CONSIDERING CLOUD? LEARN ABOUT CURRENT TRENDS IN CLOUD COMPUTING

Security in knowledge

Jeff Jones (jrjones@microsoft.com)
Microsoft – Trustworthy Computing

Frank Simorjay (frasim@microsoft.com)
Microsoft – Trustworthy Computing

RSA CONFERENCE EUROPE 2013

Session ID: ARCH-W08

Session Classification: Intermediate

Who are these guys?

Company

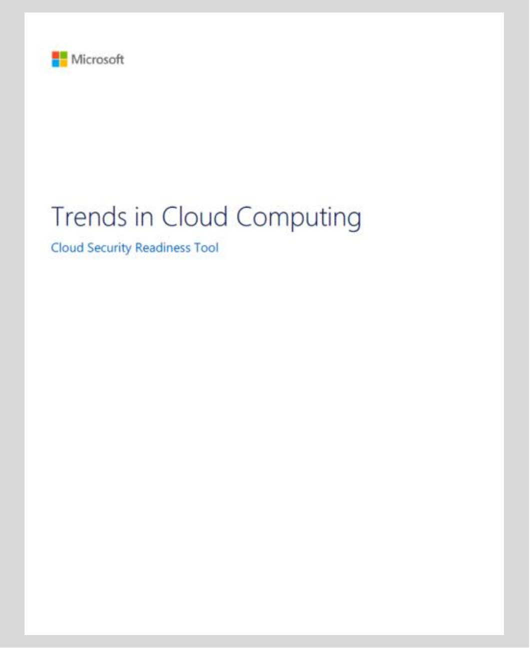
- Microsoft Corporation
- Trustworthy Computing group

Jeff Jones

- Director, Trustworthy Computing
- 25-year Security Guy : DoD, TIS, McAfee, PGP, MSFT
- Microsoft Security Blog & Trustworthy Computing Blog
- @securityjones

Frank Simorjay

- Sr. Product Manager, Trustworthy Computing
- Author and designer of CSRT, OSA paper many others
- Work extensively with community -ISSA Distinguished Fellow
- Worked at NFR (small world – Jeff and I both worked with Marcus)



Microsoft

Trends in Cloud Computing

Cloud Security Readiness Tool

Trustworthy Computing

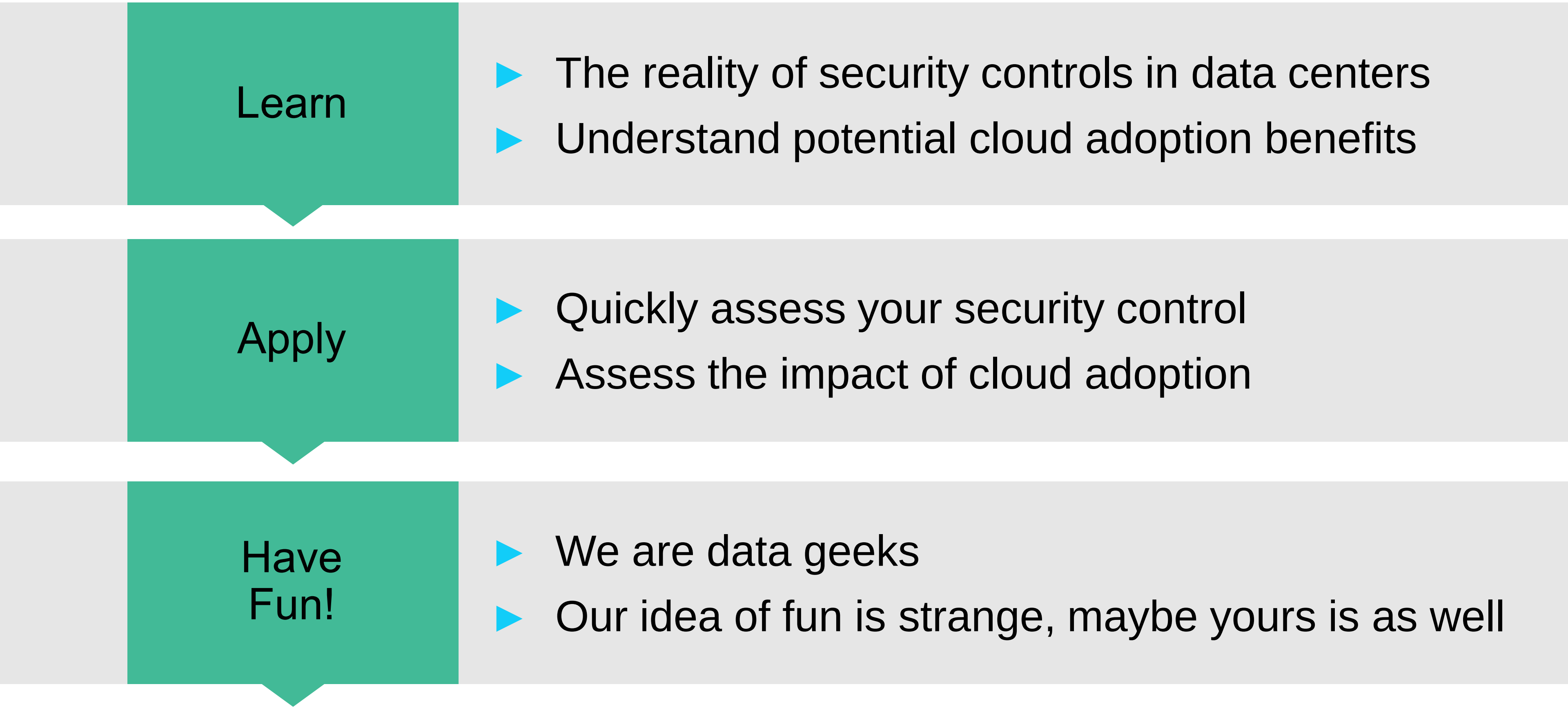
🔒 Security

Privacy

Reliability

Creating and delivering secure, private and reliable computing experiences

Session Objectives



Learn

- The reality of security controls in data centers
- Understand potential cloud adoption benefits

Apply

- Quickly assess your security control
- Assess the impact of cloud adoption

Have Fun!

