDs), which provide a breakdown of all the substances in a product by weight and/or concentration. Collecting FMDs is a proactive approach, while traditional material declarations are considered a reactive approach.



In our eBook, *Full Material Disclosures: Building Resilience With Data*, we explain how to absorb FMD collection into your compliance programs and what will need to be done to make it most effective. Download your copy to get started!

Download eBook

CHAPTER 03



Corporate Social Responsibility

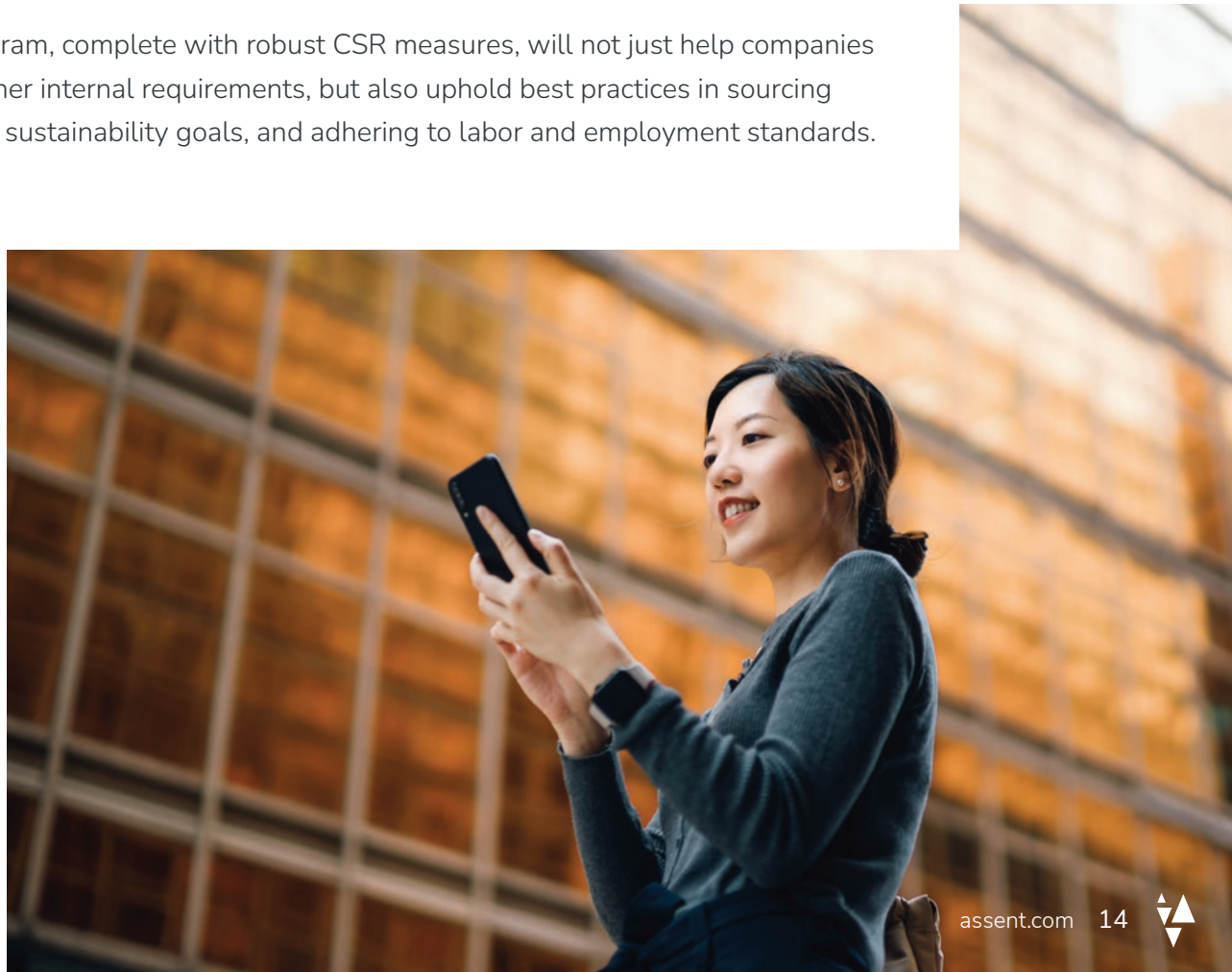
As the global demand for electronic products grows, so too does public scrutiny of the companies that make those devices. Many investors have stated that they expect the companies they invest in to engage in ethical business practices[5] and produce more detailed environmental, social, and governance (ESG) disclosures. Meanwhile, consumers increasingly want to buy from companies that demonstrate they are socially and environmentally conscious.

