Discussion on:

Evaluating Cybersecurity Coverage – A Maturity Model

Presented to:
ISACA – Charlotte Chapter
Vision for IT Audit 2020 Symposium

By:
Eric C. Lovell
PricewaterhouseCoopers LLP ("PwC")

March 24, 2015

pwc

Quest for IT Audit Enlightenment

"Are we covering the right things the right way?"

Questions Answered by the Model

Risk Identification	Have the right risks been identified at the right level of the firm?
Audit Universe	Have appropriate auditable units been defined to encompass the identified risks?
Risk Assessment	Have risks been appropriately assessed and prioritized?
Coverage Strategy	Has an appropriate coverage strategy been defined and implemented?
Testing Strategy	Have appropriate test strategies been developed on individual audit engagements and executed by skilled staff?

Survey Says…

Key Findings from 2015 Global State of Information Security Survey (GSISS)

- ***Incidents and financial impacts continue to soar:*** The total number of security incidents detected by respondents climbed to 42.8 million this year, an increase of 48% from 2013.

Survey Says…

Key Findings from 2015 Global State of Information Security Survey (GSISS)

- ***Declines in fundamental security practices:*** As security risks rise, organizations should seek to implement the necessary processes and technologies to prevent, protect, detect, and respond to elevated threats.

Survey Says…

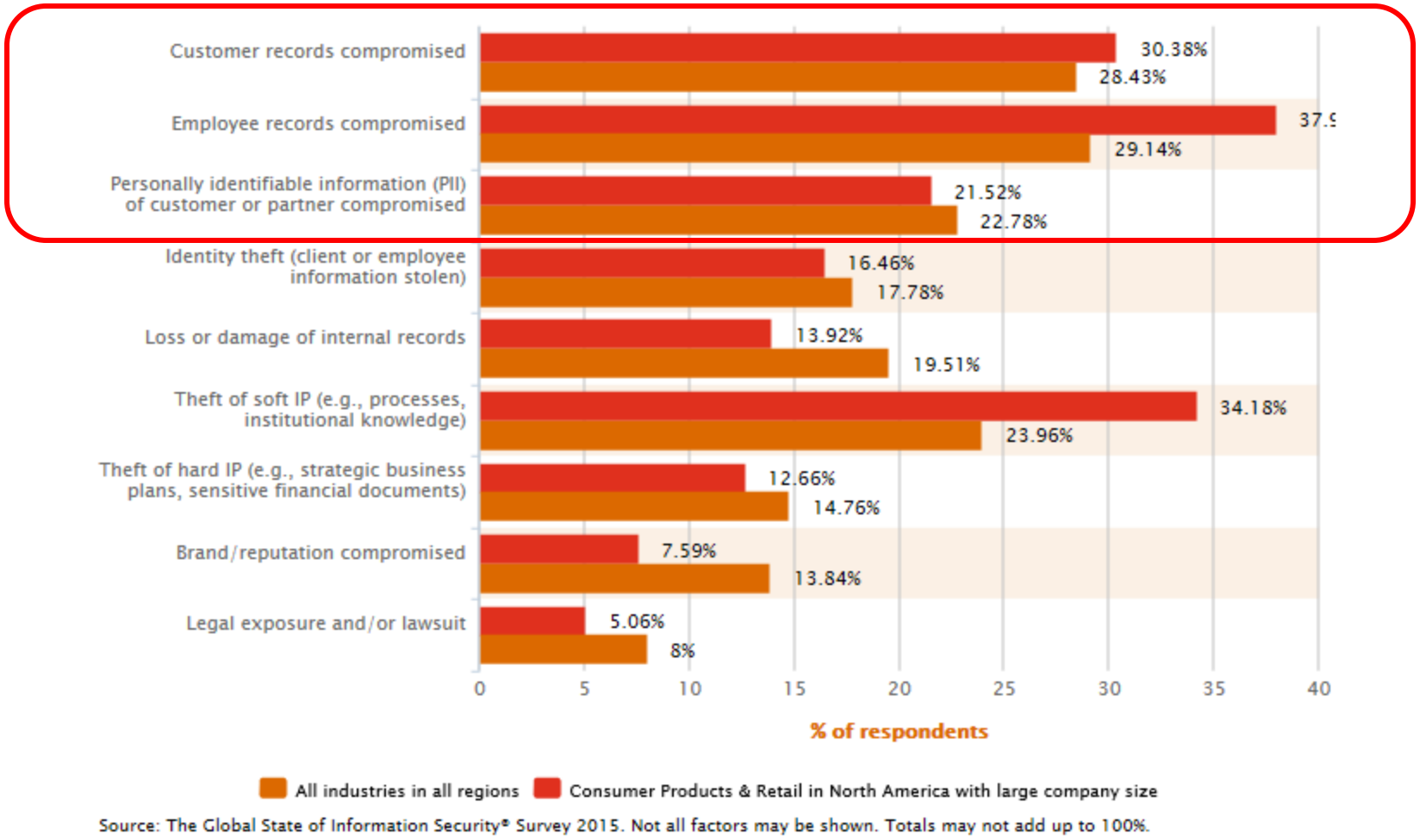
Key Findings from 2015 Global State of Information Security Survey (GSISS)

- ***As incidents rise, security spending falls:*** Information security spending is not keeping pace with increases in the frequency and costs of security incidents, despite elevated concerns about cyber risks. In fact, investments in information security budgets declined 4% over 2013.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Impacts: General impacts of security incidents