- We are data geeks
- Our idea of fun is strange, maybe yours is as well

What You Will Hear Today

Background on cloud computing

The cloud security Readiness Tool

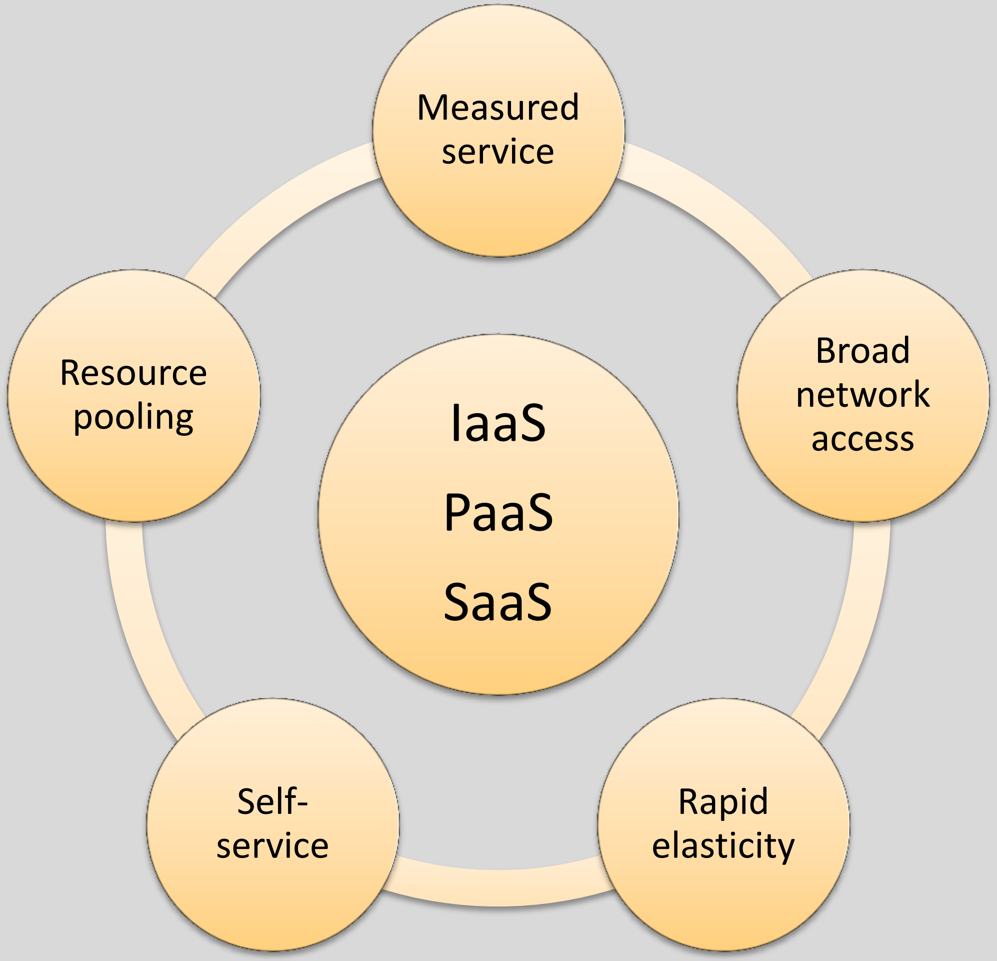
Cloud trends

Applying it

Q&A

Overview

What is cloud computing



Measured service

Broad network access

Rapid elasticity

Self-service

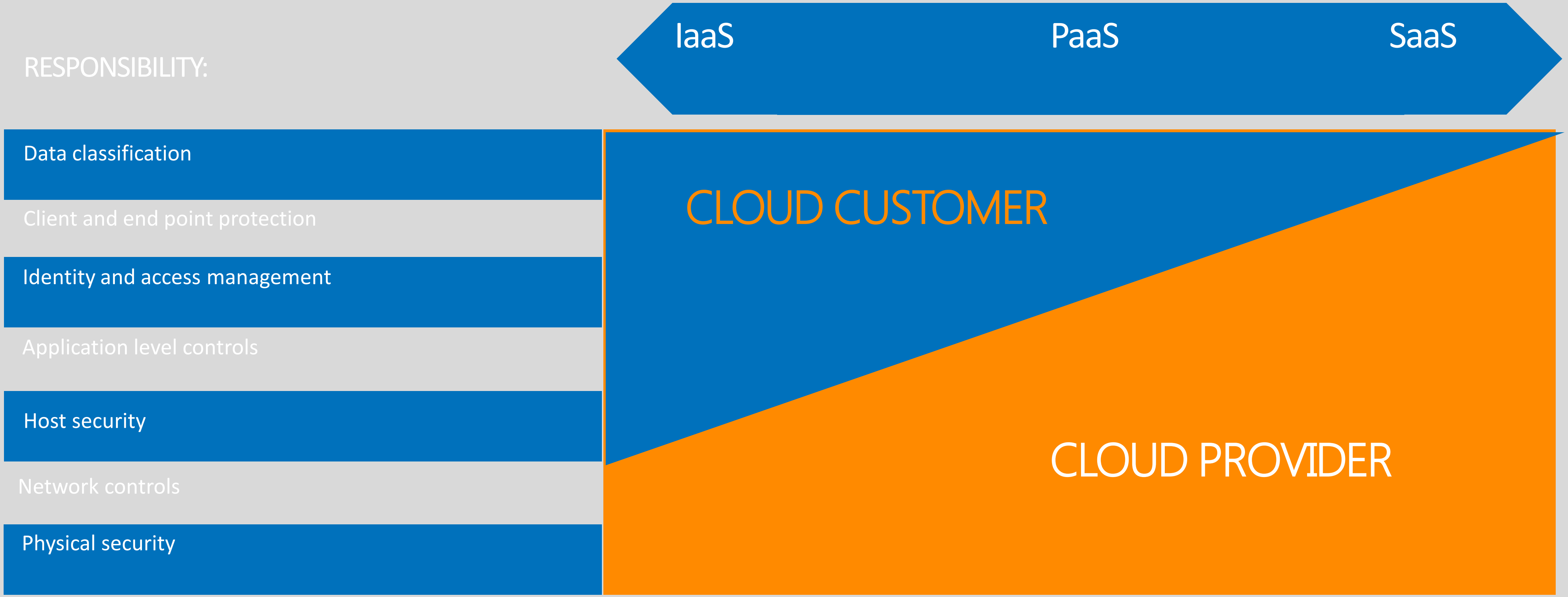
Resource pooling

IaaS

PaaS

SaaS

Provider is your partner



RESPONSIBILITY:

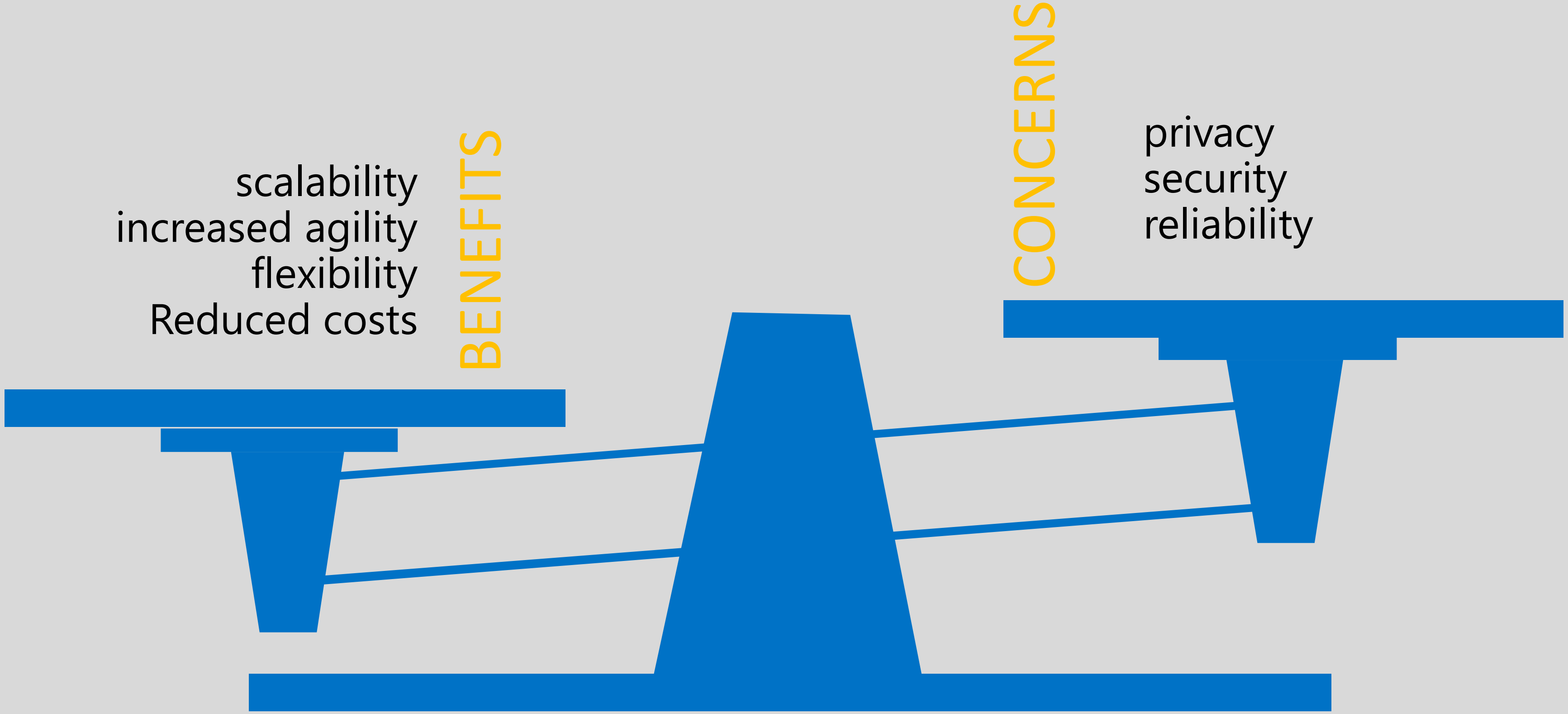
- Data classification
- Client and end point protection
- Identity and access management
- Application level controls
- Host security
- Network controls
- Physical security