5 Vittorio, A. (2017, February 22). *Investors With $3.75 Trillion Defend Conflict Minerals Rule.* https://www.bna.com/investors-375-trillion-n57982084183/

Governments around the world have also developed legislation in an effort to address human rights abuses that occur in global supply chains. Major CSR regulations that may apply to companies in the electronics industry include the:

- Australia Modern Slavery Act
- California Transparency in Supply Chains Act
- Countering America's Adversaries Through Sanctions Act (CAATSA)
- EU Conflict Minerals Regulation
- EU Non-Financial Reporting Directive
- French Duty of Care
- German Supply Chain Act (GSCA)
- Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act
- UK Modern Slavery Act
- U.S. Federal Acquisition Regulation
- U.S. Trade Facilitation and Trade Enforcement Act

A strong ESG program, complete with robust CSR measures, will not just help companies meet these and other internal requirements, but also uphold best practices in sourcing materials, meeting sustainability goals, and adhering to labor and employment standards.

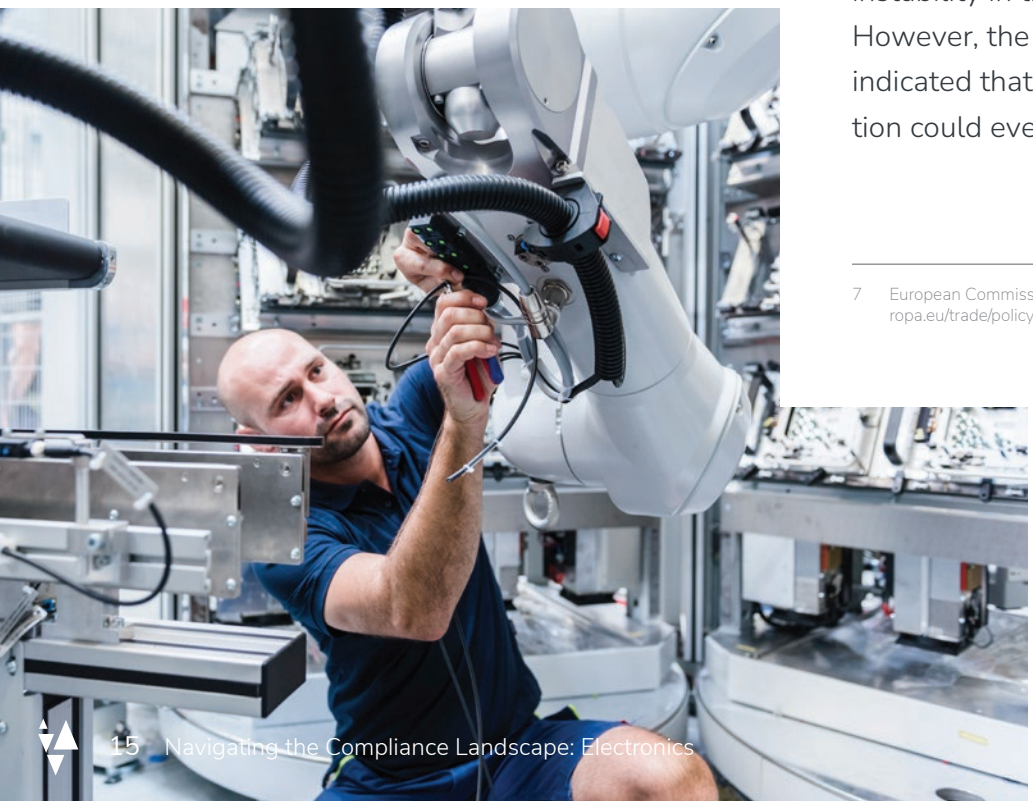


Conflict Minerals

Electronic devices and components may contain metals that are mined in conflict-affected regions, where their sale can contribute to armed violence, instability, and human rights violations. These are known as conflict minerals. They are commonly defined as tin, tungsten, tantalum, and gold (3TGs) mined in the Democratic Republic of the Congo (DRC) and its adjoining countries. The EU Conflict Minerals Regulation maintains a list of conflict-affect and high-risk areas (CAHRAs).[6]

To reduce the flow of funds to the groups that control and profit from the conflict minerals trade, both U.S. and EU regulations have established minimum requirements for the responsible sourcing of minerals.

6 European Commission. (n.d.). *What Are CAHRAs?* https://ec.europa.eu/growth/system/files/2021-09/2._what_are_cahras.pdf



The Dodd-Frank Wall Street Reform & Consumer Protection Act

Under Section 1502 of the Dodd-Frank Act, in-scope companies must track the source(s) of their minerals and submit a report to the U.S. Securities and Exchange Commission (SEC) annually. This process involves performing a Reasonable Country of Origin Inquiry (RCOI) to determine whether the minerals used originated from the DRC or its adjoining countries, and whether they were sourced in an ethical manner.

EU Conflict Minerals Regulation

The regulation requires EU importers of 3TGs to conduct due diligence to ensure their supply chains are not contributing to armed conflict and instability in the DRC and its adjoining countries.[7] However, the European Commission has also indicated that the geographic scope of the regulation could eventually extend beyond the DRC.

7 European Commission. (2017, December 13). *The regulation explained.* http://ec.europa.eu/trade/policy/in-focus/conflict-minerals-regulation/regulation-explained/

Smelters & Refiners

At some point during the production process, manufacturers must purchase metals from a smelter or refiner (SOR). These are companies that purchase raw materials from mines, recyclers, and scrap suppliers, and melt them down into metals that can be used in the production of electronic components. Smelters are considered the "pinch point" in the conflict minerals supply chain, and they are key to identifying mineral sources of origin, and thus meeting due diligence expectations. Once raw ores have been smelted, it becomes nearly impossible to determine where they came from.