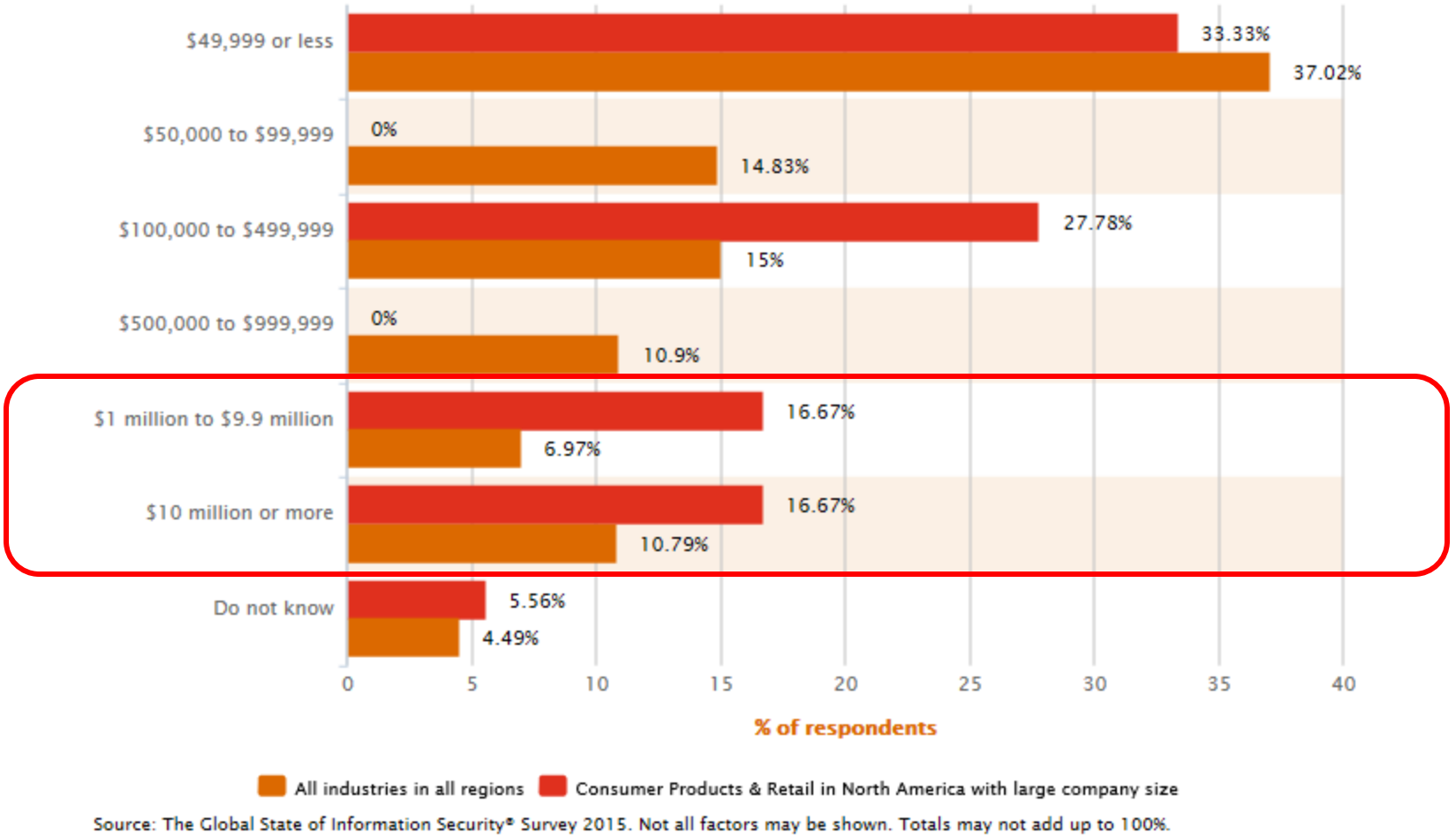


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Impacts: Estimated financial losses due to security incidents