IaaS PaaS SaaS

CLOUD CUSTOMER

CLOUD PROVIDER

Risks and rewards of adoption



BENEFITS

scalability
increased agility
flexibility
Reduced costs

CONCERNS

privacy
security
reliability

Study done in 2012:

Most Individuals confused by cloud computing

51% of respondents, believe stormy weather can interfere with cloud computing.

54% of respondents claim to never use cloud computing.

97% are actually using cloud services today via online shopping, banking, social networking and file sharing.

Microsoft Cloud Security Readiness Tool

www.micrsoft.com/trustedcloud

#RSAC

RSACONFERENCE EUROPE 2013

Problems you face

What are your current IT capabilities?

Can you improve your people, processes, and technologies?

Can cloud reduce your risks while reducing cost?

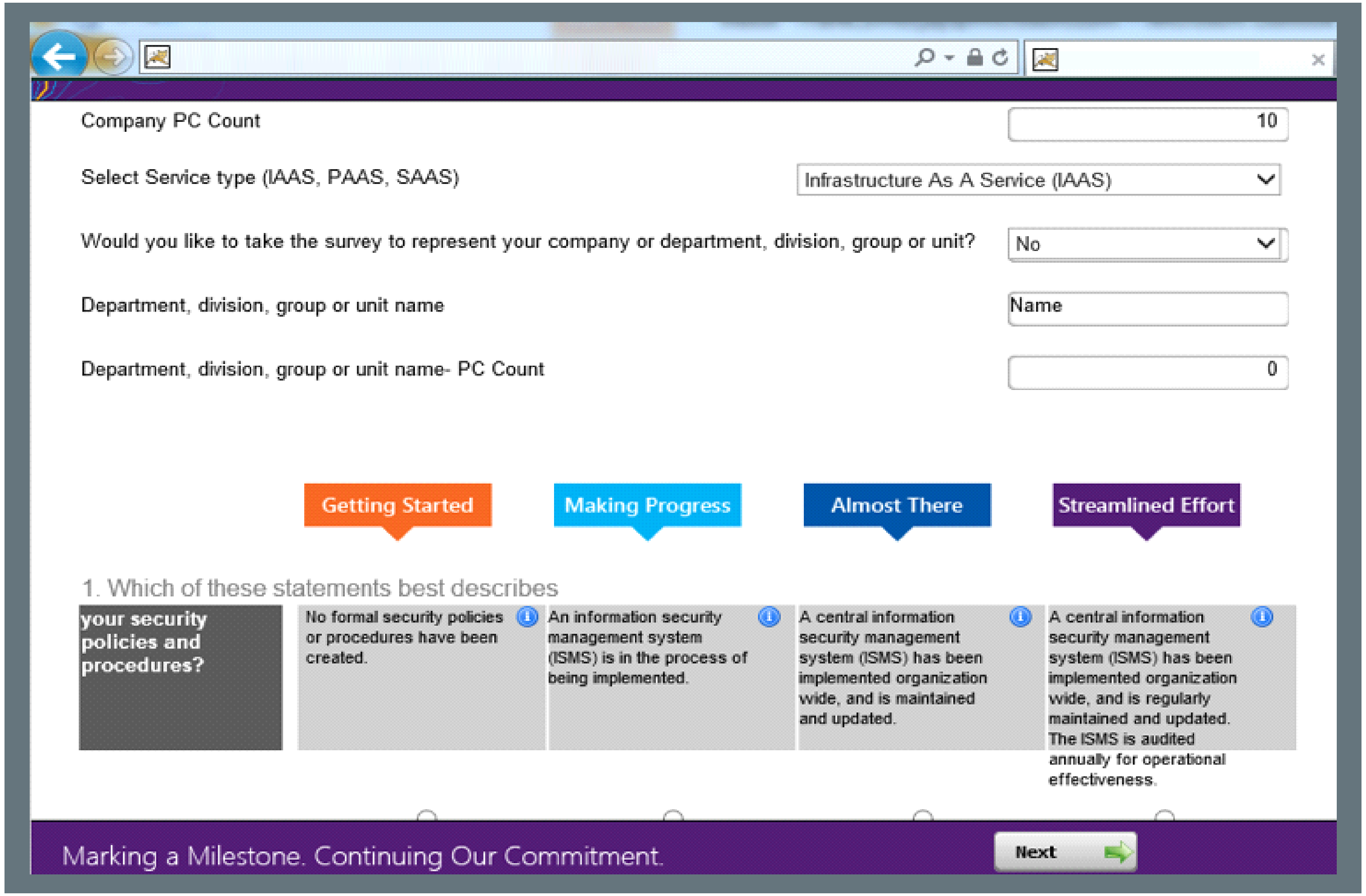
Cloud Security Alliance (CSA)

Global not-for-profit organization

Provider, and User Certification

Accepted global authority for trust in the cloud

Cloud Security Readiness Tool



Company PC Count	10
Select Service type (IAAS, PAAS, SAAS)	Infrastructure As A Service (IAAS)
Would you like to take the survey to represent your company or department, division, group or unit?	No
Department, division, group or unit name	Name
Department, division, group or unit name- PC Count	0

1. Which of these statements best describes your security policies and procedures?	Getting Started	Making Progress	Almost There	Streamlined Effort
	No formal security policies or procedures have been created.	An information security management system (ISMS) is in the process of being implemented.	A central information security management system (ISMS) has been implemented organization wide, and is maintained and updated.	A central information security management system (ISMS) has been implemented organization wide, and is regularly maintained and updated. The ISMS is audited annually for operational effectiveness.
	○	○	○	○

Marking a Milestone. Continuing Our Commitment.

