ORIGINAL FINDINGS

Global Compliance Intelligence Report

SecureTrust™
a Trustwave® division

Global Compliance Intelligence Report

Overview

Establishing an organizational maturity model for key indices of risk is an essential ingredient of current best practices in strategic planning.

Not only does SecureTrust deliver explicit Security Maturity Services, it includes Compliance Intelligence derived from its security maturity ratings with its other Global Compliance and Risk Services assessments to provide your organization with a snapshot of the maturity of your processes compared to other organizations in your region and your industry.

In this white paper, we'll examine:

- what Compliance Intelligence is
- what "good" should look like
- key global insights
- how Compliance Intelligence can benefit your organization
- how you can learn more

Executive Summary

The *SecureTrust Global Compliance Intelligence Report* gives you the opportunity to review security maturity ratings by industry and by eight key organizational controls. Key findings from this report include:

- None of the industries measured in the aggregate is achieving an optimum maturity rating of 3.5 for the controls.

  Certainly, within each industry, there are organizations that are focusing on security and compliance that achieve the optimum rating for particular controls, but there is additional focus needed for each industry as a whole.

- The Financial Services industry leads the industry group in terms of maturity ratings.

  The Financial Services industry includes organizations that are under a lot of scrutiny for their data security, such as the card brands, banks and payment gateways. It is not surprising then that the overall maturity scores for these organizations lead the industry list.

- The overall low maturity rating of the Service Provider industry is an area of concern.

  This finding correlates with the large increase in service-provider compromises noted in the *2018 Trustwave Global Security Report*. The industry maturity ratings include the ratings of mature organizations that are proactively addressing security and compliance requirements, but the overall ratings are brought down by those Service Providers who are only beginning to put their compliance programs in place.

What is Compliance Intelligence?

SecureTrust Compliance Intelligence is derived from SecureTrust security maturity ratings against key controls that are built in to each of its key assessment services, from Compliance Validation Services for Payment Card Industry compliance and General Data Protection Regulation services to information security risk assessments. As the largest Qualified Security Assessor in the world, SecureTrust has a large and growing database from which to derive the intelligence.

SecureTrust bases its maturity levels on the Capability Maturity Model Integration (CMMI), a globally-recognized set of best practices designed to enable organizations to improve performance, key capabilities, and critical business processes. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. A key benefit of the CMMI is that it establishes a framework for continuous process improvement.

SecureTrust Compliance Intelligence Five Maturity Levels

The five Compliance Intelligence levels, based on CMMI, are:

- **Level 1**
  At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.
- **Level 2**
  At the repeatable level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.
- **Level 3**
  At the defined level, an organization has developed its own standard process through greater attention to documentation, standardization, and integration.
- **Level 4**
  At the managed level, an organization monitors and controls its own processes through data collection and analysis.
- **Level 5**
  At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

What Good Should Look Like

The ideal maturity level for a particular organizational control will depend on that organization's priorities and risks. In general, however, for the Compliance Intelligence model, an organization should strive for a baseline security maturity of 3.5 on the scale of 5 outlined above, which is midway between the defined Level 3 and the managed Level 4.

Controls Measured in Compliance Intelligence

The SecureTrust Compliance Intelligence model measures the maturity of eight key organizational controls as listed below with their subprocesses. These controls were chosen for their applicability to common compliance frameworks.

Boundary Defense:

- Secure Configurations for Network Devices, Hardware, and Software
- Limitation and Control of Network Ports
- Personal Firewalls

Asset Management:

- Secure Configurations for Network Devices, Hardware, and Software
- Inventory of Authorized and Unauthorized Devicess

Change Control:

- Application Software Security
- Antivirus and Malware Defenses
- Application Development
- Data Lifecycle Management

User Management:

- Controlled Use of Administrative Privileges
- Account Monitoring and Control

Data Protection:

- Encryption
- Controlled Access Based on the Need to Know

Facility Controls:

- Security Testing and Monitoring
- Maintenance, Monitoring, and Analysis of Audit Logs

Incident Response and Management:

- Continuous Vulnerability Assessment and Remediation
- Penetration Tests and Red Team Exercises

Training:

