



Intel[®] Technology Journal

The Spectrum of Risk Management in a Technology Company

Risk Management in Restricted Countries

Risk Management in Restricted Countries

Martin D. Martinez, Information Technology, Intel Corporation

Index words: restricted countries, risk management, security in restricted countries

ABSTRACT

Assessing Intel's risks, mitigating those risks, and protecting Intel's Intellectual Property (IP) are three key items that facilitate or impact Intel's continued success when working with or in *restricted* countries. Failure to comply with US government restrictions when working with or in these countries can result in heavy fines, loss of an export license, or imprisonment. Understanding the rules of engagement is critical in today's global economy. Which countries are restricted, what are the technology restrictions, and the consequences for non-compliance with the laws that govern working with or in those countries are discussed.

Intel faces numerous challenges when working in or with *restricted* countries because of cultural differences, different business practices and ethics, and weak IP laws and their enforcement. All of these challenges need to be considered to establish a solid and effective program that keeps Intel compliant with the US and international law, and yet does not impede Intel's growth and continued success in these countries.

In the last five or more years, Intel has seen an increase in the number of foreign nationals hired at Intel who have access to or contribute to Intel's IP. Foreign nationals continue to contribute to Intel's intellectual pool across many disciplines including research and development, sales and marketing, manufacturing, engineering, and software development. Maintaining regulatory compliance across Intel and driving an effective security program while growing the business is a continuous challenge.

Over the last 10-15 years, Intel has grown overseas and established a multi-faceted program that protects its IP at home and abroad. Intel has risk mitigating strategies in several areas including export and import of Intel technologies, data and network protection, data center operations, and physical security (domestic and international).

Intel constantly stress-tests its processes, procedures, and security tools while continuing to adapt to the changing

business environment in an effort to stay ahead of internal business and process changes. The results of our effort have allowed Intel to develop an adequate infrastructure that secures our IP on many different levels to keep us compliant with regulatory requirements while growing our business overseas.

INTRODUCTION

In 1985, Intel became one of the first American semiconductor companies to establish a presence in the People's Republic of China, with the opening of an office in Beijing. In 1991, Intel began its operation in Moscow, Russia and in February 2006, Intel announced a \$300 million investment to build a semiconductor assembly and test facility in Ho Chi Minh City, Vietnam.

Every decision involving Intel's expansion overseas has a multitude of legal and security requirements that have to be met. Failure to comply can result in loss of export licenses or loss of Intel's IP. For years Intel has been so successful in complying with legal and security requirements that on March 26, 2007 Intel announced plans to build a 300-millimeter (mm) wafer fabrication facility (Fab) in the coastal Northeast China city of Dalian in Liaoning Province. The \$2.5 billion investment for the factory will become Intel's first wafer Fab in Asia and yet another major milestone for Intel.

The challenges for Intel have not only been to understand the technology restrictions imposed by the US government, but also to push the envelope by introducing advanced technologies in several foreign countries. Then Intel has the additional challenge of implementing the best possible comprehensive program for protecting our IP.

Prior to introducing a new facility in a foreign country Intel uses a pre-production model (Figure 1) to address potential technology restrictions and potential risks.

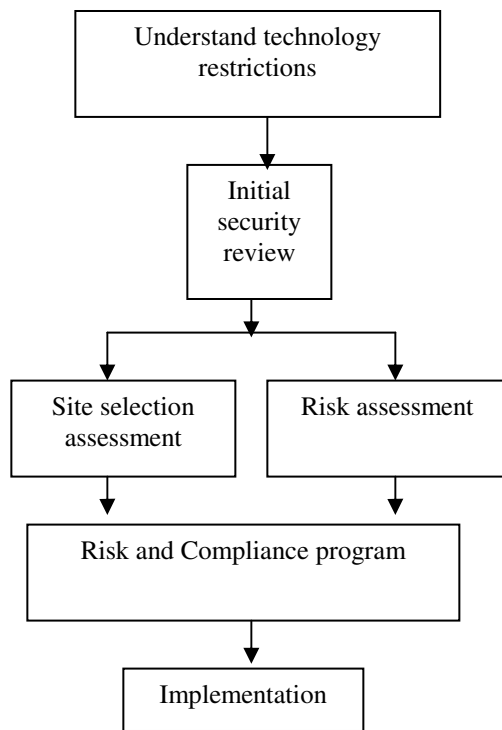


Figure 1: Pre-production model

A sustaining model (Figure 2) is used once Intel has established a facility in a foreign country and this model addresses any expansion or new businesses at that facility.