Where are we?

Where will we be?

Simplifies

Informs

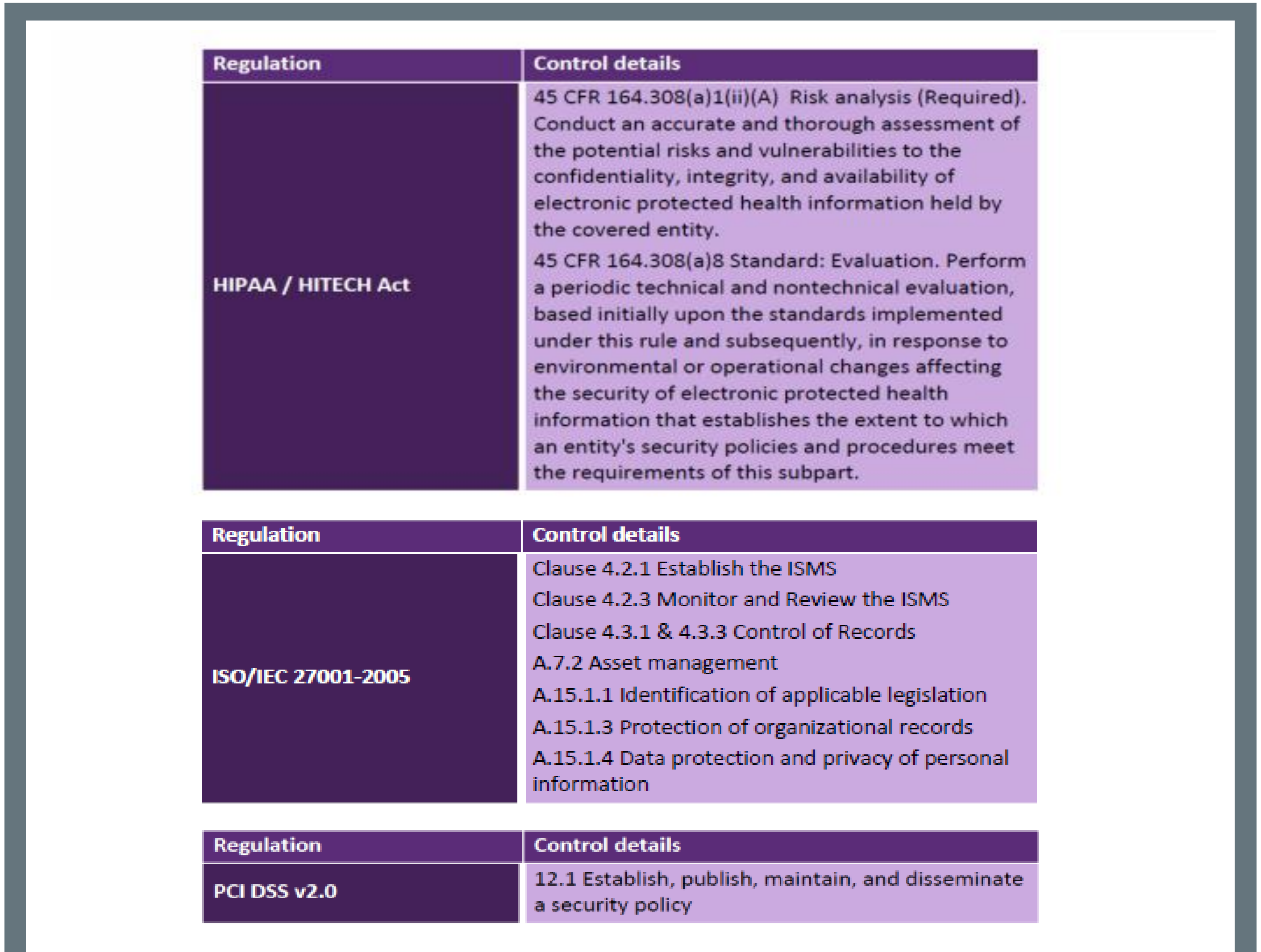
Enables

Agnostic

How it works

Generate Custom Report

- ISO 27001
- ENISA IAF
- HIPAA / HITECH Act
- NIST SP800-53 R3



Regulation	Control details
HIPAA / HITECH Act	45 CFR 164.308(a)1(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. 45 CFR 164.308(a)8 Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Regulation	Control details
ISO/IEC 27001-2005	Clause 4.2.1 Establish the ISMS Clause 4.2.3 Monitor and Review the ISMS Clause 4.3.1 & 4.3.3 Control of Records A.7.2 Asset management A.15.1.1 Identification of applicable legislation A.15.1.3 Protection of organizational records A.15.1.4 Data protection and privacy of personal information