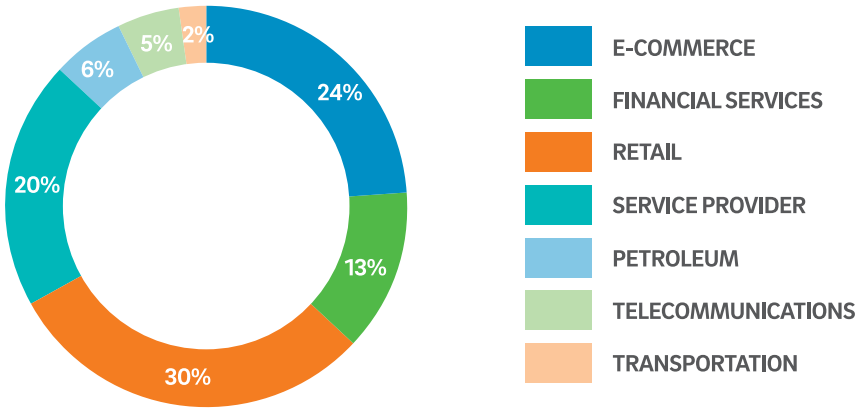
- End-user Training
- Security Staff Skills Development

Key Global Insights

In this section, we highlight overall findings in 2018 from the SecureTrust global Compliance Intelligence database.

Data Sources

The global Compliance Intelligence database is derived from the security maturity ratings that are delivered by SecureTrust Global Compliance and Risk Services team as a value-added offering with our assessments. In this view of the global Compliance Intelligence findings, Retail is largest represented industry at 30%, followed by E-Commerce at 24%, Service Provider at 20% and Financial Services at 13%.

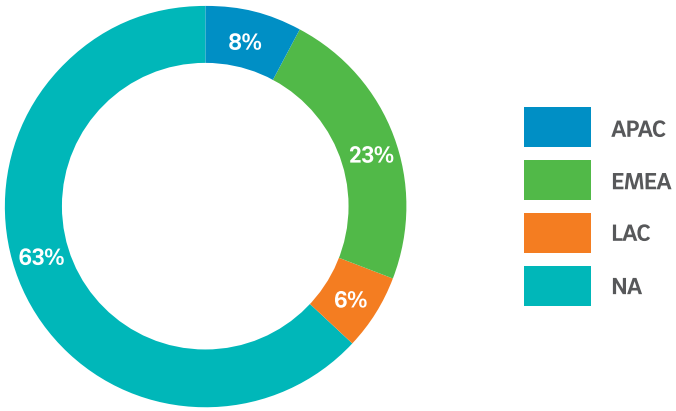


The industry breakdown for the 2018 Compliance Intelligence analysis is shown above.

SecureTrust Compliance Intelligence is measured across four regions of the world:

- North America (NA)
- Europe, Middle East and Africa (EMEA)
- Asia Pacific (APAC)
- Latin America Countries (LAC)

While North America and EMEA tend to lead in Compliance Intelligence maturity ratings, particularly Data Protection, there were commonalities across regions across the organizational controls. Most strikingly, none of the regions achieved the optimum 3.5 average rating for any of the control categories.