Companies that understand which types of metals are used in specific parts and components will be better able to identify sources, and potentially consider a smaller range of SORs when identifying sources of minerals used in specific electronic components.

Smelters can be narrowed down even further for specific electronic parts. For example, the solder for components such as microprocessors, chip sets, and solid state drives requires specially-produced, super low alpha tin, which significantly limits the potential sources for tin in those products.

Smelter & Refiner Due Diligence

Industry best practice for responsible sourcing is to follow the Organisation for Economic Co-operation and Development (OECD) Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas,[8] and leverage tools such as the Responsible Minerals Initiative RMI)'s Conflict Minerals Reporting Template (CMRT).[9] The EU Conflict Minerals Regulation states that due diligence must be in line with the OECD's five-step framework, which is as follows:

- Establish strong company management systems
- Identify and assess risk in the supply chain
- Design and implement a strategy to respond to identified risks
- Carry out an independent third-party audit of supply chain due diligence at identified points in the supply chain
- Report on supply chain due diligence[10]

8 OECD. (n.d.). *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas*. http://www.oecd.org/corporate/mne/mining.htm

9 Responsible Minerals Initiative. (n.d.). *Conflict Minerals Reporting Template*. http://www.responsiblemineralsinitiative.org/conflict-minerals-reporting-template/

10 OECD. (n.d.). *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas*. http://www.oecd.org/corporate/mne/mining.htm

Responsible Sourcing: Beyond Conflict Minerals

Increasing global reliance on electronic devices has resulted in a significant, growing demand for the raw materials needed to make them. One such mineral is cobalt, which is required for the lithium-ion batteries found in smartphones.

While reporting on cobalt is not legally required by existing conflict mineral laws, consumer and industry-driven efforts have encouraged companies to audit for cobalt — among other materials — to mitigate the risk of human rights violations. Electronics companies may choose to complete a materiality assessment to identify whether cobalt, or any other at-risk materials, are used in their products.

Human Trafficking & Slavery

Human trafficking and slavery touch many industries in many countries around the world, particularly in Asia.[11] Governments have passed laws such as the UK Modern Slavery Act, which places the responsibility of mitigating this risk onto companies. The act requires companies with an annual turnover of more than 36 million GBP and operations in the UK to provide a statement outlining the steps they have taken during the financial year to ensure slavery and human trafficking are not taking place in their operations and supply chains.

> *"New research suggests that forced labor often enters the labor supply chain through subcontracted agencies. It's crucial that you monitor this supply chain alongside your procurement supply chain to sufficiently protect your company against slavery and human trafficking. When it comes to auditing your labor supply chain, do not try to create a parallel auditing process. Instead, embed it into your existing systems."*
>
> — **Sarah Carpenter, Manager, Business & Human Rights, Assent**



11 Responsible Business Alliance. (n.d.) *Trafficked & Forced Labor.* http://www.responsiblebusiness.org/initiatives/trafficked-and-forced-labor/

U.S. Sanctions on Forced Labor

Some types of forced labor in the supply chain can carry significant penalties for companies that do not conduct the appropriate due diligence. Under the Countering America's Adversaries Through Sanctions Act (CAATSA), which became U.S. law in 2017, companies are required to operate based on the presumption that all North Korean labor is forced labor.[12]

As electronics companies have long and complex supply chains, with a significant amount of raw material sourcing involved, it can be particularly difficult to ensure products are free from North Korean forced labor. This includes labor that occurs in North Korea and forced labor of North Koreans abroad. North Korean laborers are often trafficked to other countries to generate revenue for the state, with wages paid directly to the North Korean government, which may fund weapons of mass destruction and ballistic missile programs.

Forced labor out of the Xinjiang province in China is also a concern for companies. The U.S. has issued a record number of withhold release orders (WROs) under the Tariff Act of 1930. The act prohibits the importation of any product believed to be manufacturers, wholly or in part, by forced labor. Companies with held products must produce significant due diligence to have their goods released.[13]

Mitigating the Risk of Human Trafficking & Slavery

According to a May 2018 KnowTheChain report, the largest global electronics companies are often leaders in prohibiting forced labor across the supply chain.[14]

On average, the electronics companies that are most diligent at mitigating human trafficking and slavery in their supply chains are likely to have in place:[15]

- A supplier code of conduct that incorporates international standards against forced labor
- A flow-down process for the supplier code of conduct throughout the supply chain
- An employee training program on forced labor
- A supplier policy against worker-paid recruitment fees
- An audit process to assess forced labor in the supply chain



12 United States Department of the Treasury. (2018, July 23). *North Korea Sanctions & Enforcement Actions Advisory.* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf

13 U.S. Customs and Border Protection. (n.d.). *Withhold Release Orders and Findings List.* https://www.cbp.gov/trade/forced-labor/withhold-release-orders-and-findings?_ga=2.223059163.1771931437.1640204455-542056593.1640204455