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

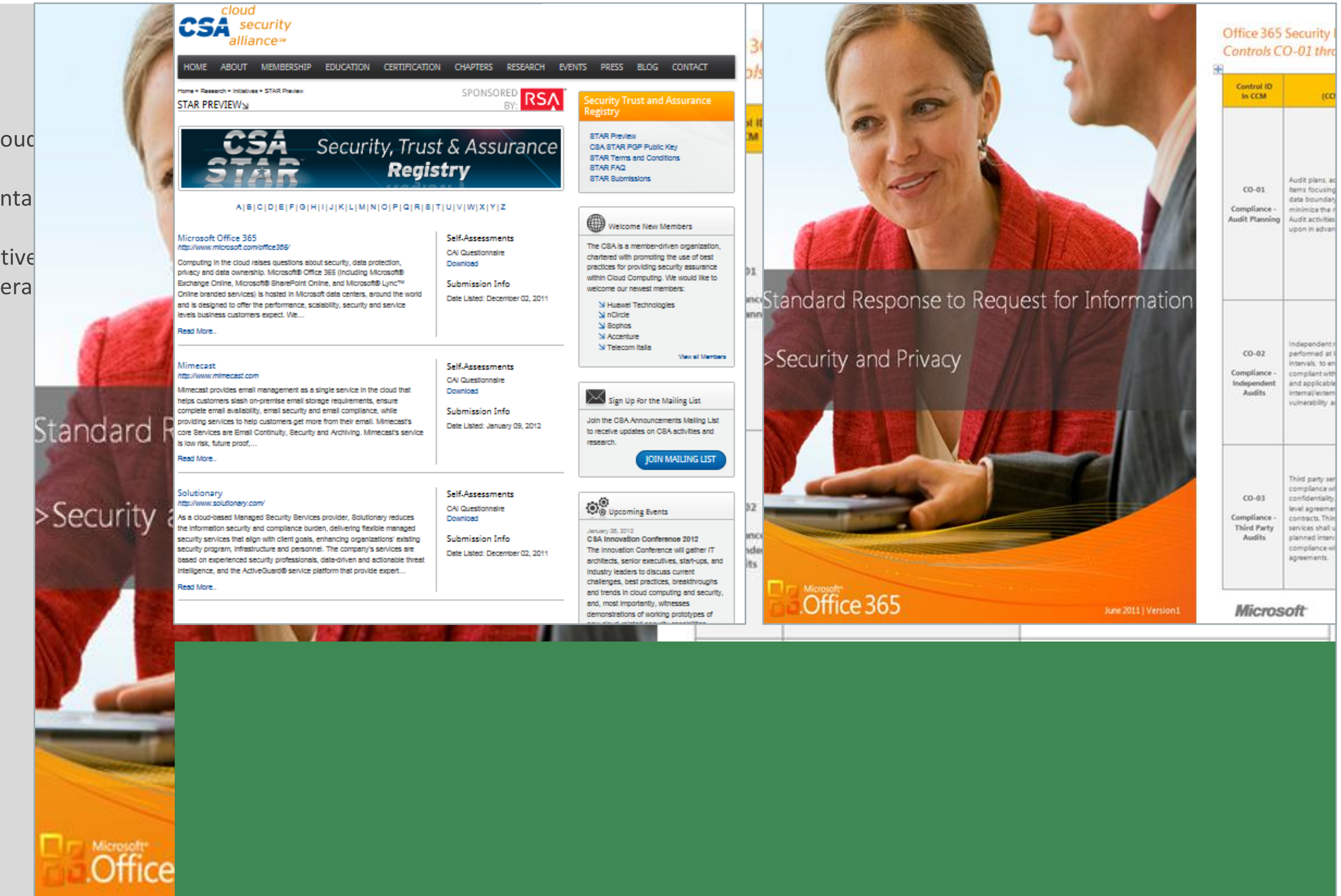
Control /question

security policies and procedures?	employee change/termination process?	security policies and procedures?	capacity planning efforts?
security policies review process?	physical security access method?	staging to production requirements?	selects its data center location(s)?
security program is updated?	equipment support contracts?	application testing using customer data?	redundancy if utility service outages should occur?
personnel background checks?	data classification efforts?	asset inventory program?	patch management processes?
(NDA) requirements?	grants access to data?	conducts risk assessments?	antivirus efforts?
physical access by role?	data retention and recovery program?	responds to an incident ?	firewalls to protect data?
security policies and procedures?	destroys data?	disaster recovery plan?	time setting policies?

CSA Security, Trust & Assurance Registry

Cloud Security Alliance (CSA)

The Cloud Security Alliance Cloud Matrix (CCM) is specifically designed to provide fundamenta principles to guide cloud vendors and to assist prospective customers in assessing the overa risk of a cloud provider.



cloud security alliance℠

HOME ABOUT MEMBERSHIP EDUCATION CERTIFICATION CHAPTERS RESEARCH EVENTS PRESS BLOG CONTACT

Home » Research » Initiatives » STAR Preview

STAR PREVIEW

SPONSORED BY: RSA

CSA STAR Security, Trust & Assurance Registry

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Microsoft Office 365
http://www.microsoft.com/office365/

Computing in the cloud raises questions about security, data protection, privacy and data ownership. Microsoft® Office 365 (including Microsoft® Exchange Online, Microsoft® SharePoint Online, and Microsoft® Lync™ Online branded services) is hosted in Microsoft data centers, around the world and is designed to offer the performance, scalability, security and service levels business customers expect. We...

Read More..

Self-Assessments
CAI Questionnaire
Download

Submission Info
Date Listed: December 02, 2011

Mimecast
http://www.mimecast.com

Mimecast provides email management as a single service in the cloud that helps customers slash on-premise email storage requirements, ensure complete email availability, email security and email compliance, while providing services to help customers get more from their email. Mimecast's core Services are Email Continuity, Security and Archiving. Mimecast's service is low risk, future proof,...

Read More..

Self-Assessments
CAI Questionnaire
Download

Submission Info
Date Listed: January 09, 2012

Solutionary
http://www.solutionary.com/

As a cloud-based Managed Security Services provider, Solutionary reduces the information security and compliance burden, delivering flexible managed security services that align with client goals, enhancing organizations' existing security program, infrastructure and personnel. The company's services are based on experienced security professionals, data-driven and actionable threat intelligence, and the ActiveGuard® service platform that provide expert...

Read More..

Self-Assessments
CAI Questionnaire
Download

Submission Info
Date Listed: December 02, 2011

Security Trust and Assurance Registry

- STAR Preview
- CSA STAR PGP Public Key
- STAR Terms and Conditions
- STAR FAQ
- STAR Submissions

Welcome New Members

The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security assurance within Cloud Computing. We would like to welcome our newest members:

- Huawei Technologies
- nCircle
- Sophos
- Accenture
- Telecom Italia

View all Members

Sign Up for the Mailing List

Join the CSA Announcements Mailing List to receive updates on CSA activities and research.

JOIN MAILING LIST

Upcoming Events

January 25, 2012
CSA Innovation Conference 2012
The Innovation Conference will gather IT architects, senior executives, start-ups, and industry leaders to discuss current challenges, best practices, breakthroughs and trends in cloud computing and security, and, most importantly, witnesses demonstrations of working prototypes of

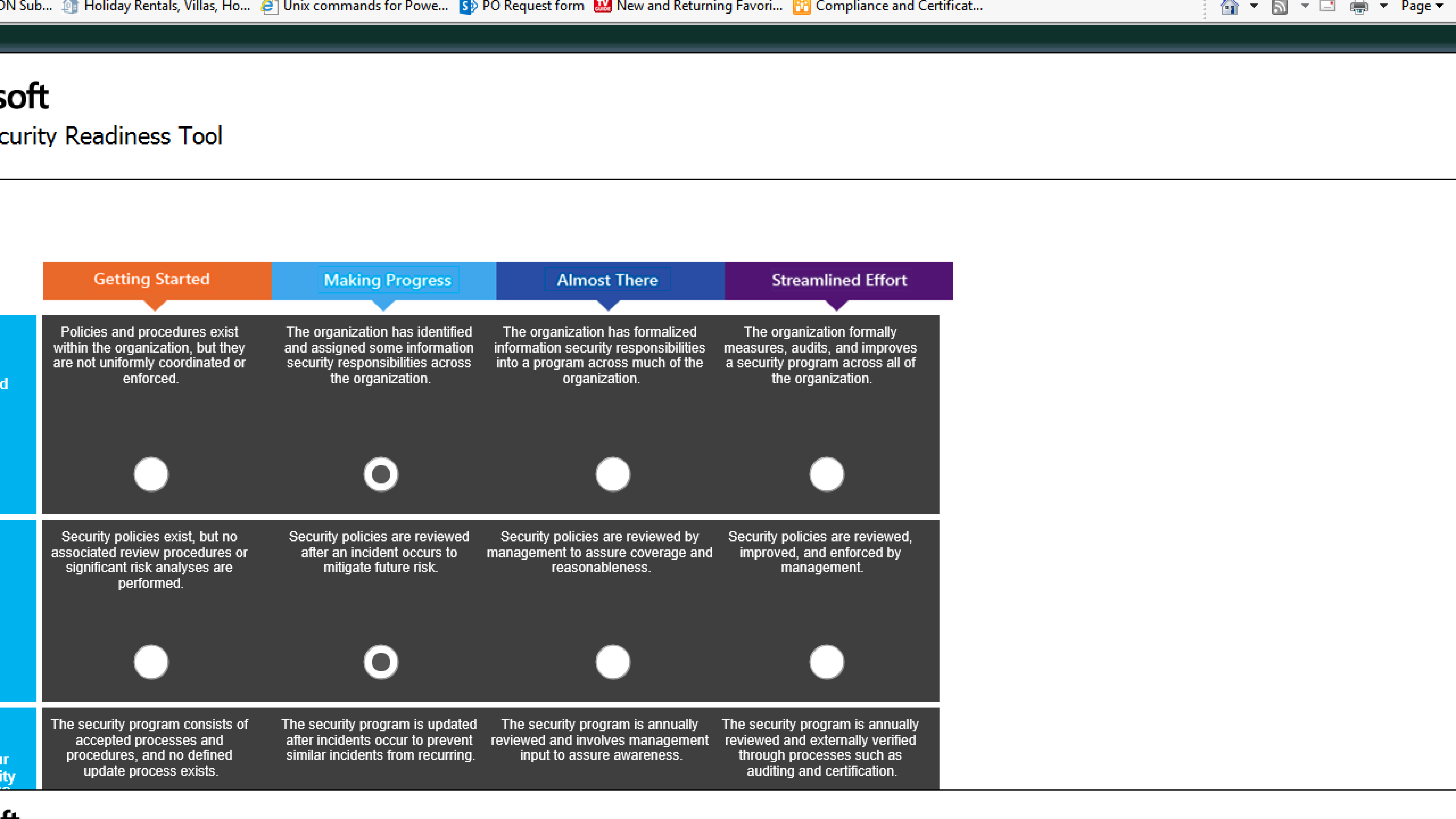
Standard Response to Request for Information
>Security and Privacy
Microsoft Office 365
June 2011 | Version1
Office 365 Security
Controls CO-01 thro
Control ID in CCM
CO-01 Compliance - Audit Planning
CO-02 Compliance - Independent Audits
CO-03 Compliance - Third Party Audits
Microsoft