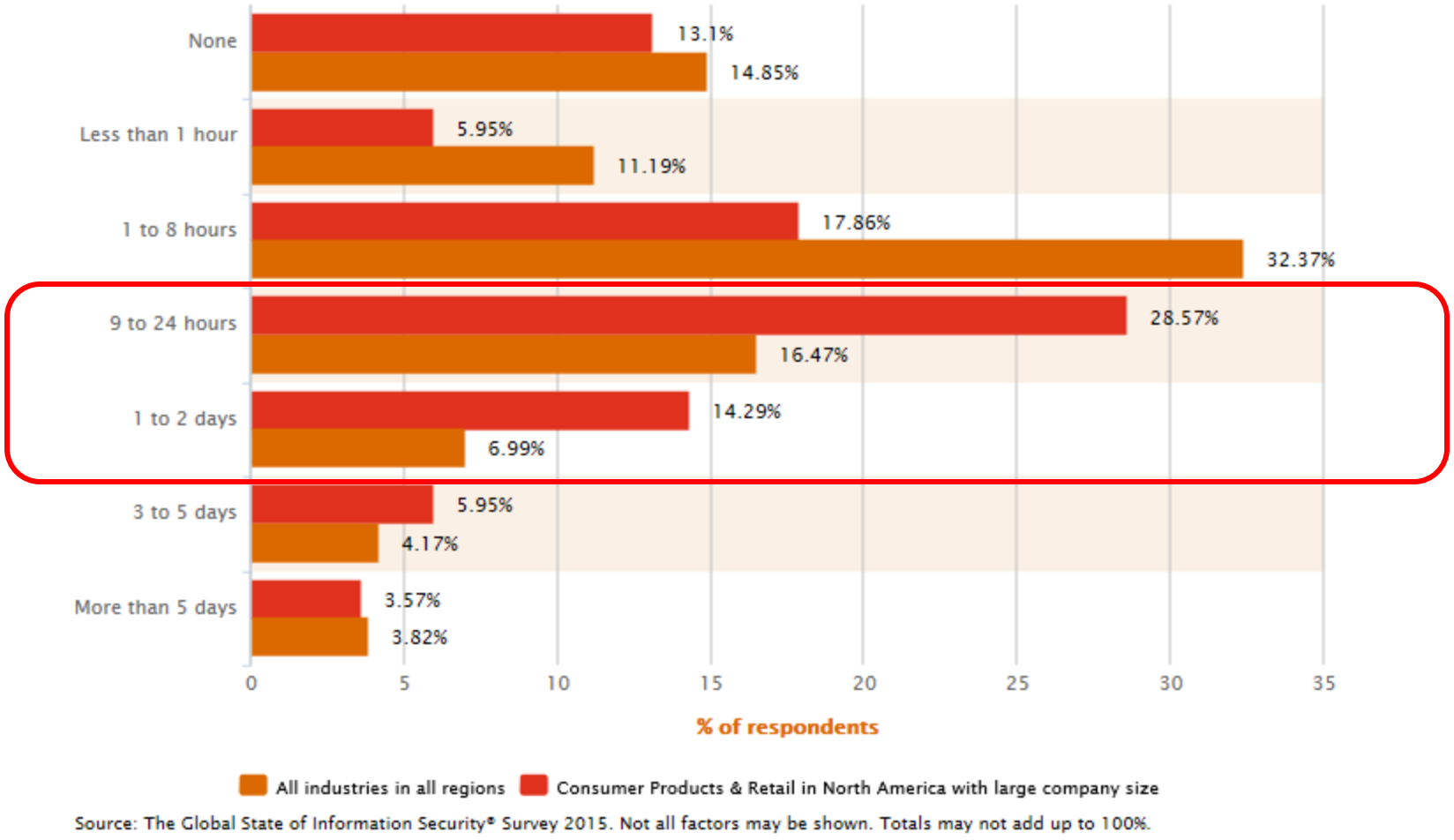


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Impacts: Total downtime over past 12 months due to security incidents

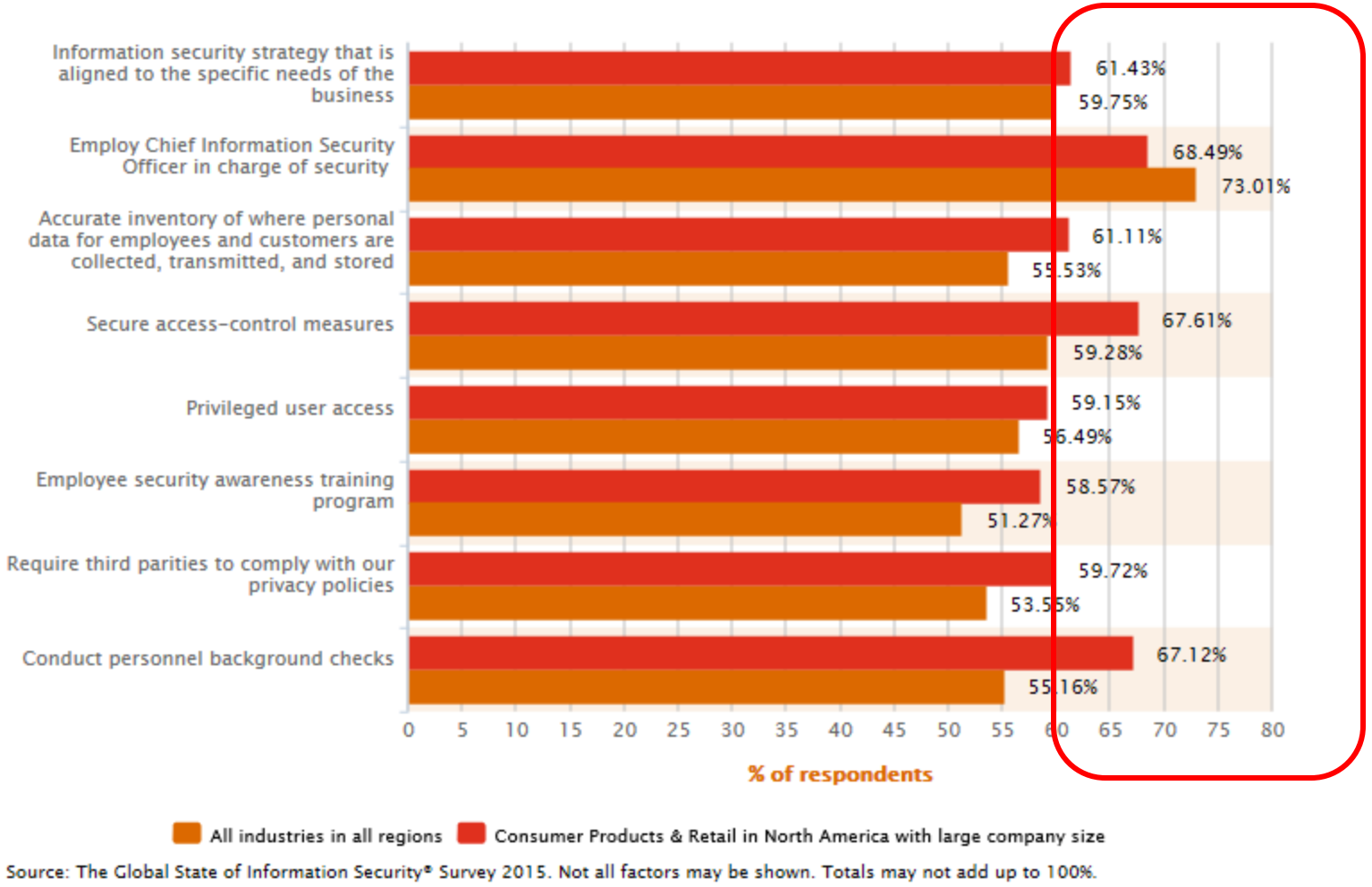


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Safeguards: Preventative measures in place