14 KnowTheChain. (2018, May). *2018 Information and Communications Technology Benchmark Findings.* https://knowthechain.org/wp-content/plugins/ktc-benchmark/app/public/images/benchmark_reports/KTC-ICT-May2018-Final.pdf

15 KnowTheChain. (2018, May). *2018 Information and Communications Technology Benchmark Findings.* https://knowthechain.org/wp-content/plugins/ktc-benchmark/app/public/images/benchmark_reports/KTC-ICT-May2018-Final.pdf

CHAPTER 04



Vendor Management

The nature of the electronics supply chain — with its sheer volume of parts and components, and reliance on a multitude of global suppliers — leaves electronics companies open to significant risk of disruption. With proper supply chain vendor management, however, companies can minimize this risk, as well as cost surges and reputational damage.

Tariffs & Trade Compliance

Many companies in the electronics industry rely on critical vendors that are often based in countries at risk for tariff impacts, such as China. This makes it critical for EEE companies that import products to accurately track country of origin and Harmonized Commodity Description and Coding System (HS) codes (known as Harmonized Tariff Schedule, or HTS codes in the U.S.) in order to accurately calculate tariffs.

Failure to properly track country of origin and HS codes can lead to paying unnecessary tariffs, or significant fines and penalties for underpayment. In the electronics industry, the country of origin is frequently misreported as the country where a product component ships from, resulting in inaccurate tariff calculations and/or violations of the law.

Tracking the correct country of origin is also critical to avoiding audits by U.S. Customs and Border Protection, a part of the Department of Homeland Security, product seizure, or fraud charges. To manage this, some companies choose to establish a dedicated trade compliance business function that consists of an internal staff member or a trade compliance team.

Four questions to ask yourself about vendor risk:

1. *Does my company distribute a code of conduct through the supply chain, including manufacturing factories?*

2. *If tariffs were to impact imported products from China, how much would our profit margins be affected?*

3. *Who conducts our factory audits, and what training have they undertaken?*

4. *If a natural disaster occurred, do I have a cluster of suppliers or manufacturers that would all be affected? What would the impact be on my company?*

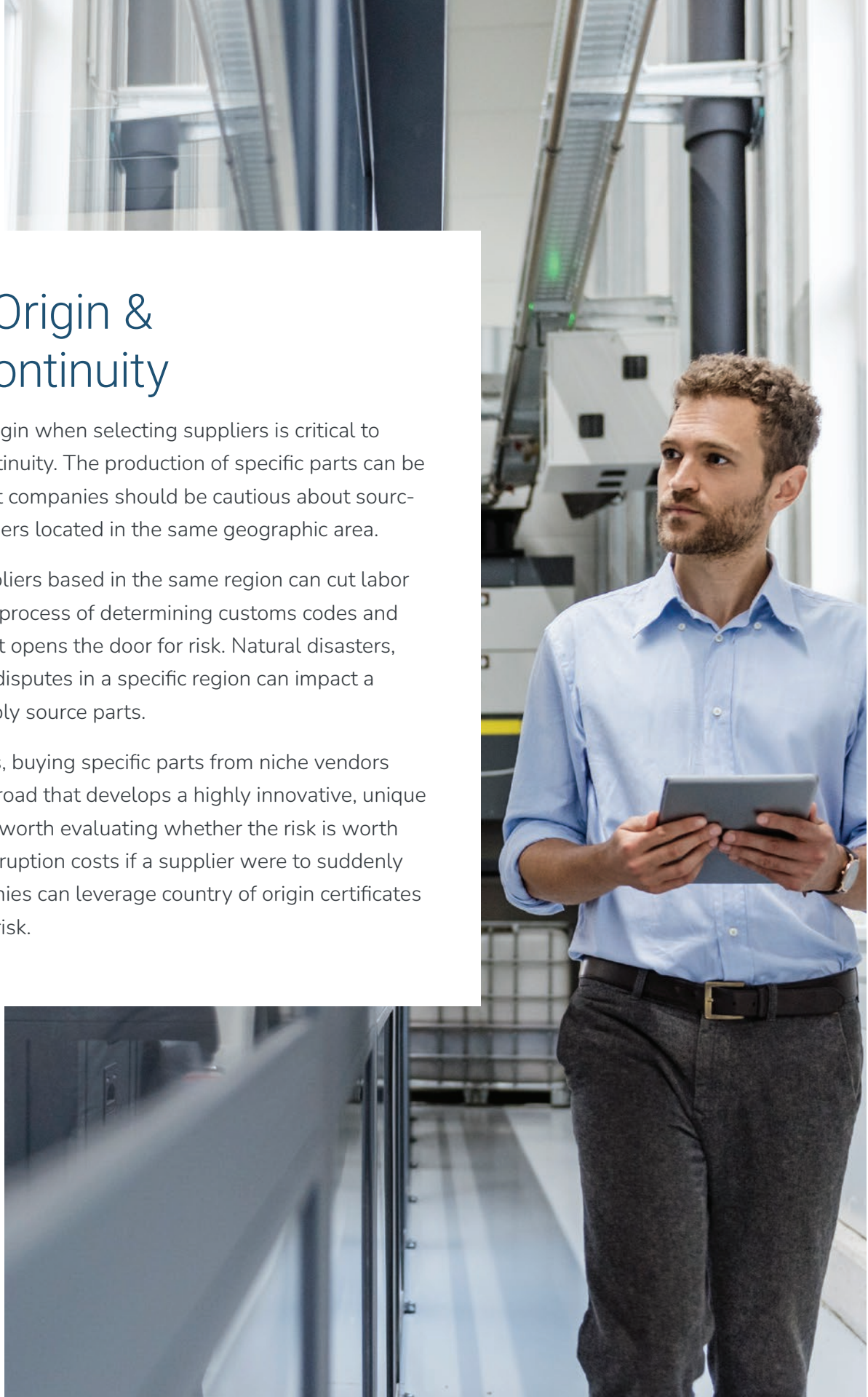
— Travis Miller, General Counsel, Assent