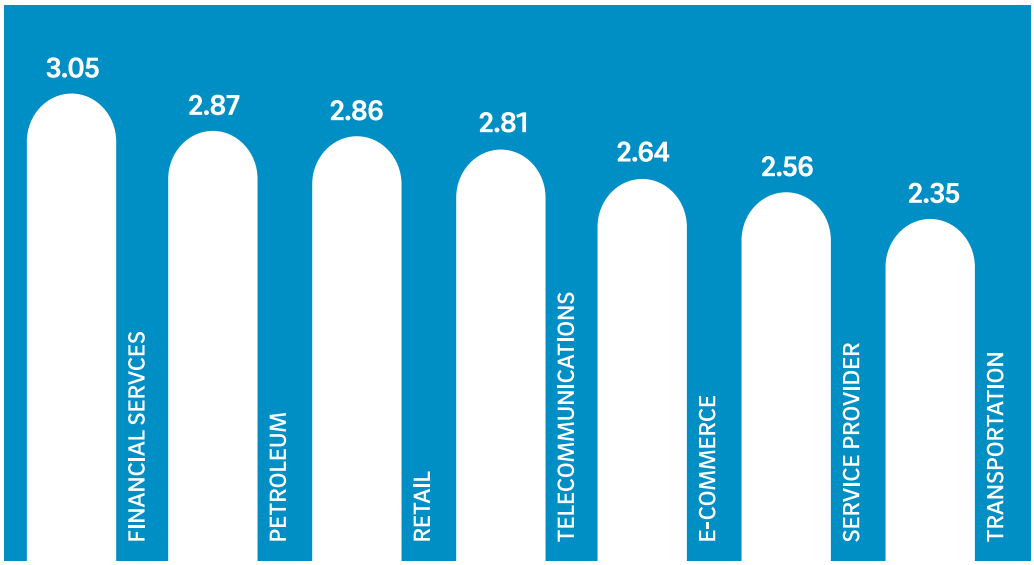


The industry breakdown for the 2018 Compliance Intelligence analysis is shown above.

In the 2018 global Compliance Intelligence findings, North America (North America) is largest represented region at 63%, followed by Europe, Middle East and Africa (EMEA) at 23%, Asia Pacific (APAC) at 8% and Latin American Countries (LAC) at 6%.

Maturity by Industry

The Financial Services industry leads the industries in terms of overall ratings with a maturity score of 3.05. It also leads for each of the eight controls except for Facility Controls, where Telecommunications is narrowly ahead.



No industry measured has achieved the desired 3.5 optimum maturity level.

Service Provider Industry Maturity Findings

The relatively low ranking of Service Provider maturity within the industry group is worthy of comment. This finding correlates to findings in the *2018 Trustwave Global Security Report*. It noted, "Of particular concern is the large increase in service-provider compromises, which includes any business that provides IT services to other businesses. This industry can be an attractive proposition for targeted attacks as a successful compromise can give an attacker access to numerous businesses. We assisted a variety of service providers, including web-hosting providers, point-of-sale (POS) integrators and helpdesk providers, in responding to breaches in 2017. In 2016, service-provider compromises did not even register in our statistics."[1]

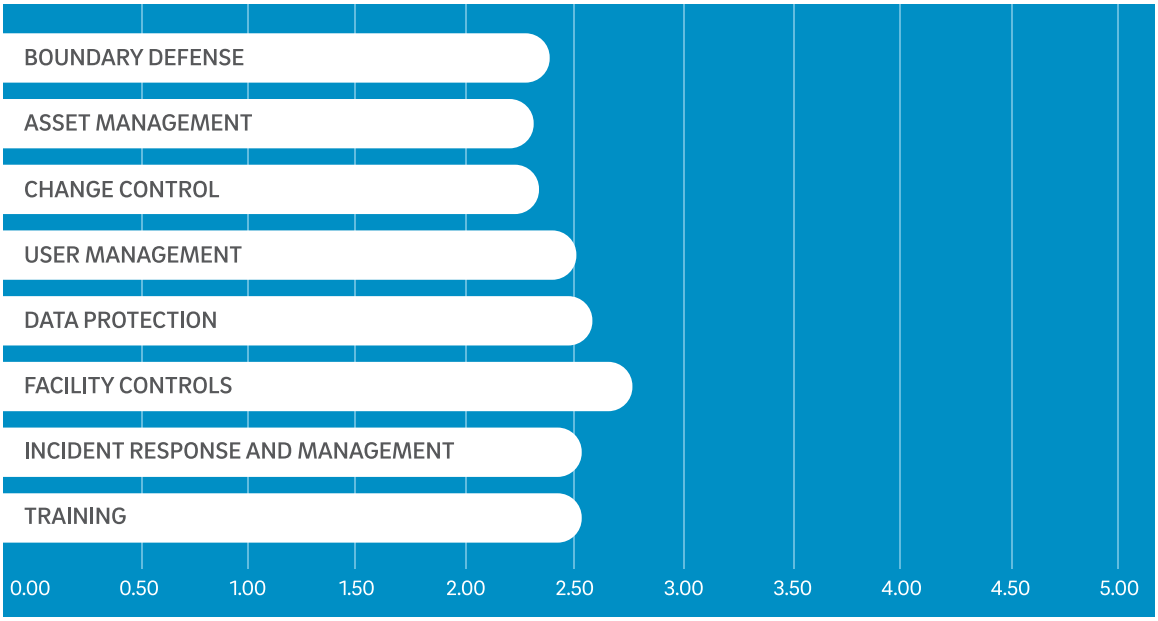
One of the reasons for the lower scores overall is that many Service Providers are only beginning to understand that they are required to meet compliance standards. The industry maturity ratings include the ratings of mature Service Provider organizations that are proactively addressing security and compliance requirements, but the overall ratings are brought down by those Service Providers that are only beginning to put their compliance programs in place. Service Providers that service a large number of organizations tend to be more mature in their processes, while Service Providers with smaller populations are often just beginning to recognize and address compliance requirements such as the Payment Card Industry Data Security Standard. There is anecdotal reporting that these organizations with immature programs may be seeking the most expedient, as opposed to the most thorough, approach to meeting their compliance obligations. Clearly this is something that organizations employing Service Providers should take in to account for their own security.