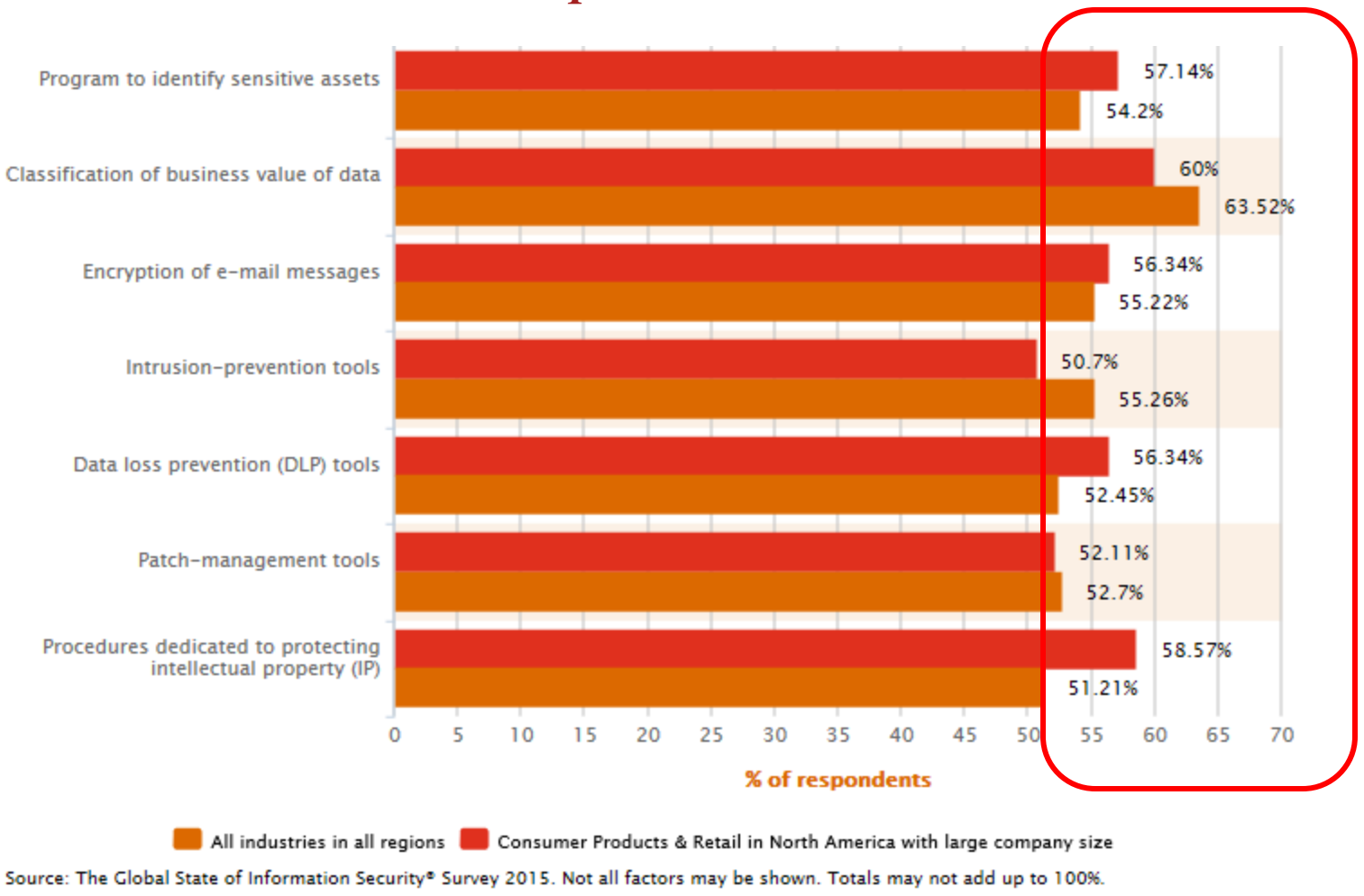


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Safeguards: Preventative measures in place