Country of Origin & Business Continuity

Considering country of origin when selecting suppliers is critical to maintaining business continuity. The production of specific parts can be extremely specialized, but companies should be cautious about sourcing from a group of suppliers located in the same geographic area.

While sourcing from suppliers based in the same region can cut labor costs, and streamline the process of determining customs codes and the import tariff process, it opens the door for risk. Natural disasters, political turmoil, or labor disputes in a specific region can impact a company's ability to reliably source parts.

For electronics companies, buying specific parts from niche vendors (e.g., a small company abroad that develops a highly innovative, unique part) carries this risk. It is worth evaluating whether the risk is worth the potential business disruption costs if a supplier were to suddenly cease operations. Companies can leverage country of origin certificates to determine the level of risk.



Information Security

With the number of suppliers and manufacturers involved in the production of a single part or component, companies in the electronics industry must exchange a significant volume of data, which carries a variety of risks for all involved. Full material disclosures, product designs, and specifications contain sensitive and proprietary data. To protect the customers and suppliers they do business with, companies must ensure the data they handle remains confidential.

An example of this is SOC 2 compliance, which requires companies to ensure the security, privacy, availability, confidentiality, and integrity of their customers' data. Companies can gain SOC 2 certification through a technical audit.

Another example is the ISO 27001 standard for information security management, which sets out requirements for establishing and maintaining an information security management system that preserves data confidentiality. It is a widely-accepted security standard, and many customers and suppliers will expect the companies they work with to have it in place.[16]

NIST Standards

To qualify for U.S. government procurement contracts, companies are required to comply with National Institute of Standards and Technology (NIST) standards to protect controlled unclassified information. Companies in scope of the Defense Federal Acquisition Regulation Supplement (DFARS) that do business with the U.S. Department of Defense (DOD) must comply with the NIST SP 800-171 Security Requirements standard.[17] The standard has more than 100 requirements that govern how sensitive information is stored, accessed, and exchanged.[18] Electronics companies may come in scope through the flow-down requirements of their customers that contract with the U.S. government.

Companies must be prepared to respond to inquiries regarding data and information security, particularly when dealing with proprietary data, or supplying to companies that bid on federal procurement contracts or sell to the U.S. government.

16 International Organization for Standardization. (n.d.). *ISO/IEC 27000 family - Information security management systems.* https://www.iso.org/isoiec-27001-information-security.html

17 NIST. (n.d.). *DFARS Cybersecurity Requirements.* https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance

18 Bovee, I. (2018, May 4). *7 Steps for getting it right with NIST 800-171.* FCW. https://fcw.com/articles/2018/05/04/comment-800-171-compliance.aspx

ITAR Controls

Many electronics companies are in scope of the International Traffic in Arms Regulations (ITAR), which control the export of technical data from the U.S. For example, the U.S. government contributed significant funds to the development of semiconductor technology, resulting in legacy designs that fall under ITAR.[19] Many companies also have some products or subcomponents that are controlled by the Export Administration Regulation (EAR) Commerce Control List (CCL), potentially due to cryptology or another special classification.

Gathering HTS codes and Export Control Classification Numbers (ECCNs) is necessary to determine whether information exchanged about these parts is controlled under ITAR or CCL. Harmonized Tariff Schedule code and ECCN information can help companies ensure that controlled technical data is properly managed, and that the appropriate licenses are acquired if third-party vendors are engaged to house information or support the manufacture of products featuring controlled technology.



HTS Codes

The U.S. HTS codes implement the World Customs Organization's HS codes in the U.S. All shipments imported and exported require a customs code.

19 Defense Advanced Research Projects Agency. (n.d.). *Where the Future Becomes Now.* https://www.darpa.mil/about-us/darpa-history-and-timeline?ppl=viewall

Quality Assurance

To ensure quality across globalized manufacturing processes and to reduce the occurrence of defective products, many companies leverage quality control standards, audits, and quarterly performance reviews to ensure parts and components are made to an equal standard.