With the increasing scrutiny on Service Providers as a critical link in an organization's security chain, we would expect the maturity ratings in this industry to increase in coming years.

Looking at the individual controls for the Service Provider industry, we would expect both Boundary Defense and Asset Management to be higher, as critical elements of their third-party services role.

[1] 2018 Trustwave Global Security Report, Data Compromise, page 29.

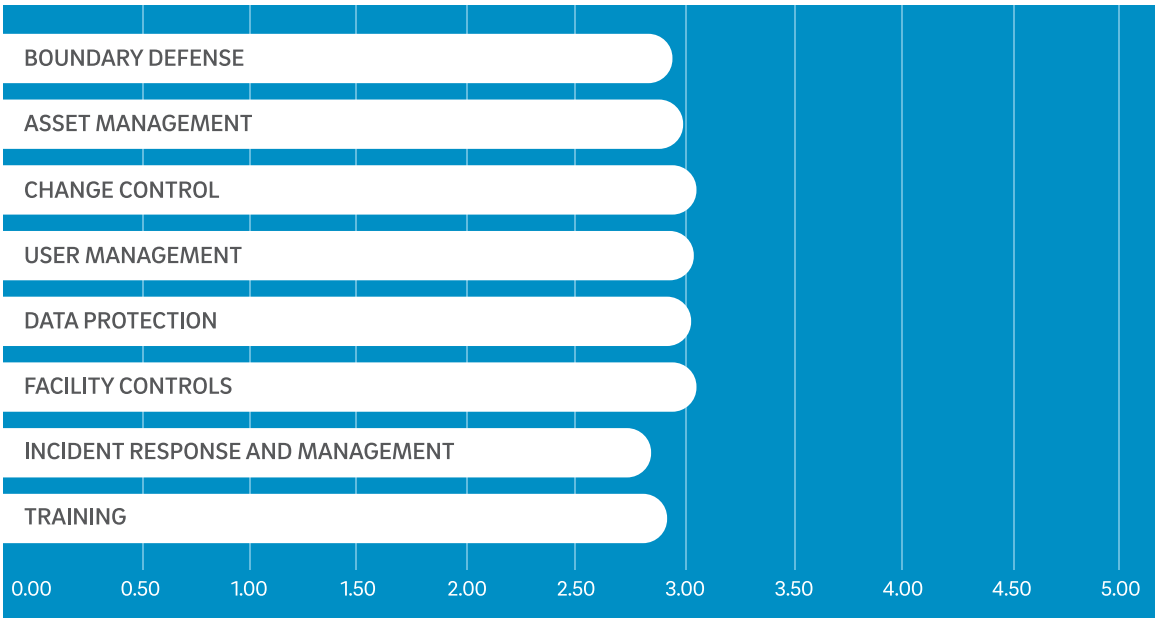
Service Provider



Financial Services

The Financial Services industry includes organizations that are under a lot of scrutiny for their data security, such as the card brands, banks and payment gateways. It is not surprising then that the overall maturity scores for these organizations lead the industry list. Note that the ratings are lower than would be expected, however, for both Boundary Defense, which includes secure network configurations and firewall protection, and Incident Response and Management, which includes continuous vulnerability assessment and remediation and penetration tests and Red Team exercises.