Microsoft's Standard Responses for STAR

Specific details about Office 365, Windows Azure and Dynamics CRM controls are mapped to the CCM.

Available on Microsoft trust centers.

CSRT Demo


ON Sub...
Holiday Rentals, Villas, Ho...
Unix commands for Powe...
PO Request form
New and Returning Favori...
Compliance and Certificat...
Page

soft

curity Readiness Tool

	Getting Started	Making Progress	Almost There	Streamlined Effort
d	Policies and procedures exist within the organization, but they are not uniformly coordinated or enforced. ○	The organization has identified and assigned some information security responsibilities across the organization. ◉	The organization has formalized information security responsibilities into a program across much of the organization. ○	The organization formally measures, audits, and improves a security program across all of the organization. ○
	Security policies exist, but no associated review procedures or significant risk analyses are performed. ○	Security policies are reviewed after an incident occurs to mitigate future risk. ◉	Security policies are reviewed by management to assure coverage and reasonableness. ○	Security policies are reviewed, improved, and enforced by management. ○
ur ity	The security program consists of accepted processes and procedures, and no defined update process exists.	The security program is updated after incidents occur to prevent similar incidents from recurring.	The security program is annually reviewed and involves management input to assure awareness.	The security program is annually reviewed and externally verified through processes such as auditing and certification.

ft

Cloud Trends

#RSAC

RSA CONFERENCE EUROPE 2013

Trends in cloud computing

Trends in Cloud Computing

Cloud Security Readiness Tool

Cloud Security Readiness Tool (CSRT) data between September 2012 and September 2013.

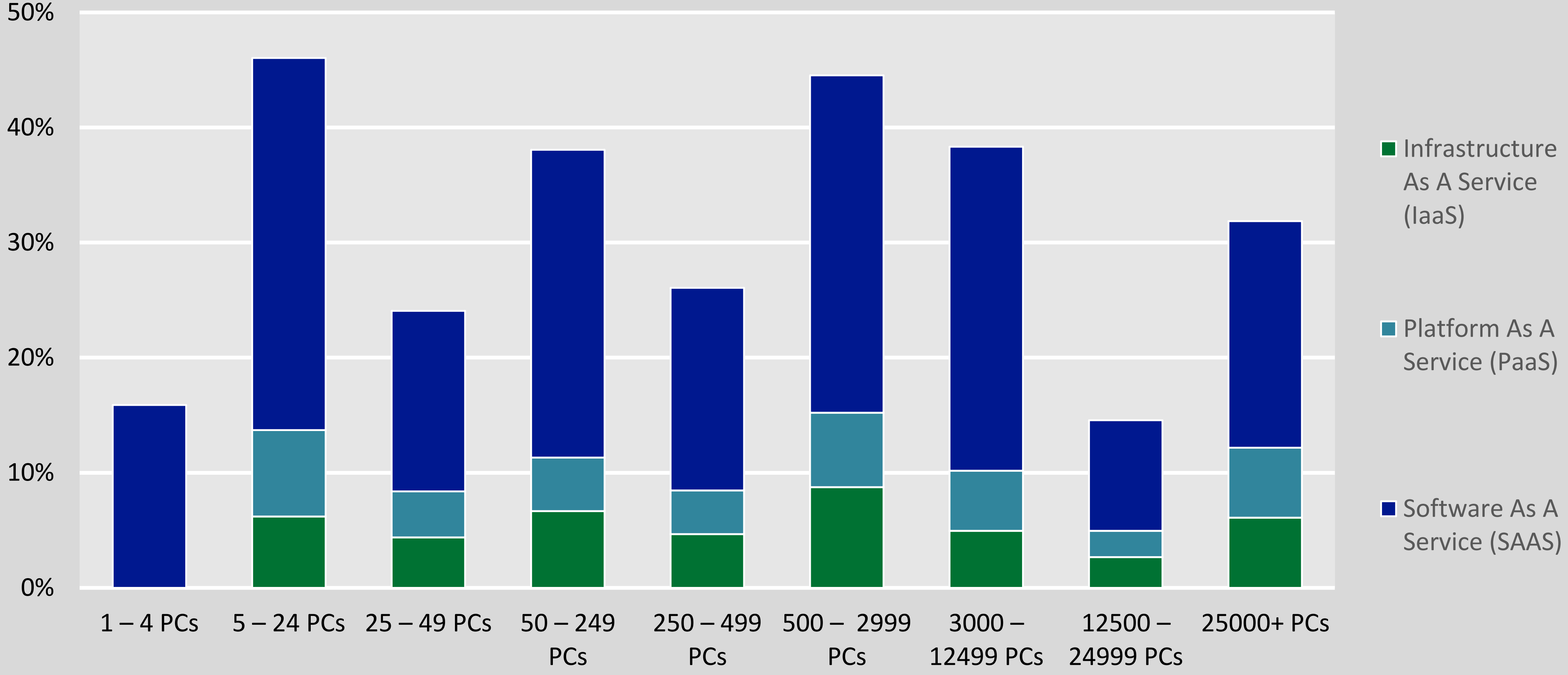
Approximately 10,000 anonymized answers to CSRT questions