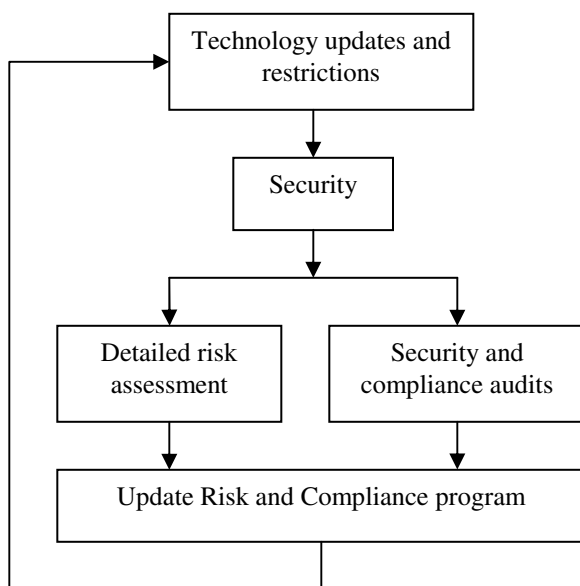


Figure 2: Sustaining model

The two models feed directly and independently into Intel’s security requirements that drive Intel’s overall risk and compliance program involving multiple efforts and organizations.

The consistency between these two models has contributed to the evolution of Intel’s risk management and compliance program and both have played a significant part in expanding our growth in foreign countries. Intel has successfully introduced and expanded sales marketing, research and design, software development, assembly and test facilities, and Fabs in various countries around the world.

The technology restrictions and security requirements continue to be complicated, but Intel’s risk management efforts continue to support business growth as Intel expands overseas.

RESTRICTED COUNTRY CLASSIFICATIONS

Foreign countries are considered “restricted” by the U.S. [Bureau of Industry and Security](#) (BIS) [4] for a variety of reasons; e.g., national security, foreign policy, terrorism, proliferation activities, etc. Intel further divides restricted countries into three categories (Table 1): High Performance Computing (HPC) Countries, Controlled Countries (CC), and Embargoed Countries.

Table 1: Intel's own categorized list of restricted countries

High Performance Computing (HPC)	Controlled Countries(CC)	Embargoed and Sanctioned Countries
Brazil	Albania	Burma (Myanmar)
Costa Rica	Armenia	Cuba
Hong Kong (region)	Azerbaijan	Iran
India	Belarus	North Korea
Israel	Cambodia	Sudan
Korea	China	Syria
Malaysia	Georgia	
Philippines	Iraq	
Singapore	Kazakhstan	
Taiwan etc.	Kyrgyzstan	
	Laos	
	Libya	
	Macau	
	Moldova	
	Mongolia	
	Russia	
	Tajikistan	
	Turkmenistan	
	Ukraine	
	Uzbekistan	
	Vietnam	

Note that even though Hong Kong is part of mainland China, export regulations identify Hong Kong as an HPC country. Therefore, the China technology constraints are not applicable to Hong Kong business activities.

The additional classification in Table 1 allows Intel security groups the flexibility to manage risk and compliance more effectively.

TECHNOLOGY RESTRICTIONS

Export regulations are imposed on restricted countries, and these regulations are monitored for compliance by the BIS. These regulations outline legal requirements for

exporting or re-exporting various products and technologies. When dealing with a restricted country, being aware of the regulations is very important. Failure to comply with export regulations can result in fines, loss of export licenses, or even imprisonment, all of which can vary depending on the nature of the incident and the restricted country involved.

Based on the three categories in Table 1 Intel adheres to the following technology restrictions (not all-inclusive):

High Performance Computing (HPC) countries: Currently Intel identifies and maintains a list of ~140+ countries as HPC. An export license is required to export or re-export HPC technology, generally involving design collateral for advanced chipsets. The BIS has a specific formula for calculating computer performance measured in Weighted TeraFLOPS (Trillion Floating point Operations per Second) that also sets boundary conditions for specific technologies that are applied across all restricted countries.