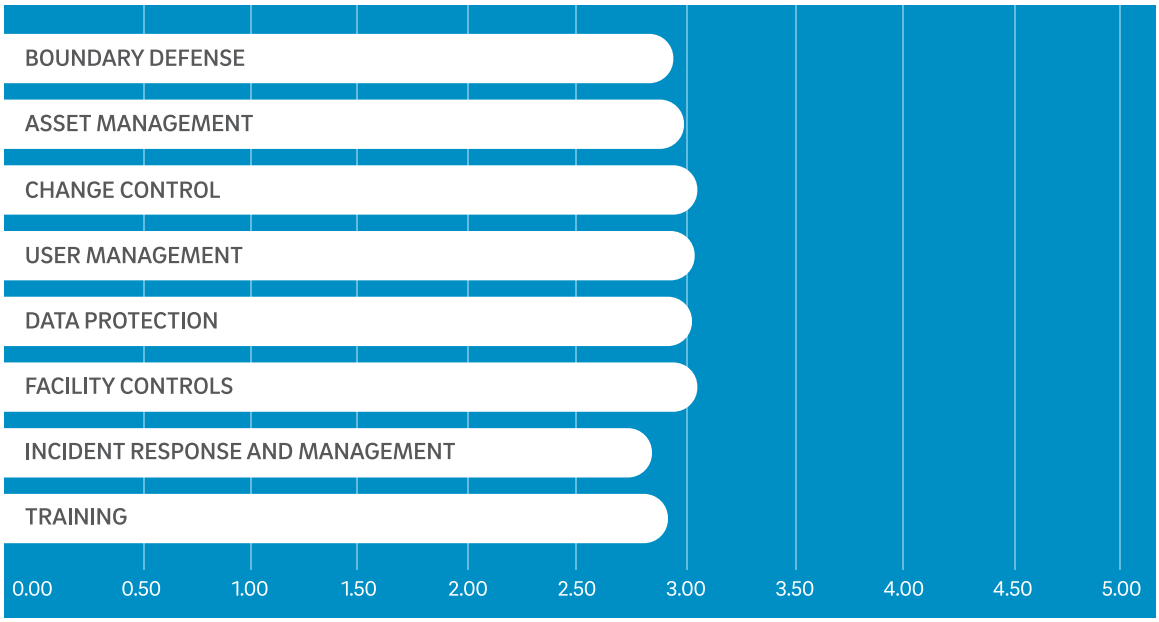
Financial Services



Retail

In the Retail industry, the ratings show that Change Control and Asset Management are the controls with most room for improvement. For Retail, management and tracking of point-of-sale systems is an ongoing challenge, which is reflected in the lower Asset Management rating.