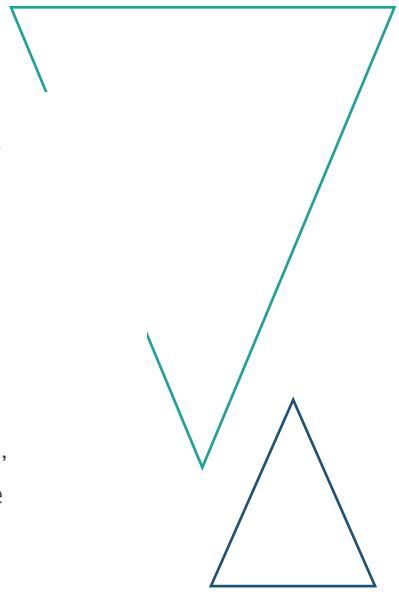
The growing prevalence of electronics being installed into vehicles, for example, has resulted in the electronics industry adopting automotive quality standards, which are robust and challenging to meet. Because electronics inside vehicles must function when installed beside parts such as motors, rigid quality assurance must show they can withstand engine heat, extreme weather fluctuations, and vibrations.

To maintain market access, most electronics companies have gravitated toward the automotive standard ISO/TS 16949 over the last decade. Gaining ISO/TS 16949 certification involves an audit process that reviews the design, development, production, and installation of electronic parts and devices against the requirements of the quality standards. [20]

Audits & Inspections

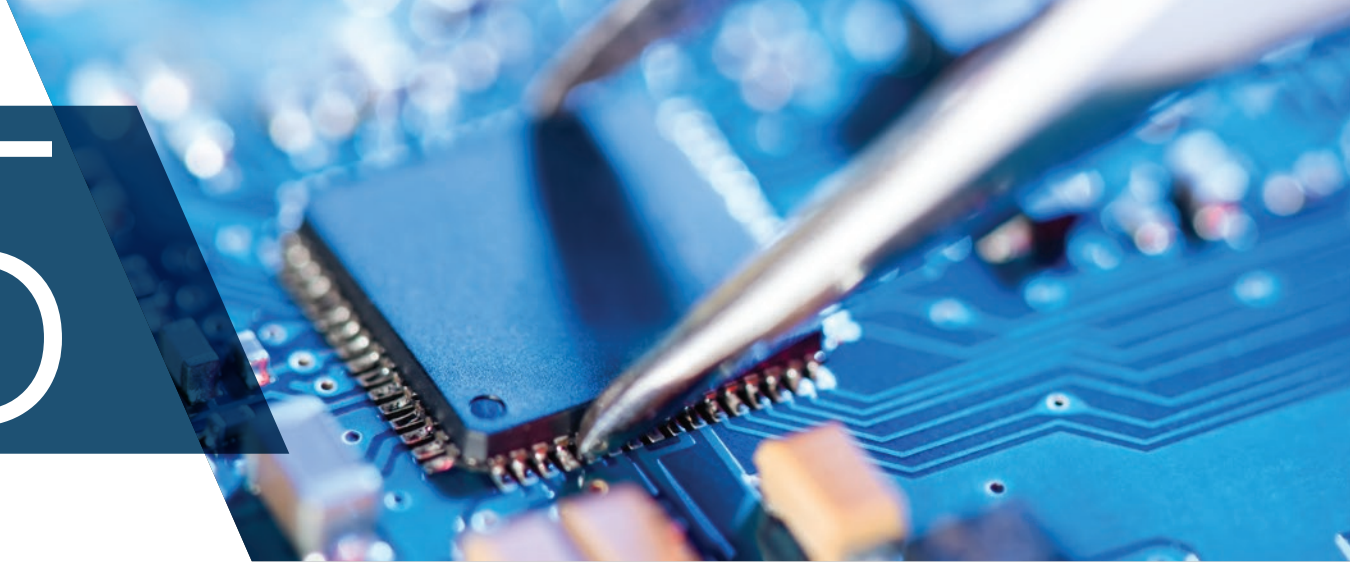
Working with vendors carries risk, which is why companies use regular audits and inspections to ensure their suppliers are complying with the policies and standards stipulated in their business contracts and other flow-down requirements. It is common practice for a director of quality control or supply chain to make an on-site visit to supplier factories.

Companies that send a member of their compliance team to conduct a supplier audit often encounter gaps in their evaluations. For this reason, companies are recommended to use a tool or product that can facilitate a step-by-step inspection, and reduce the risk of missing key questions or data sets for in-scope regulations during an on-site assessment.



20 APB Consultant. (n.d.). *Internal Quality Management System Audit Checklist (ISO9001:2015).* http://isoconsultantpune.com/wp-content/uploads/2016/02/audit-iso9001-2015-checklist-.pdf

CHAPTER 05



Enforcement & Risk Mitigation

Enforcement

Even momentary loss of market access can have significant ramifications for companies. In one instance, three weeks before Christmas, $160 million USD in gaming systems were impounded by Dutch customs officers because of excess cadmium levels found in cables.[21] Products were seized, prime Christmas-season sales were lost and Sony was forced to quickly manufacture reformulated cables to regain market access.