Controlled Countries (CC): Of the 21 countries on the list, Intel has facilities in nine of the CCs. Export licenses are required to export or re-export CPU design or manufacturing information, encryption products and technology, and HPC technology. Intel also has several export licenses that enable limited R&D and coordination throughout the company on new product development.

Embargoed Countries: US companies and individuals are prohibited from doing business with countries embargoed by the BIS. There are no license exemptions for these countries, and there is a presumption of denial for all exports and re-exports of products and technologies.

Intel has to abide by US regulations when exporting US technology from the US directly to a restricted country. However, when Intel is re-exporting US technology from within a restricted country to another restricted country we have to abide by both US regulations and any export or import regulations imposed by the countries involved.

For example, if we have an export license to export high-end chipsets with embedded encryption from the US to Russia and then that same product or technology is re-exported from Russia to Vietnam, we have to have an export license for Vietnam to comply with US export regulations. Russia may have additional export laws that Intel has to comply with, and Vietnam may have import regulations as well.

BIS also maintains a definitive list of *Non-Controlled Countries (Non-CC)* that are not considered restricted and generally there are no export restrictions when dealing with Non-CCs (e.g., Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Ireland,

Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States). Export restrictions are however applicable any time a Non-CC is dealing with any of the other three categories of restricted countries. Note that other regulatory agencies (i.e., Department of State, Office of Foreign Asset Control, or Department of Treasury) might impose regulatory restrictions on these countries that are not covered by BIS restrictions.

The Global Trade group within Intel is responsible for tracking the frequent export regulation changes, assessing the impact to Intel’s business activities, and implementing control processes as required. Intel has an excellent relationship with BIS officials and routinely meets with licensing officers to resolve questions and obtain export license approvals. Intel’s proactive efforts continue to be one of our key successes in working with or in restricted countries, something that is demonstrated by the various export licenses that we currently have in place among HPC countries and CCs.

Bilateral and multilateral requirements are in place in every aspect of Intel’s business (e.g., sales and marketing, research and development, assembly and test, manufacturing, etc.) that are governed by specific export requirements, and determining these requirements ahead of time is crucial.

METHODOLOGY FOR DETERMINING RISKS AND THREATS

Intel’s next challenge is comprehending the risks and threats. The methodology used (Figure 3) outlines the basic components of Intel’s security and risk model.

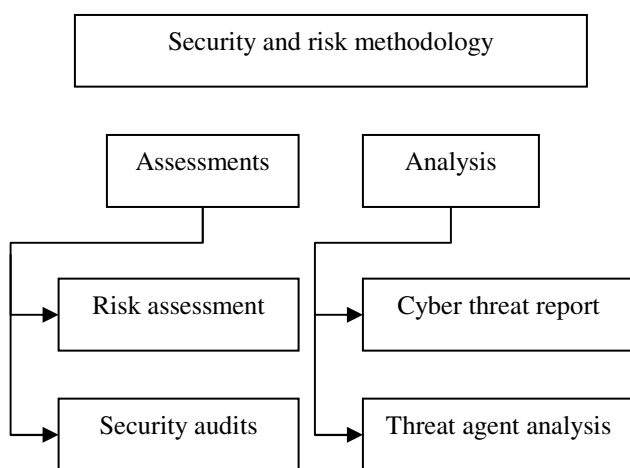


Figure 3: Security and risk model

In the assessment component of Figure 3, risk assessments are conducted as part of Intel’s site selection process when considering opening a new facility. The site selection process evaluates political stability, terrorism, IP vulnerability, corruption, crime, and site security services. Each category is rated across five levels ranging from unacceptable to exceeds expectations.

Additional risk assessments are conducted diving deeper into the business to determine risks and threats. Security professionals work closely with internal customers to understand the business environment, and to identify major or minor gaps that could potentially compromise Intel’s IP. Security audits are conducted to determine overall compliance with security standards and to find any new security risks. In addition, all risk and security assessment teams use an in-house developed tool as a standard base for all risk assessments. Domestically and internationally, the assessments and audits are conducted annually and randomly.