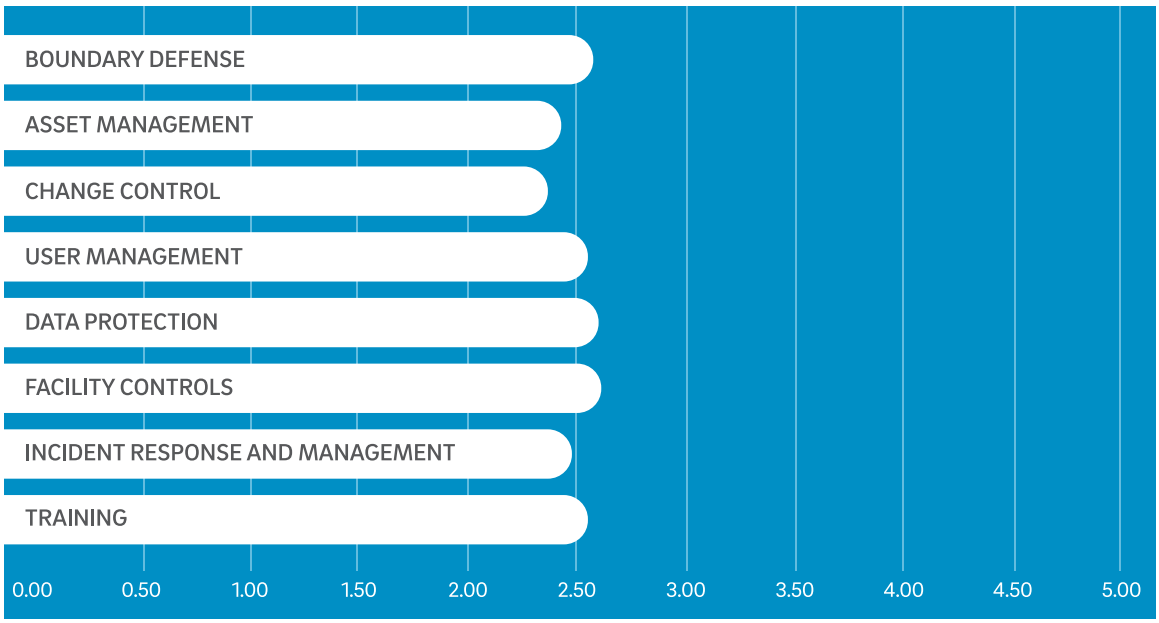
Retail



E-Commerce

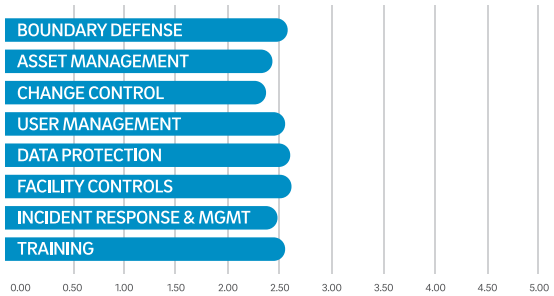
For the E-Commerce industry, due to the focus in online transactions, we would expect Boundary Defense, Data Protection and Change Control (critical in a highly fluid environment) to be higher.