Margin of error

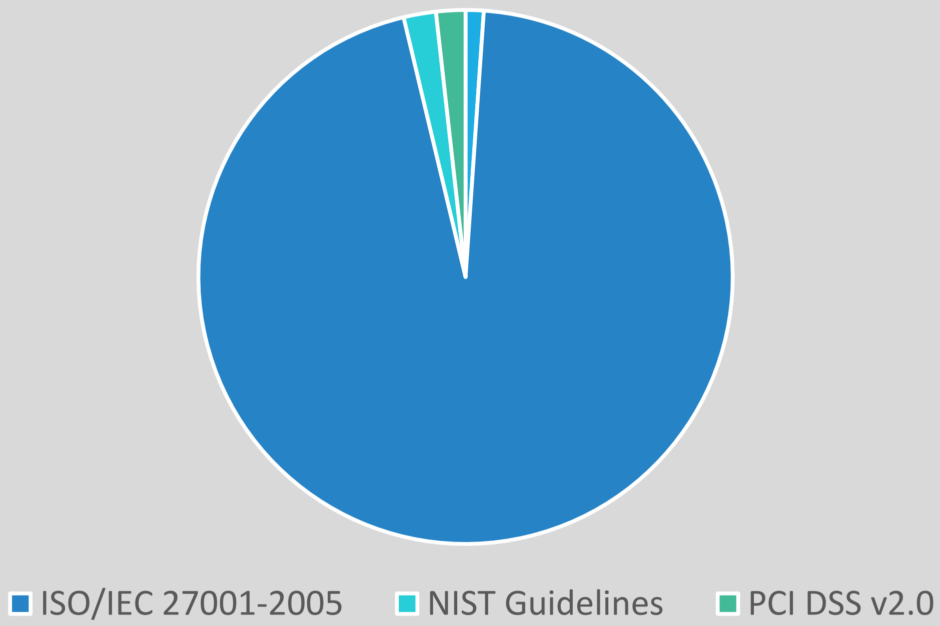
+/- 1% USA/EUROPE

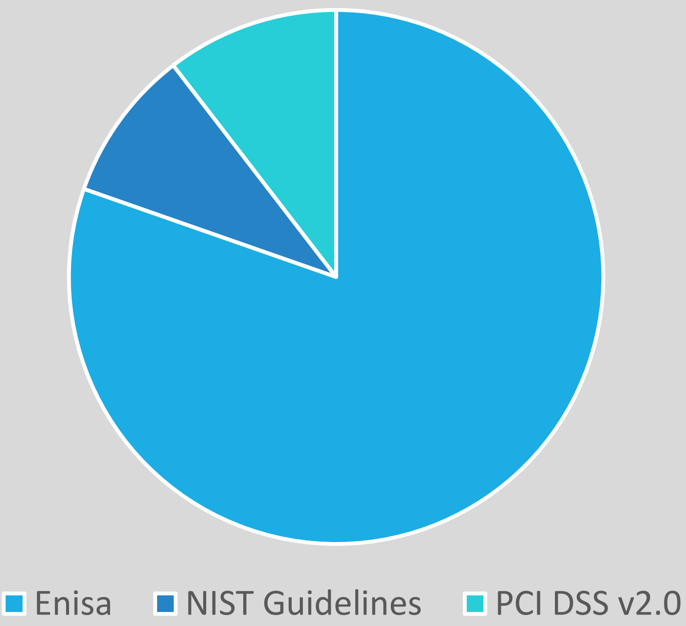
+/- 10% ASIA

Service type used in Europe



Regulations in use


USA/ME/Africa/Australia


Europe/Asia

Maturity levels

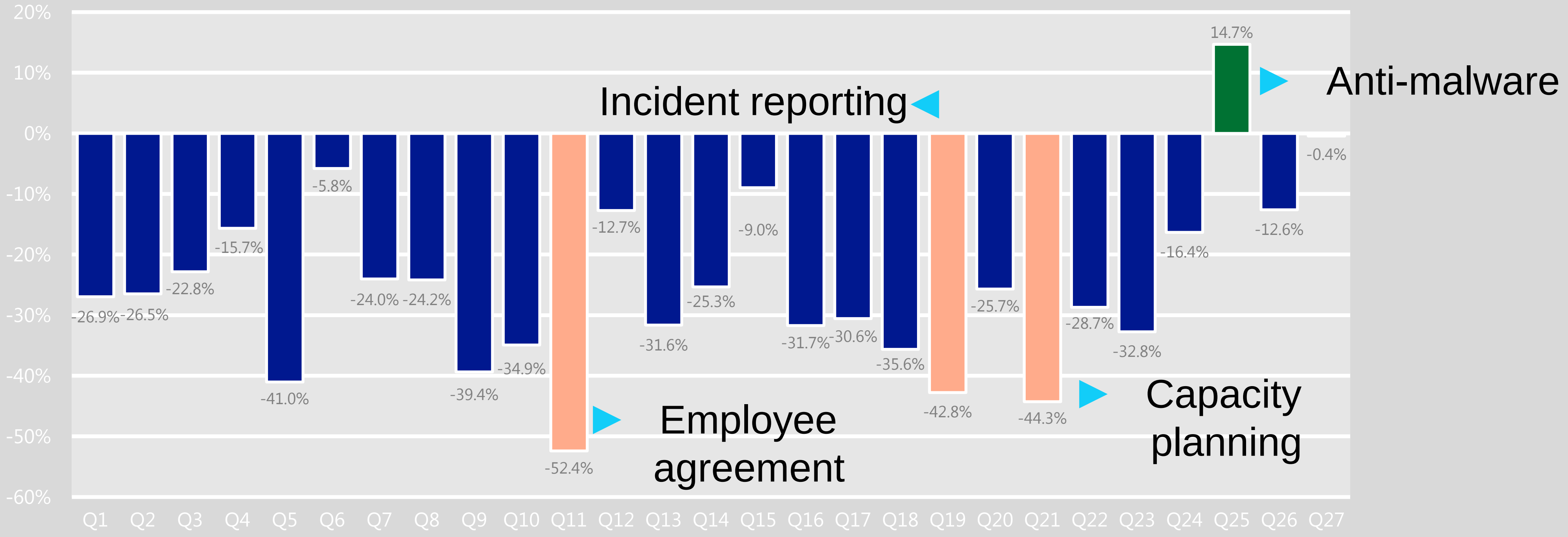
Getting Started.
Undocumented, ad hoc state. Reactive and incident or event response-driven.

Making Progress.
Response-driven, following trends, and somewhat repeatable with limited automation in segments.

Almost There.
Scaled response, using programs. Limited scaling still segmented.

Streamlined.
Centralized, automated, self-service, and scalable. Can allocate resources automatically.