In the risk assessments component in Figure 3, we evaluate regulatory compliance, ethical and business practices, business issues, espionage, safety, personnel, information technology (IT), IP protection, and physical security. A common risk and threat equation used within Intel evaluates total risk as:

$$Threats \times Vulnerability \times Asset \ value = Total \ Risk$$

During this assessment Intel security understands the basic risks and threat without any additional mitigation controls in place. This provides a general overview of the issues Intel will need to address and tells us where to focus our resources.

Adding the mitigation controls provides a clear picture of the residual risks, and Intel can determine if risks and threats have been reduced to an acceptable level.

$$(Threat \times Vulnerability \times Asset \ value) \times Mitigation \ controls = Residual \ risk$$

The combination of the two equations yields the likelihood of a risk, potential impact, and a final ranking of each risk (e.g., business, regulatory, ethical, and security).

In the analysis component of Figure 3 an ongoing process that incorporates a team of security professionals across multiple security groups is conducted.

Quarterly cyber threat reports evaluate current and future cyber threats to allow security groups to understand implications to the business environment and the possible mitigation strategies available.

The Threat Agent Group (TAG) provides analysis across an extensive list of “characteristics” that represent the human factor within Intel’s threat model. A standardized

approach is used that facilitates security professionals to speak in a common language regarding the various threat agents and provides the means to measure the threats in a relative manner.

The threat agent matrix considers non-hostile threats (e.g., employee recklessness or untrained employees) and hostile threats (e.g., terrorist, vandalism, data miners, internal spy, disgruntled employees, corrupt suppliers or government officials, etc.). The process attempts to determine desired outcome, skill level, and resources available to the threat agent, among other criteria.

Additional assessments are also considered: for example, the office of the [US Trade Representative](#) [2] maintains an IP report on how well a country is managing IP protection that helps companies like Intel in driving policy changes within restricted countries. [Transparency International](#) [3] is another organization viewed by Intel security professionals that identifies various indicators on overall corruption in a given country.

The benefit of having the right data (e.g., corruption indicators, IP protection issues, etc.) allows Intel's security groups to conduct the best analysis possible; which provides a more accurate assessment of the risk and threats.

Business and security groups within Intel need to know who is after Intel's IP and what resources are being brought to bear to counteract this threat. Resources and finances are limited, so having the correct data in a timely fashion allows Intel to focus its resources in the countries that pose the greatest risks to Intel. This allows us to establish the best and widest possible parameters to protect our assets.

WHAT ARE THE RISKS AND THREATS

Kidnappings, street crime, organized crime, road traffic accidents, resistance to foreign-ownership by state-owned enterprises, medical problems (i.e., Avian flu) are but a few intangible considerations revealed by past site selection assessments.

Current Intel cyber and threat assessment reports a continued rise in cyber security risks. The ease of technical surveillance is also increasing, which causes IP and regulatory concerns to remain high.

Immediate benefits have been realized from the cyber and threat agent analysis. For example, this analysis can help us determine if risks or threats are driven by the private sector, or are sponsored by governments or the military. The private sector can be driven by a desire to be more competitive with multinational companies to avoid having their own small to midsize companies less competitive due to US influence or the influence of other multinational

companies. Governments can be driven by a desire to be more competitive on a global scale to help their own economies improve. The military of course can be driven by a desire to utilize US technology to not only upgrade their own weapons, but also to sell their own military technology to other countries at a much reduced rate, or to sell arms to countries that the US might not sell to.

Government- or military-sponsored activities tend to be better financed than those of the private sector. To complicate matters further, once the wrongdoer is identified, the judicial system may not always be in Intel's favor. IP protection is obviously a big concern and Intel aggressively pursues this with the legal establishment in restricted countries, especially in ones that are known to have weak IP protection laws.

Past assessments and analysis have indicated that the values and culture of a country can be a challenge and must be understood. Intel's business ethics may sometimes be diametrically opposed by certain individuals, groups, or suppliers. Failure to understand other cultures can be costly, bribes being a prime example. Bribes are viewed differently in Asian, Latin, or Eastern European cultures. They can be seen as a necessity in not only getting things done, but also in building the necessary relationships with the right people. If mishandled this can result in "losing face" on one end and impacting business on the other. Consequences of not giving bribes can be felt from construction to food services to obtaining permits, and therefore can easily double the time required to complete the simplest of tasks. However, one of Intel's key corporate principles is to *not* offer or accept bribes or kickbacks under any circumstances.