As this story illustrates, regulatory enforcement can take many forms — and the penalties can be labor-intensive and costly.

Loss of Market Access

Loss of market access can heavily impact a business, with diminished revenues or a hold on products at customs eating into profits. In order to regain market access, companies could be required to complete a product redesign to eliminate the offending substance from the product in question.

In the electronics industry, product redesigns are often complicated and expensive. A redesign of a small piece with complex engineering may require a significant amount of labor, or the vetting of new suppliers.

21 Smith, F. (2011, December 5). *Dutch officials seize cadmium-packed PlayStation kit. The Register.* https://www.theregister.co.uk/2001/12/05/dutch_officials_seize_cadmiumpacked_playstation/

When violations occur, the OEM suffers the majority of the impact. However, if the violation is due to the lack of a declaration or a false declaration from a company, the OEM has the ability to pursue legal action and monetary compensation from the supplier in question. The OEM may also choose to sever ties with the supplier.

Fines & Audits

With respect to trade and tariffs, fines for mis-declared items can be costly. Due to the complex nature of electronics, and the different classifications for subcomponents within a product, companies may struggle to properly classify all products and ensure all controlled technology (such as under ITAR or CCL) is properly managed.

In such cases, companies may even face audits by U.S. Customs and Border Protection international agents. A customs audit can include a multiple-day review of all records, and may lead to significant repercussions if violations are discovered — including personal criminal liability.

22 Wakefield, J. (2016, January 19). *Apple, Samsung and Sony face child labour claims.* BBC Technology. https://www.bbc.com/news/technology-35311456

Reputational Risk

In recent years, major OEMs have made headlines after an Amnesty International report discovered child labor was being used to mine cobalt for products such as smartphones.[22] When forced labor or child labor is discovered in the supply chains of companies, the reputational damage is often irreparable.

In turn, reputational damages can have a financial impact. An increasing number of investors are choosing to support companies that have strong CSR programs. In ethical investing — which can include socially responsible investing (SRI) and investing based on environmental, social and governance (ESG) criteria — investors consider a range of CSR factors before making investment decisions.



The Blueprint for Success

There is no single key to building an effective compliance program. The strongest programs are backed by knowledge of all regulations a product may be in scope of, and have a full view into the entire supply chain. These programs often have executive buy-in and are supported by the resources necessary to maintain them.

Successful companies leave little to chance and proactively mitigate a range of risks at all levels of their supply chains, ensuring they deliver profitable, safe products to consumers.

Risk Mitigation Best Practices

The following best practices can guide companies in mitigating the risks of non-compliance:

1. **Know your regulations.**

   Have a complete view into all of a product's use cases, and regulations of which it may be in scope.

2. **Deep-map your product.**

   Make sure you have as much information about your product as possible, by going down to the base suppliers of even the smallest components. By leveraging FMDs, companies can easily search for specific substances and more efficiently manage regulatory shifts.

3. **Expert access.**

   Have regulatory subject matter experts either in-house or available as consultants to support best practices.

4. **Gain executive buy-in.**

   Success often comes from the top down, and compliance starts with a culture that encourages it.

5. **Leverage technology.**

   There are a wide range of standards, tools, and solutions that can be used to collect and manage data.

6. **Supplier access.**

   Ensure your suppliers can communicate with you easily — ideally in their preferred language.

7. **Centralize data.**

   Consolidate data into a central location, avoiding the use of multiple spreadsheets or disparate data sets.

8. **Standardize information.**

   Present data in similar formats so reports can be easily generated.