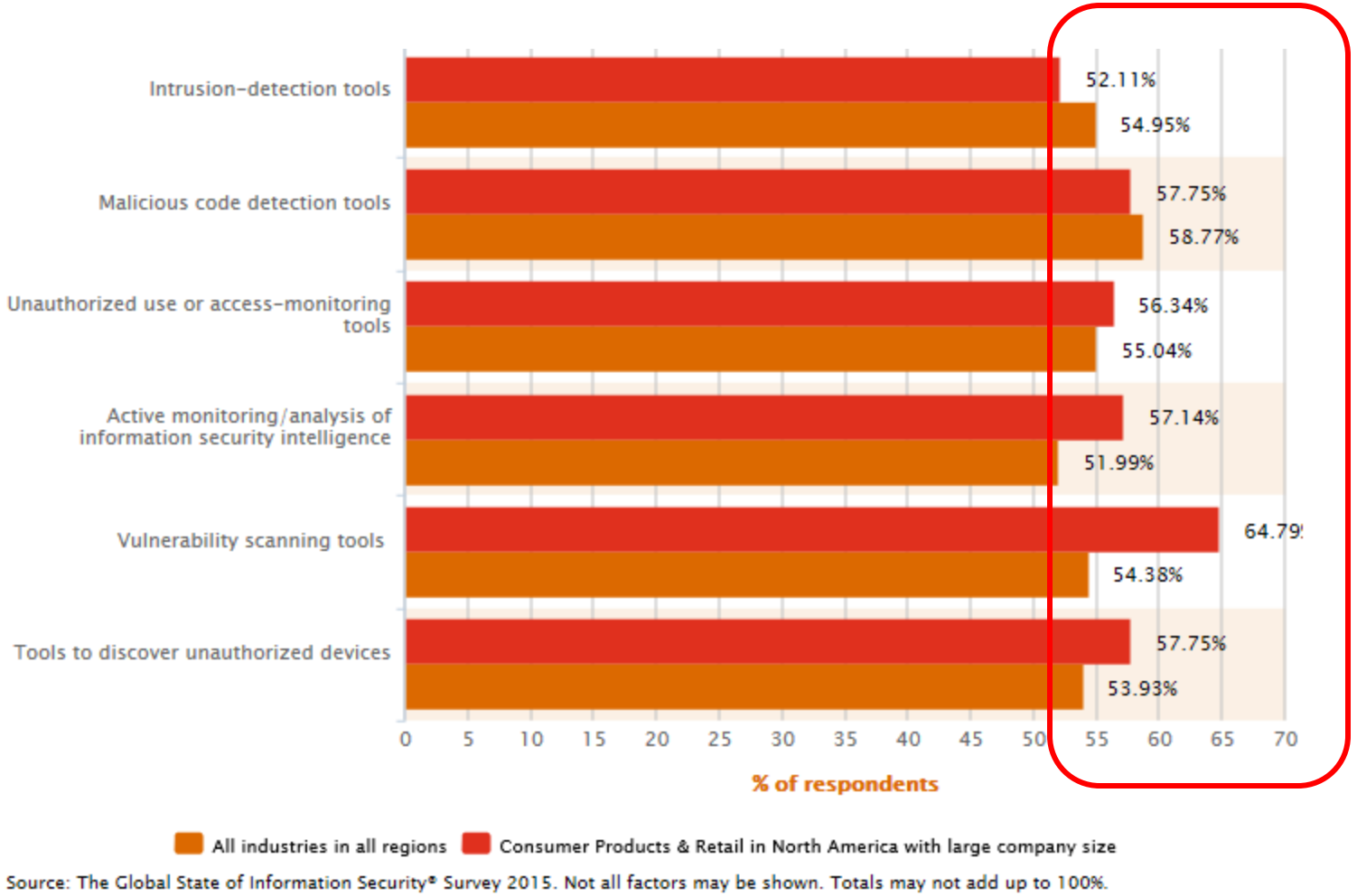


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Safeguards: Detective measures in place