Misplaced or stolen laptops can sometimes be an issue also. In some countries it is a common practice for employees to sell their laptops to supplement their own income.

What is called plagiarism or copyright infringement in the US is viewed as borrowing from the best or copying with pride in some countries. Attempts to educate a local culture with Intel's business culture can be difficult but it has to be done. Patience is required: change seldom happens overnight. Cooperation between security and business groups moving to restricted countries helps Intel to be proactive in managing risks and threats.

Disciplinary actions can also vary given that in some regions (e.g., Asia) there are laws in place that can make termination of employees difficult. Each case can vary depending on the circumstances, but Intel works with all parties involved to come to an amicable solution.

DEEMED FOREIGN NATIONALS

Another area that needs to be addressed, and that is equally important to understand, is the use of deemed foreign nationals (DFNs) that have access to restricted technology within Intel. DFN is the classification used to identify foreign nationals hired in the US. Generally DFNs are hired from US universities, but sometimes they are also hired from other US-based companies.

Intel has a significant population of DFNs from many restricted countries. When Intel hires a DFN, business groups have to take into account if that DFN is from an HPC country, a CC, or an Embargoed country. If a DFN is from a CC or an Embargoed country, an export license will need to be obtained when that person is hired. Since Intel generally hires DFNs for technical positions, an export license is automatically a requirement. In the event a DFN moves onto another job that may require access to restricted technology Intel avoids any delays by having an export license in place in the early stages of employment.

DFNs from an HPC country generally do not require the same level of scrutiny, due to the fact that the threshold of technology is much higher for an HPC country. In those rare cases where a DFN from an HPC country requires access to restricted technology beyond what an HPC country is allowed, then Intel has to obtain an export license.

Also note that when a DFN obtains permanent residency or becomes a US citizen, then an export license is no longer required. Obtaining permanent residency or US citizenship can take between three to seven years.

Obtaining credible background data on employees equivalent to what Intel can obtain in the US is also a challenge. In Asia, for example, a person can potentially pay to have damaging information removed from their records or to even add false information. Hiring foreign nationals in the US comes with additional challenges. Intel is still limited to the information provided by the country the foreign nationals come from. Competitive intelligence (a.k.a., espionage) and the insider threat have taken on a whole new meaning in the 21st century.

The better-educated Intel employees are about the risks and mitigating strategies, the culture, how best to do business in restricted countries, the better Intel can deal with problems they may face when doing business in or with restricted countries.

HOW INTEL MANAGES RISKS AND THREATS

Intel defines overall requirements for managing risks and threats based on regulatory, and security and risk managements efforts.

The regulatory component is driven by the Global Trade group and drives compliance with US and international export regulations. Some key aspects of the regulatory component include the following:

- The Global Trade group interprets export regulations, classifies restricted technology, and determines export restrictions to international destinations.
- The Global Trade group and Information Security conduct technology reviews with business groups in advance of moving operations (part or all) to overseas destinations. Such reviews assess the scope of the project, associated technologies, and determine license and security requirements that allow Intel to have consistent controls across the corporation.
- The Global Trade group defines and manages the global hiring processes and foreign national license reviews. Here, Global Trade evaluates the job requirements of Intel's foreign national employees, classifies the type of technology the employee will be able to access, and obtains the appropriate export license for each foreign national.

The security and risk management component (Figure 4) drives Intel's IP and regulatory protection efforts consistently across the various security groups at Intel.



Figure 4: Security management model

Having clear security policies that outline roles and responsibilities, expectations, and requirements is the cornerstone of Intel's security program. Flexibility is maintained within security policies by working with the business groups to understand the demands of the business. For example, data segmentation or additional security monitoring may be required when sensitive IP is involved in certain high-risk countries.

Security groups work closely with Global Trade and take additional precautions to adhere to any conditions that are spelled out in any export license that Intel obtains.

To stay current with competitive intelligences, cyber threats, and availability of the latest security tools, education of Intel's security professionals is actively pursued. Through participation in security conferences and seminars and working with external security organizations (e.g., [Information Risk executive council](#) [1]) Intel is able to stay abreast of the latest information in the security field.

Additionally, most security professionals at Intel have or are pursuing some type of security credentials. Among the most common are Certified Information System Security Professional (CISSP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), and Global Information Assurance Certification (GIAC). The wide variety of certifications maximizes the capabilities of Intel's security professionals and maintains a high standard across multiple security groups.