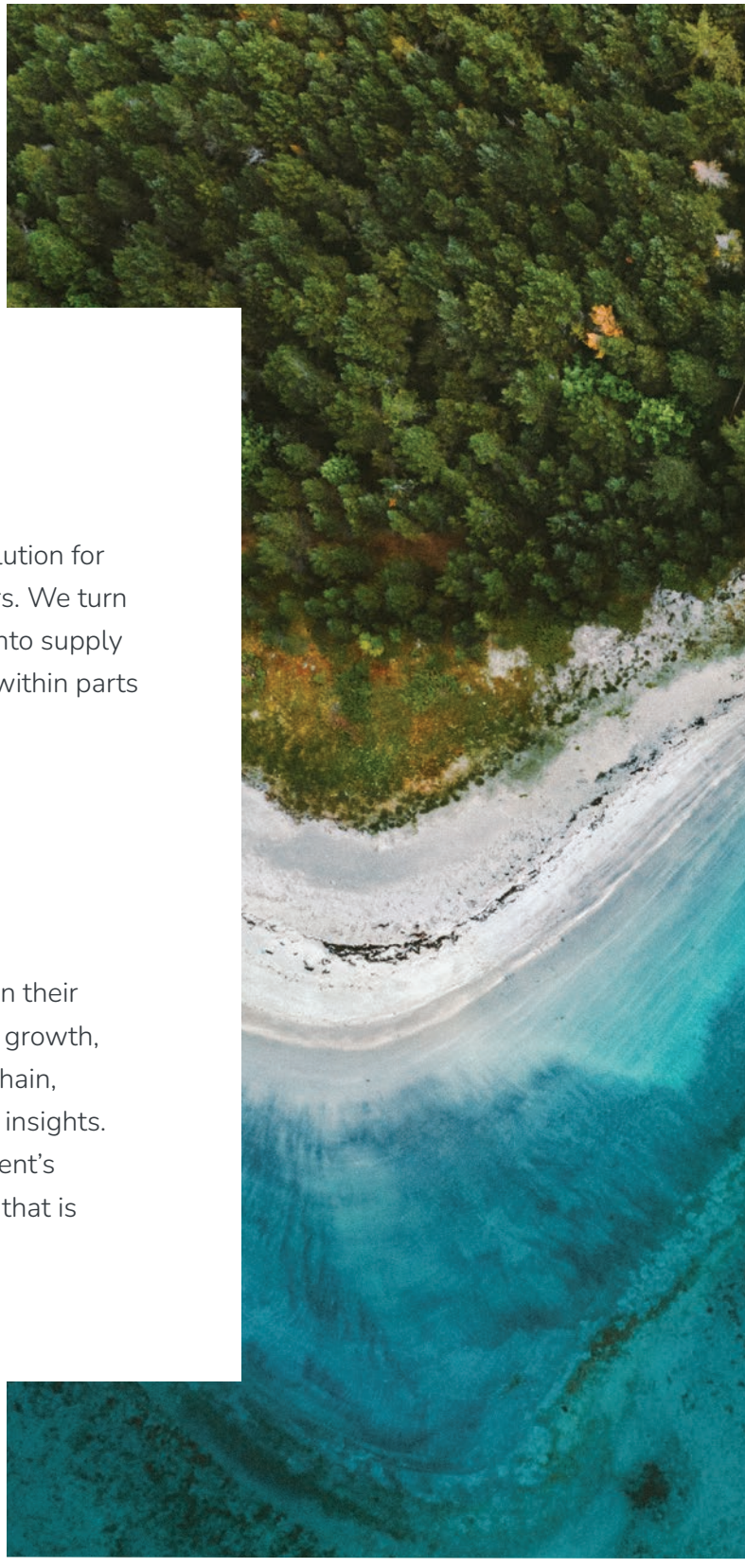
9. **Communicate.**

   Ensure customers and investors receive clear, confident reports on your due diligence efforts that can be supported by data.



These practices, and ensuring everyone in your supply chain is using the same standardized data tools, will help ensure your compliance program runs efficiently and effectively, even in the face of growing requirements.

For more information about how Assent can help electronics companies manage a robust, comprehensive compliance program, contact us at **info@assent.com**.



Who is Assent?

Assent is the supply chain sustainability management solution for the world's most forward-thinking complex manufacturers. We turn sustainability goals into tangible action by delving deep into supply chains, identifying suppliers, parts, and even substances within parts to map the entire complex manufacturing genome.

What We Do

We help companies spot sustainability risks hiding deep in their supply chains and identify new areas of focus to enhance growth, efficiency, and value. By digging deep within the supply chain, we pull and validate more actionable data to provide real insights. Guided by regulatory experts with a diverse skill set, Assent's solution delivers a cross-enterprise view of sustainability that is necessary for true leadership in the field.



[Assent is] a low touchpoint program with very high results and program growth, year in and year out.

— Ryan Zelhofer, Former Product Compliance Manager, Plexus

Over **200,000** parts managed

80% reduction in staff management hours

The Assent Solution

The journey toward sustainability demands a new way of thinking about supply chains. Assent turns your supply chain data into a critical tool to make safe, sustainable, and ethical products by providing:

- Clean data collected from the source using automated engagement techniques that dive deeper into supply chains
- Crucial, at-a-glance supply chain sustainability data through streamlined dashboards
- An adaptable program that evolves alongside regulations and industry trends

People are the beating heart of any sustainability program. Assent combines its leading technology with expert guidance, ensuring each program is tailored to your specific needs. Dedicated customer success managers make sure you have a familiar face to speak to about changing program goals or enhancements.

Our Global Offices

Canada
525 Coventry Road
Ottawa, ON K1K 2C5
Canada

Toll Free: 1 866 964 6931

Eldoret, Kenya
Daima Towers
21st & 22nd Floor
Eldoret, Kenya

Malaysia
Unit 9.02, Menara Boustead Penang
39, Jalan Sultan Ahmad Shah
10050 Penang

Netherlands
Barbara Strozzilaan 101, 1083 HN
Amsterdam, Netherlands

+31 20 299 1714

United Kingdom
Longcroft House
2-8 Victoria Avenue
Bishopsgate
London | UK | EC2M 4NS

United States
20 E Broad ST FL 8
Columbus, OH 43215-3403
U.S.A.

Toll Free: 1 866 964 6931

assent.com
info@assent.com

Assent will put you at the forefront of our changing world. See how in your personal demo.

Book My Demo



525 Coventry Road
Ottawa, ON K1K 2C5
Canada

1 866 964 6931
info@assent.com
assent.com

EE-EB-220325