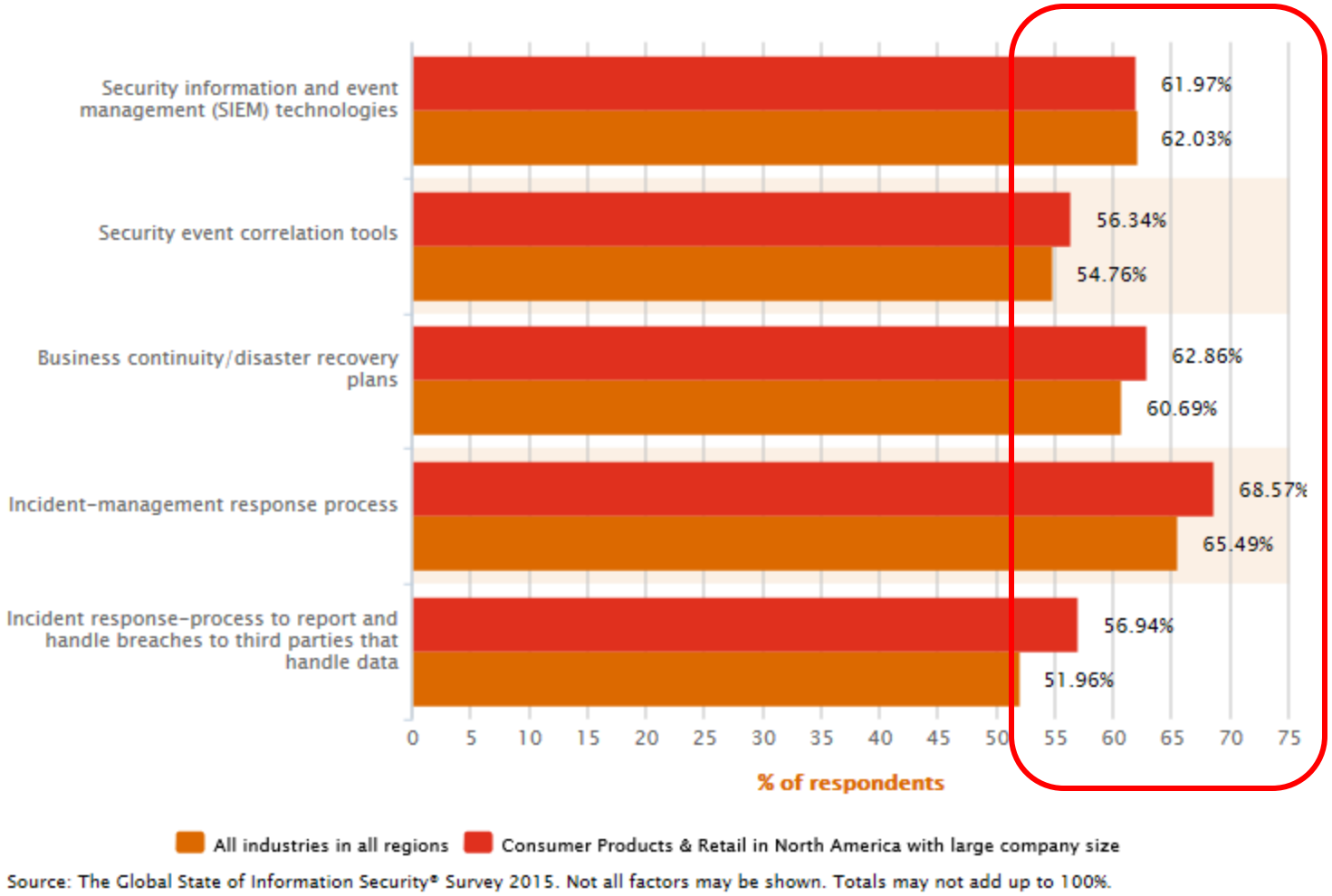


Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

GSISS 2015 - Snapshot of Consumer and Retail Segment

Safeguards: Response measures in place



Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Survey Says…

Nearly 7 in 10 respondents viewed cyberattacks and other security threats as a high or critical priority.

More than half of the chief audit executives (CAEs) and directors who responded consider the identification of emerging risks to be their biggest challenge. Yet only about one-third expressed a high degree of confidence in their ability to identify such concerns.

- The IIA Audit Executive Center's North American Pulse of Internal Audit survey (2014)

CEOs see cyber security technologies as a top-three most strategically important type of digital technology for their organization. And 53% think it's 'very important' strategically – a higher proportion than for any other type of digital technology we asked about.

- 18th Annual Global CEO Survey –PwC (2015)

Internal Audit's critical role in cybersecurity

IA provides a critical line of defense in providing assurance to the board and executive management that company information security practices aren't becoming inadequate and obsolete. However, there are four typical barriers we find to internal audit playing an effective role in security:

1. ***Apathy - A mindset that believes adequate controls are already in place - "We have firewalls, we do SOX and we comply with PCI".*** The fact is that many disastrous security breaches have occurred in companies that had strong firewalls, seemingly tight access controls, and in compliance with regulation. Since exposures are changing constantly, policies and controls need to change alongside them.

2. ***Budgets - Management considers the money and effort to build and maintain Information Security assurance programs too high.*** Often leaders don't realize the magnitude of the potential downside.

3. ***Competence - Many audit committees and top management view the IA function as competent in assessing financial controls and sometimes information security controls, but often do not trust their ability to assess information security holistically.*** IA departments need to have the right people – either hire and train in this area or outsource as needed to experts.

4. ***Distributed responsibilities - Often split between various functional groups within IT. When that happens, it's almost certain that some things will fall through the cracks.*** Auditing across functional groups is *hard*...make sure someone is responsible, has access to the right resources to assess the risks, and the authority to address them.

Food for Thought

The National Association of Corporate Directors (NACD), in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA), published a report outlining the five principles that all corporate boards should consider "as they seek to enhance their oversight of cyber risks." The first principle is:

> ***Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.***

The NACD then made the following recommendation:

> **The board must assume the role of the fourth line of defense against cyber risks within the entire organization. In this capacity, the board must require internal audit to provide an annual "health check" report of the organization's cybersecurity program. This comprehensive report must cover all domains of the cybersecurity and be conducted by either the internal audit staff or an external security organization.**

The Model

Maturity Model – Cybersecurity Audit Coverage

	Less Mature		**Maturity Level**		More Mature
	1	**2**	**3**	**4**	**5**
Risk Identification	No, or limited understanding of Firm-wide or business segment and/or function Information Security (IS)risks	Business segment or function risks are known, but neither well documented or aggregated	Business segment or functional risks are documented, but outdated and with limited aggregation	Business segment and/or function risks are documented, periodically refreshed with some aggregation	A well-documented, firm wide view of risk exists and is periodically refreshed
Audit Universe	No IS specific entities are defined and no ITGC testing is performed	No IS specific entities are defined, however, limited ITGC testing is performed	A single IS related Audit Entity has been defined, but there is lack of clarity as to which IT processes are included. Well defined ITGC testing regime exists	There is some differentiation between IS related Audit Entities and clarity exists regarding which processes are included. Audit Entities are aligned to IT/IS functions rather than	There is a logical set of IS related Audit entities which are tied to a recognized controls framework, providing clarity regarding included processes and comprehensive coverage
Risk Assessment	No formal assessment of IS risk is performed	Assessment of IS risk is included as part of general IT risk assessment	IS Risk is assessed, but only at a broad level and based on inconsistent measures. Some consideration of IS risk occurs for non IT Audit Entities	IS risk is formally and consistently assessed from year to year, but risks may not be adequately mapped to the audit universe. Formal consideration of IS risk for non IT Audit Entities occurs	IS risk is mapped to well defined audit entities, performed with consistent measures and considers both business segment/functional and aggregate firm risk
Coverage Strategy	No discernable coverage strategy or pattern exists	IS coverage is included in ITGC application audit testing	Basic coverage is determined based on IS risk assessment, with higher risk processes receiving priority treatment	A coverage strategy is developed based on a risk informed multi-year cycle… or risk based with no cycle. A continuous monitoring program may exist	A robust coverage strategy exists, which includes risk informed prioritization of coverage and a formal monitoring program
Engagement Test Strategy	No discernable testing strategy or tie-in to a controls framework exists	A basic test strategy is formulated, but based more on staff skill set than risk	A risk based test strategy is developed, but not balanced, focusing either on program level processes or lower level	A balanced, risk based test strategy is developed based on a recognized framework and performed by competent	Test strategy remains balanced and framework based, but high/critical risk process testing is supported by SMEs