Training Intel employees is just as important as educating Intel's security workforce and is paramount in keeping Intel compliant. Intel's training and awareness programs cover both security and global export education. Courses provide basic understanding on expectations, regulatory and security requirements, and case studies to educate Intel employees. The native language of a country is also used where possible to facilitate learning.

The combination of regulatory and security efforts allows Intel to conduct compliance assessments across the company. Assessments are conducted annually while differentiating between export and Intel security compliance. Business groups require a clear understanding between US government vs. Intel requirements to better manage their own resources to address gaps and continually improve.

CONSEQUENCES OF NON-COMPLIANCE

Intel makes a tremendous effort to understand regulatory requirements, comprehend risks and threats, and implement the right amount of security based on those risks. Failure in any area can result in loss of IP or legal action from the BIS.

There are legal ramifications for compromising Intel's IP as such actions adversely impact Intel's strategic competitiveness or result in financial loss. Recovery from IP loss can take several years and within Intel's competitive environment significant or critical IP loss is not an acceptable risk.

The complexity of the regulatory environment mandates that questions be asked to determine if an export license is needed; e.g., what type of technology will be used, which restricted countries are involved, are DFNs a factor, will technology or products be re-exported, etc. Each one of the above may come with conditions or restrictions that have to be clearly understood and implemented.

Honest mistakes can and will be made, but the ones that are not reported can do the most damage. Export regulations are complex and often have "gray" areas that might be open to interpretation. By working very closely with the BIS and other government agencies Intel has avoided potential road blocks.

The consequences of a bad interpretation of an export regulation or for not adhering to conditions that are part of an export license, for example, can result in penalties to Intel and its employees.

The BIS breaks down Export Administration Regulations (EAR) violations into two categories: criminal and civil:

Criminal

For *willful violations* that involve a company and/or employees who deliberately are involved in covering up an EAR violation and do not report it, the consequences can be severe:

A corporation could be fined up to \$1,000,000 or five times the value of the exports for each violation, depending on which is the greater.

An individual could be fined up to \$250,000 or be imprisoned for up to ten years, or both, for each violation.

For *knowing violations* that involve a company and/or employees who are involved in an EAR violation but report the violation upon discovery, the consequences can also be severe:

A corporation could be fined up to \$50,000 or five times the value of the exports for each violation, depending on which is the greater.

An individual could be fined up to \$50,000 or five times the value of the exports, or can be imprisoned for up to five years, or both, for each violation.

Civil

For each violation of EARs companies and individuals can be penalized as follows:

They can be *denied export privileges*. This means all of the export privileges of a company or individual will be removed to prevent an imminent export control violation. These orders cut off not only the right to export from the US, but also the right to receive or participate in exports from the US.

They can be *excluded from trade* and/or a fine of up to \$11,000 for each violation can be imposed.

Violations involving national security can result in fines of up to \$120,000 for each violation.

To better illustrate the consequences, here are two examples of recent cases.

In September 2004, the BIS assessed a \$560,000 administrative penalty against Lattice Semiconductor Corporation for sending extended range programmable logic devices and technical data to China and sharing restricted technology with Chinese foreign nationals in the US. The items and technology are controlled for national security reasons.

In April 2006, Boeing Corporation settled a long-running case with the State Department’s Directorate of Defense Trade Controls for a sum of \$15 million in penalties for violation of export laws involving gyro chips to China.

Export laws change from year to year and specific country-based restrictions can change numerous times during any given year: staying abreast of these changes is a necessity.

Intel is very assertive in maintaining the proper security to restrict and avoid inadvertent access to unauthorized

technology by restricted country employees. Both Global Trade and Corporate Security take an active role to protect Intel’s IP. Intel’s expectation is that every employee shares in the responsibility of keeping Intel compliant with export regulations, internal security, and IP requirements at all times.

SUMMARY

Managing Intel’s business activities in restricted countries, maintaining regulatory compliance, and adhering to security guidelines is complex and challenging, as is maintaining compliance with license requirements for DFNs.

Intel’s ability to build a Fab in China, and the great strides Intel has made in other countries such as Russia and Vietnam have been possible due in large part to Intel’s due diligence in understanding regulatory requirements and mapping a successful security and risk management strategy.