E-Commerce

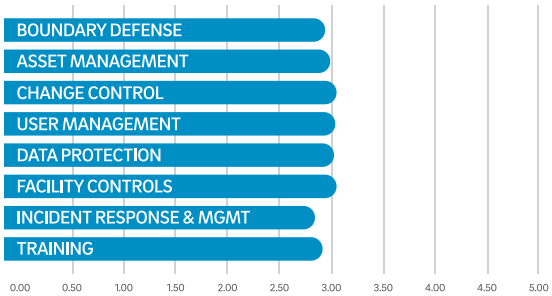


Maturity Ratings by Industry

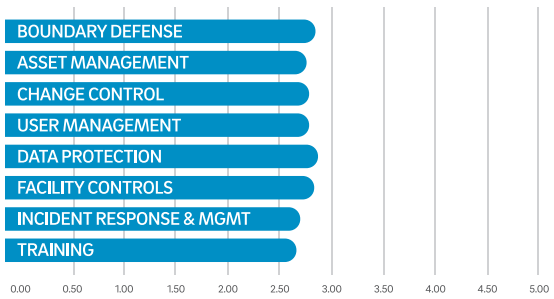
E-Commerce



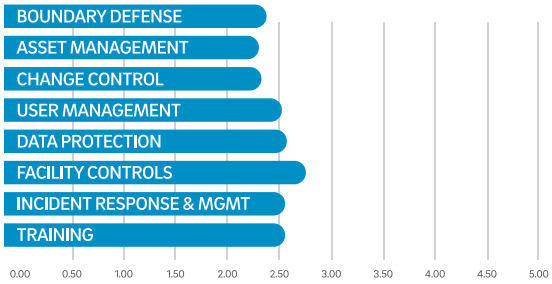
Financial Services



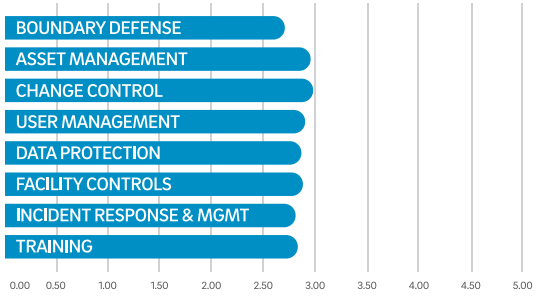
Retail



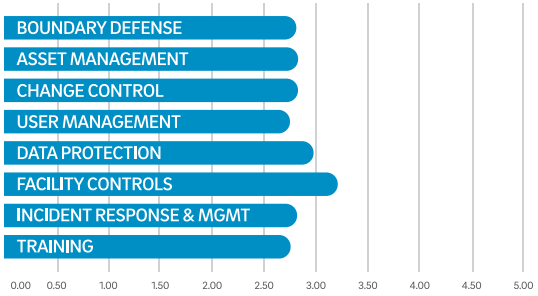
Service Provider



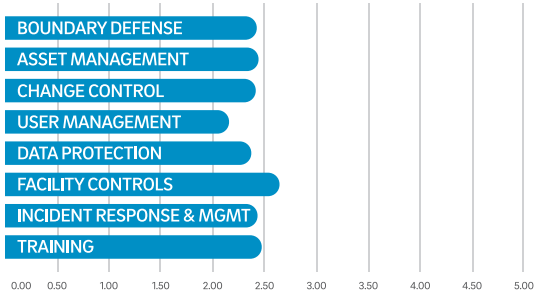
Petroleum



Telecommunications

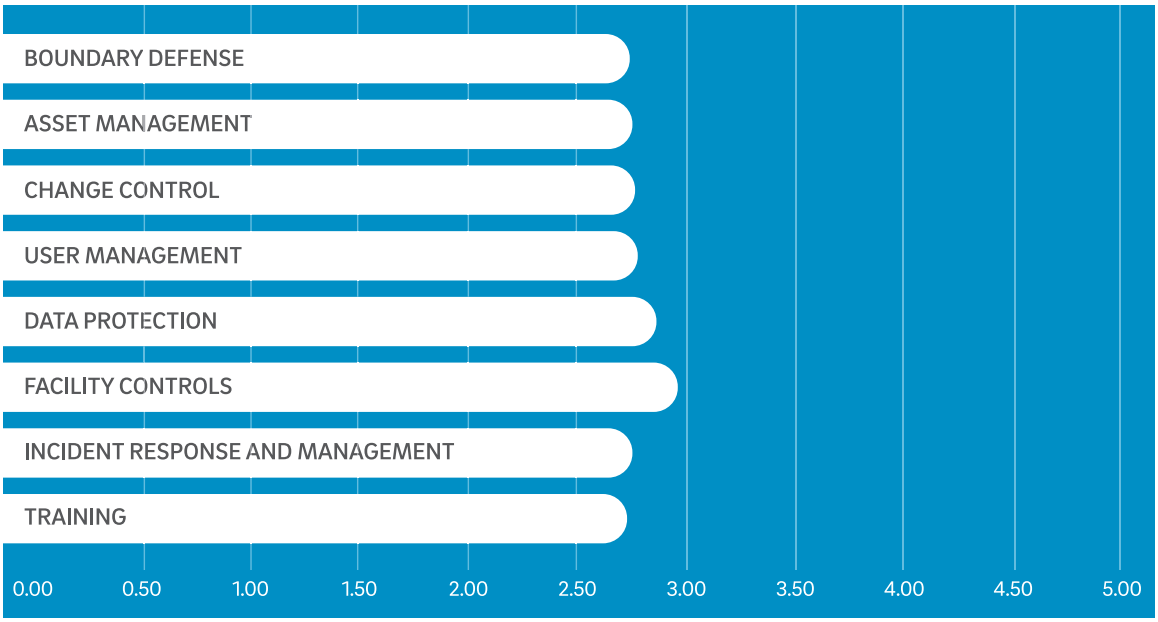


Transportation



Analysis by Control

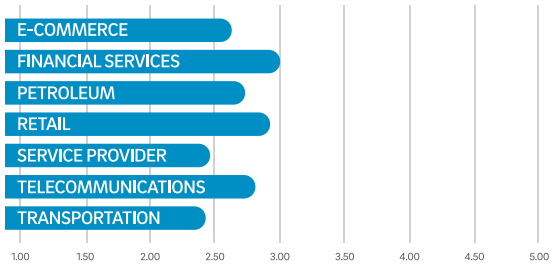
When we examine the maturity ratings by Control, as shown in the charts below, we find that Facility Controls has one of the higher maturity ratings. This is attributed to the fact that Facility Controls are typically easily achieved. But ease of implementation does not seem to the sole factor in the maturity ratings for the controls. Note that Incidence Response and Management, which is one of the more difficult controls, has an overall maturity rating that is higher than Training, which should be a relatively simple control to achieve.



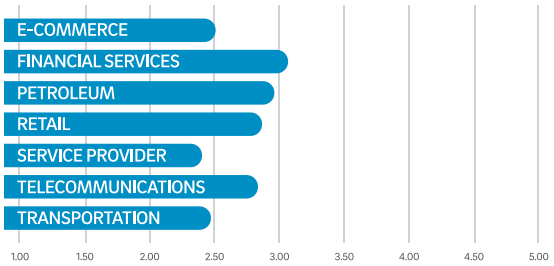
Facility Controls is one of the easiest to implement and shows the highest overall maturity rating.