Risk Identification

	Less Mature	**Maturity Level**			More Mature
	1	**2**	**3**	**4**	**5**
Risk Identification	No, or limited understanding of Firm-wide or business segment and/or function Information Security (IS)risks	Business segment or function risks are known, but neither well documented or aggregated	Business segment or functional risks are documented, but outdated and with limited aggregation	Business segment and/or function risks are documented, periodically refreshed with some aggregation	A well-documented, firm wide view of risk exists and is periodically refreshed

Audit Universe

	Less Mature — Maturity Level — More Mature				
	1	**2**	**3**	**4**	**5**
Audit Universe	No IS specific entities are defined and no ITGC testing is performed	No IS specific entities are defined, however, limited ITGC testing is performed	A single IS related Audit Entity has been defined, but there is lack of clarity as to which IT processes are included. Well defined ITGC testing regime exists	There is some differentiation between IS related Audit Entities and clarity exists regarding which processes are included. Audit Entities are aligned to IT/IS functions rather than	There is a logical set of IS related Audit entities which are tied to a recognized controls framework, providing clarity regarding included processes and comprehensive coverage

Risk Assessment

	Less Mature	Maturity Level			More Mature
	1	**2**	**3**	**4**	**5**
Risk Assessment	No formal assessment of IS risk is performed	Assessment of IS risk is included as part of general IT risk assessment	IS Risk is assessed, but only at a broad level and based on inconsistent measures. Some consideration of IS risk occurs for non IT Audit Entities	IS risk is formally and consistently assessed from year to year, but risks may not be adequately mapped to the audit universe. Formal consideration of IS risk for non IT Audit Entities occurs	IS risk is mapped to well defined audit entities, performed with consistent measures and considers both business segment/functional and aggregate firm risk

Coverage Strategy

	Less Mature	Maturity Level			More Mature
	1	**2**	**3**	**4**	**5**
Coverage Strategy	No discernable coverage strategy or pattern exists	IS coverage is included in ITGC application audit testing	Basic coverage is determined based on IS risk assessment, with higher risk processes receiving priority treatment	A coverage strategy is developed based on a risk informed multi-year cycle… or risk based with no cycle. A continuous monitoring program may exist	A robust coverage strategy exists, which includes risk informed prioritization of coverage and a formal monitoring program

Engagement Test Strategy

	Less Mature	Maturity Level			More Mature
	1	**2**	**3**	**4**	**5**
Engagement Test Strategy	No discernable testing strategy or tie-in to a controls framework exists	A basic test strategy is formulated, but based more on staff skill set than risk	A risk based test strategy is developed, but not balanced, focusing either on program level processes or lower level controls	A balanced, risk based test strategy is developed based on a recognized framework and performed by competent internal staff	Test strategy remains balanced and framework based, but high/critical risk process testing is supported by subject matter experts

Level One

	Less Mature	**Maturity Level**			More Mature
	1	**2**	**3**	**4**	**5**
Risk Identification	No, or limited understanding of Firm-wide or business segment and/or function Information Security (IS)risks				
Audit Universe	No IS specific entities are defined and no ITGC testing is performed				
Risk Assessment	No formal assessment of IS risk is performed				
Coverage Strategy	No discernable coverage strategy or pattern exists				
Engagement Test Strategy	No discernable testing strategy or tie-in to a controls framework exists				

Level Two

	Less Mature	Maturity Level			More Mature
	1	2	3	4	5
Risk Identification		Business segment or function risks are known, but neither well documented or aggregated			
Audit Universe		No IS specific entities are defined, however, limited ITGC testing is performed			
Risk Assessment		Assessment of IS risk is included as part of general IT risk assessment			
Coverage Strategy		IS coverage is included in ITGC application audit testing			
Engagement Test Strategy		A basic test strategy is formulated, but based more on staff skill set than risk			

Level Three

	Less Mature		Maturity Level		More Mature
	1	2	3	4	5
Risk Identification			Business segment or functional risks are documented, but outdated and with limited aggregation		
Audit Universe			A single IS related Audit Entity has been defined, but there is lack of clarity as to which IT processes are included. Well defined ITGC testing regime exists		
Risk Assessment			IS Risk is assessed, but only at a broad level and based on inconsistent measures. Some consideration of IS risk occurs for non IT Audit Entities		
Coverage Strategy			Basic coverage is determined based on IS risk assessment, with higher risk processes receiving priority treatment		
Engagement Test Strategy			A risk based test strategy is developed, but not balanced, focusing either on program level processes or lower level controls		

Level Four

	Less Mature		Maturity Level		More Mature
	1	2	3	4	5
Risk Identification				Business segment and/or function risks are documented, periodically refreshed with some aggregation	
Audit Universe				There is some differentiation between IS related Audit Entities and clarity exists regarding which processes are included. Audit Entities are aligned to IT/IS functions rather than	
Risk Assessment				IS risk is formally and consistently assessed from year to year, but risks may not be adequately mapped to the audit universe. Formal consideration of IS risk for non IT Audit Entities occurs	
Coverage Strategy				A coverage strategy is developed based on a risk informed multi-year cycle… or risk based with no cycle. A continuous monitoring program may exist	
Engagement Test Strategy				A balanced, risk based test strategy is developed based on a recognized framework and performed by competent internal staff	