Intel’s security and risk management efforts have been discussed in varied detail and are summarized in Figure 5. This figure illustrates the high-level components of Intel’s effort to remain compliant, protect our IP, and still be flexible enough to stay on track with our dynamic business environment.

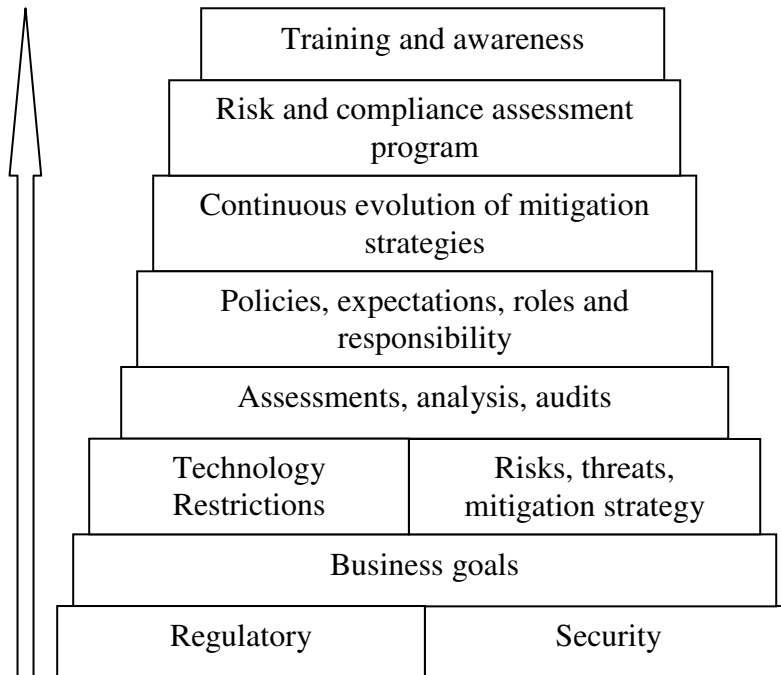


Figure 5: Security and risk management model

Intel understands the job requirements, business goals, and the diversity of cultures in these countries and realistically maps the risks and threats by country.

As Intel continues to grow and expand into restricted countries, new market segments and new technology areas, Intel's export and security compliance program continues to evolve in support of corporate objectives. We have established one of the most assertive security programs for our industry. Dealing with export requirements and numerous cyber security threats, along with internal and external security issues requires due diligence on the part of all employees. Educating everyone in the company on the risks, threats, consequences, and expectations protects Intel's IP and employees, our most valuable corporate assets.

ACKNOWLEDGMENTS

We acknowledge Keith Core, Information Risk and Security, Data Protection Compliance manager, Carol Kasten, Information Risk and Security, Data Protection Department manager, Victoria Gomez Kelsey, Technology and Manufacturing Group–Risk and Controls, Glen Shirley, Principle Engineer, Technology and Manufacturing Group, and Susan A. Straub, Director of Global Trade, for their contributions to this paper.

REFERENCES

- [1] Information Risk executive council at <https://www.irec.executiveboard.com/Public/Default.aspx>*
- [2] Office of the US Trade Representative at <http://www.ustr.gov/>*
- [3] Transparency International at <http://www.transparency.org/>*
- [4] US Bureau of Industry and Security–US Department of Commerce at <http://www.bis.doc.gov/>*

AUTHOR'S BIOGRAPHY

Martin D. Martinez is the Control Country Business Manager for Intel since 1999. Martin worked in China for two-and-a-half years and travels overseas on an annual basis. He has a B.S. degree in Computer Science from the University of Texas in San Antonio. His current interest revolves around competitive intelligence. His e-mail address is martin.d.martinez@intel.com.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4,

IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel Leap ahead., Intel Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Intel's trademarks may be used publicly with permission only from Intel. Fair use of Intel's trademarks in advertising and promotion of Intel products requires proper acknowledgement.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

Intel Corporation uses the Palm OS® Ready mark under license from Palm, Inc.

Copyright © 2007 Intel Corporation. All rights reserved.

This publication was downloaded from <http://www.intel.com>.

Additional legal notices at: <http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

For further information visit:

developer.intel.com/technology/itj/index.htm