Maturity Ratings for Each Control

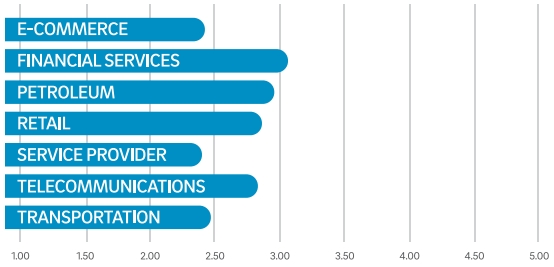
Boundary Defense



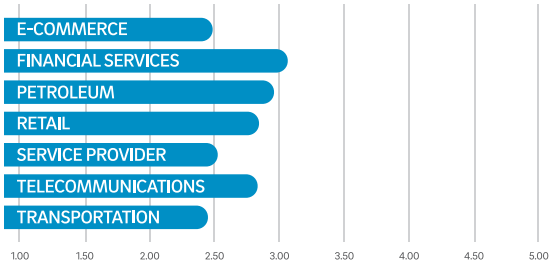
Asset Management



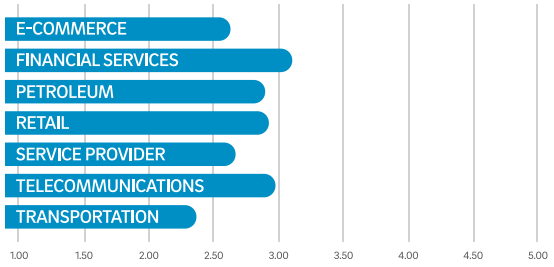
Change Control



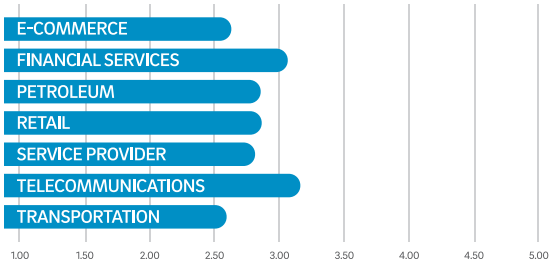
User Management



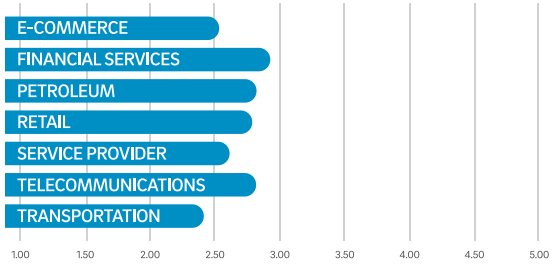
Data Protection



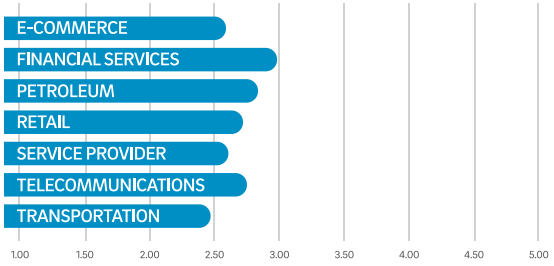
Facility Controls



Incident Response and Management



Training



How Compliance Intelligence Can Benefit Your Organization

When you receive your *Compliance Intelligence Report* from SecureTrust along with your contracted service, you are given information that you can use to your strategic advantage. The report shows you how your organization rates on each of the key controls and subprocesses, so you understand where improvements should be made to reach the rating of 3.5 as a minimum standard. You will also understand how your organization ranks among other (anonymized) organizations in your industry and your region. This offers you an objective view of where you stand against competitors in your industry and gives you a starting point from which to plan for ongoing process improvement to align the maturity of your processes with your organization's goals.

Learn More

With each of the key SecureTrust assessments, we will deliver your organization's Compliance Intelligence ratings as compared to other anonymized organizations in your region and your industry. To learn more, contact us at www.securetrust.com.