Level Five

	Less Mature		Maturity Level		More Mature
	1	2	3	4	5
Risk Identification					A well-documented, firm wide view of risk exists and is periodically refreshed
Audit Universe					There is a logical set of IS related Audit entities which are tied to a recognized controls framework, providing clarity regarding included processes and comprehensive coverage
Risk Assessment					IS risk is mapped to well defined audit entities, performed with consistent measures and considers both business segment/functional and aggregate firm risk
Coverage Strategy					A robust coverage strategy exists, which includes risk informed prioritization of coverage and a formal monitoring program
Engagement Test Strategy					Test strategy remains balanced and framework based, but high/critical risk process testing is supported by subject matter experts

Moving the Dial

	Less Mature		Maturity Level		More Mature
	1	**2**	**3**	**4**	**5**
Risk Identification	No, or limited understanding of Firm-wide or business segment and/or function Information Security (IS)risks	Business segment or function risks are known, but neither well documented or aggregated	Business segment or functional risks are documented, but outdated and with limited aggregation	Business segment and/or function risks are documented, periodically refreshed with some aggregation	A well-documented, firm wide view of risk exists and is periodically refreshed
Audit Universe	No IS specific entities are defined and no ITGC testing is performed	No IS specific entities are defined, however, limited ITGC testing is performed	A single IS related Audit Entity has been defined, but there is lack of clarity as to which IT processes are included. Well defined ITGC testing regime exists	There is some differentiation between IS related Audit Entities and clarity exists regarding which processes are included. Audit Entities are aligned to IT/IS functions rather than	There is a logical set of IS related Audit entities which are tied to a recognized controls framework, providing clarity regarding included processes and comprehensive coverage
Risk Assessment	No formal assessment of IS risk is performed	Assessment of IS risk is included as part of general IT risk assessment	IS Risk is assessed, but only at a broad level and based on inconsistent measures. Some consideration of IS risk occurs for non IT Audit Entities	IS risk is formally and consistently assessed from year to year, but risks may not be adequately mapped to the audit universe. Formal consideration of IS risk for non IT Audit Entities occurs	IS risk is mapped to well defined audit entities, performed with consistent measures and considers both business segment/functional and aggregate firm risk
Coverage Strategy	No discernable coverage strategy or pattern exists	IS coverage is included in ITGC application audit testing	Basic coverage is determined based on IS risk assessment, with higher risk processes receiving priority treatment	A coverage strategy is developed based on a risk informed multi-year cycle… or risk based with no cycle. A continuous monitoring program may exist	A robust coverage strategy exists, which includes risk informed prioritization of coverage and a formal monitoring program
Engagement Test Strategy	No discernable testing strategy or tie-in to a controls framework exists	A basic test strategy is formulated, but based more on staff skill set than risk	A risk based test strategy is developed, but not balanced, focusing either on program level processes or lower level	A balanced, risk based test strategy is developed based on a recognized framework and performed by competent	Test strategy remains balanced and framework based, but high/critical risk process testing is supported by SMEs

Moving the Dial

	Less Mature		Maturity Level		More Mature
	1	**2**	**3**	**4**	**5**
Risk Identification	No, or limited understanding of Firm-wide or business segment and/or function Information Security (IS)risks	Business segment or function risks are known, but neither well documented or aggregated	Business segment or functional risks are documented, but outdated and with limited aggregation	Business segment and/or function risks are documented, periodically refreshed with some aggregation	A well-documented, firm wide view of risk exists and is periodically refreshed
Audit Universe	No IS specific entities are defined and no ITGC testing is performed	No IS specific entities are defined, however, limited ITGC testing is performed	A single IS related Audit Entity has been defined, but there is lack of clarity as to which IT processes are included. Well defined ITGC testing regime exists	There is some differentiation between IS related Audit Entities and clarity exists regarding which processes are included. Audit Entities are aligned to IT/IS functions rather than	There is a logical set of IS related Audit entities which are tied to a recognized controls framework, providing clarity regarding included processes and comprehensive coverage
Risk Assessment	No formal assessment of IS risk is performed	Assessment of IS risk is included as part of general IT risk assessment	IS Risk is assessed, but only at a broad level and based on inconsistent measures. Some consideration of IS risk occurs for non IT Audit Entities	IS risk is formally and consistently assessed from year to year, but risks may not be adequately mapped to the audit universe. Formal consideration of IS risk for non IT Audit Entities occurs	IS risk is mapped to well defined audit entities, performed with consistent measures and considers both business segment/functional and aggregate firm risk
Coverage Strategy	No discernable coverage strategy or pattern exists	IS coverage is included in ITGC application audit testing	Basic coverage is determined based on IS risk assessment, with higher risk processes receiving priority treatment	A coverage strategy is developed based on a risk informed multi-year cycle… or risk based with no cycle. A continuous monitoring program may exist	A robust coverage strategy exists, which includes risk informed prioritization of coverage and a formal monitoring program
Engagement Test Strategy	No discernable testing strategy or tie-in to a controls framework exists	A basic test strategy is formulated, but based more on staff skill set than risk	A risk based test strategy is developed, but not balanced, focusing either on program level processes or lower level	A balanced, risk based test strategy is developed based on a recognized framework and performed by competent	Test strategy remains balanced and framework based, but high/critical risk process testing is supported by SMEs

Moving the Dial

Risk Identification:

Let business risk help drive how you approach cybersecurity

Moving the Dial

Audit Universe:

Know in detail what processes are included in Audit Entities

Moving the Dial

Risk Assessment:

Look for cyber related risks outside of traditional IT Audit Entities

Moving the Dial

Coverage Strategy:

Don't be afraid of auditing a process across multiple functions

Bonus!!!

– Identify/track a couple key cybersecurity metrics

Moving the Dial

Engagement Test Strategy:

Don't shirk going deep on the technical testing

Bonus!!!

– Don't be afraid of auditing the CISO's strategy

Thank You!