CSRT respondent answers



Incident reporting

Anti-malware

Employee agreement

Capacity planning

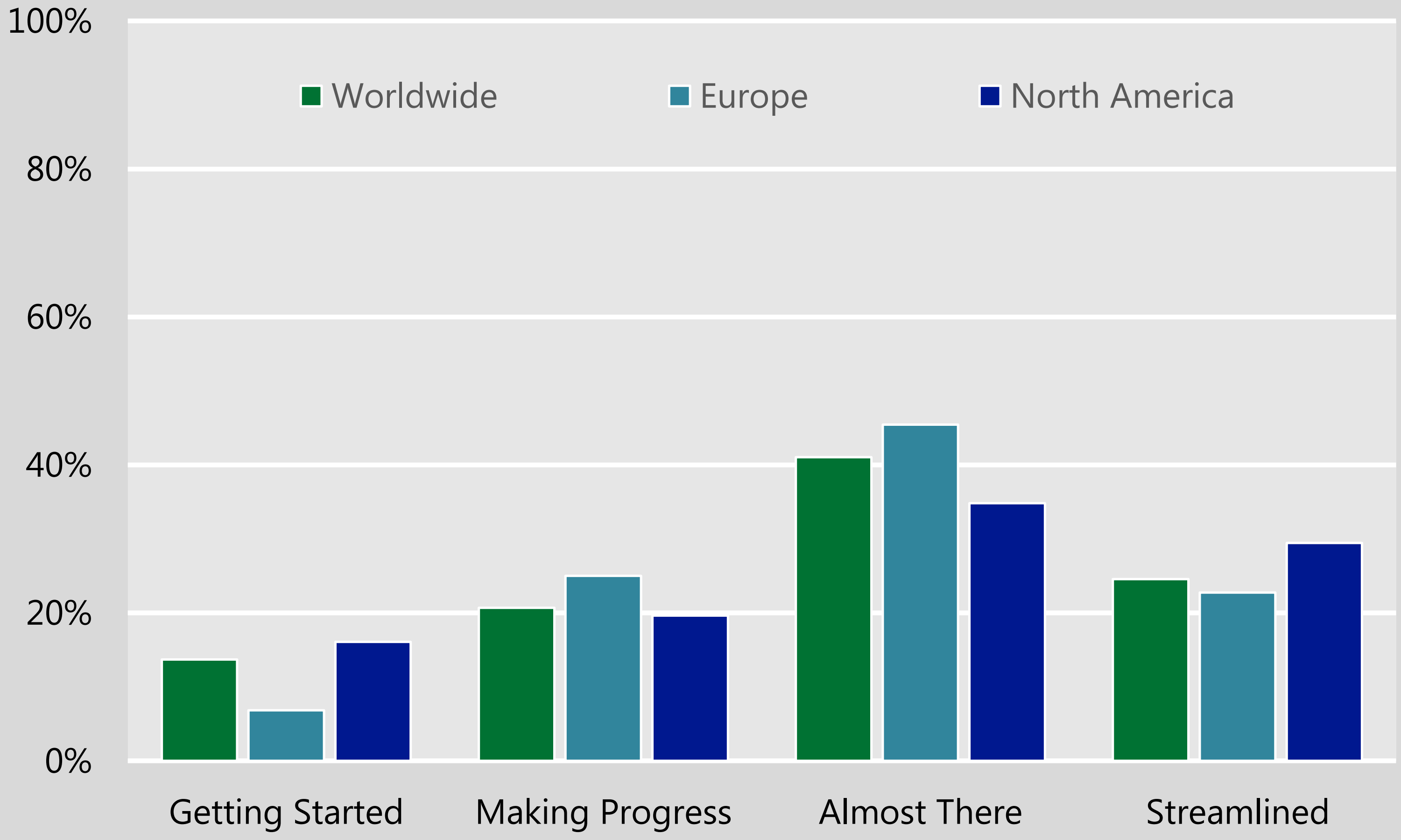
Values were assigned to each of the four possible answers for each question:

- If the answer was Almost There or Streamlined, a +1 value was assigned for maturity.
- If the answer was Getting Started or Making Progress, a -1 value was assigned for maturity.

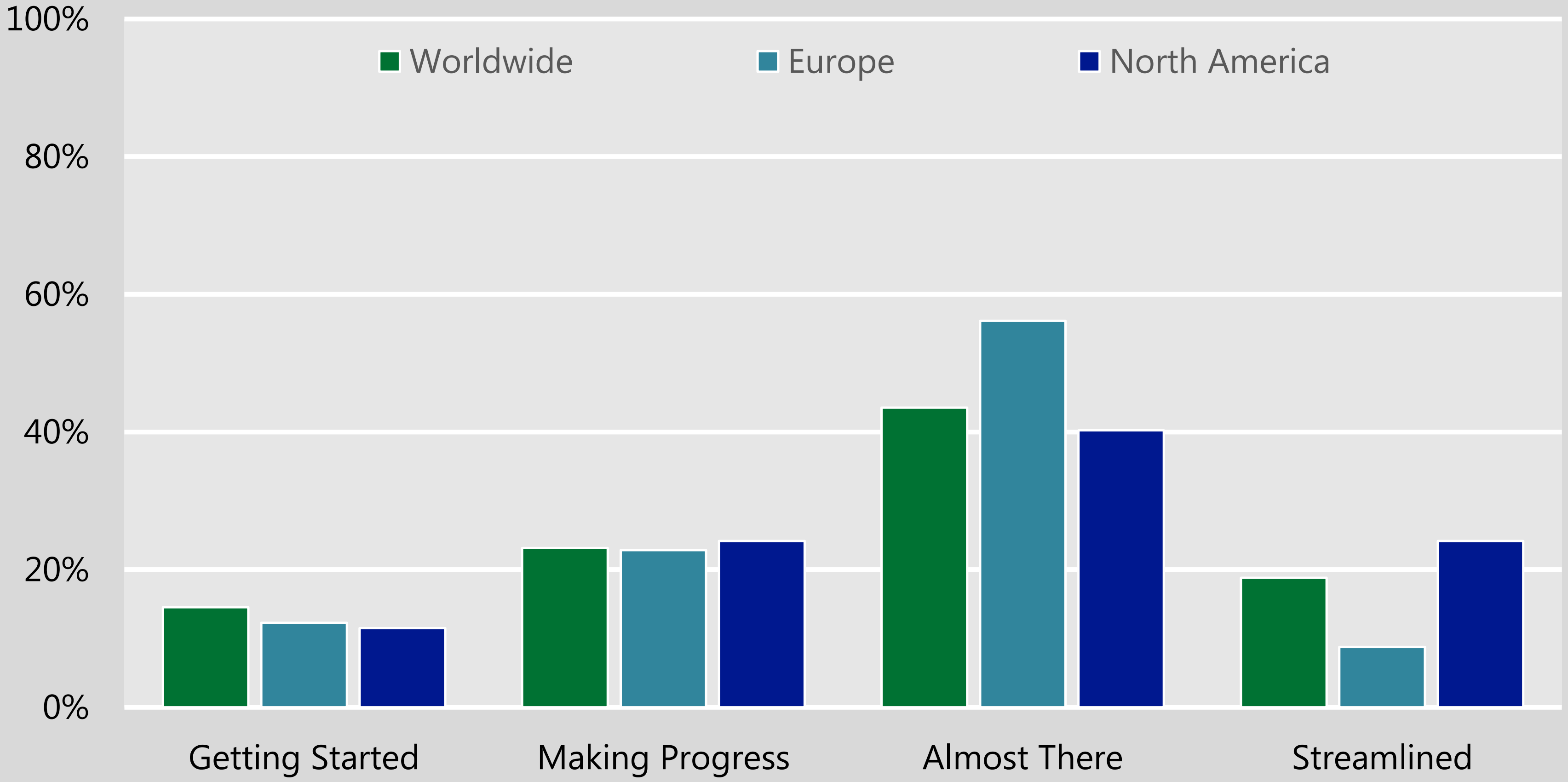
Which of these statements best describes your organization's antivirus efforts?

Getting Started	Some computers run antivirus programs and maintain their own update frequency.
Making Progress	All computers run an antivirus program that is provided by the organization. Each computer initiates its own updates.
Almost there	All computers run an antivirus program that is provided by the organization. Updates are managed and scheduled centrally.
Streamlined	All computers run an antivirus program that is provided by the organization. Updates are managed and scheduled centrally. Testing and review of the antivirus program is performed on a regular basis.

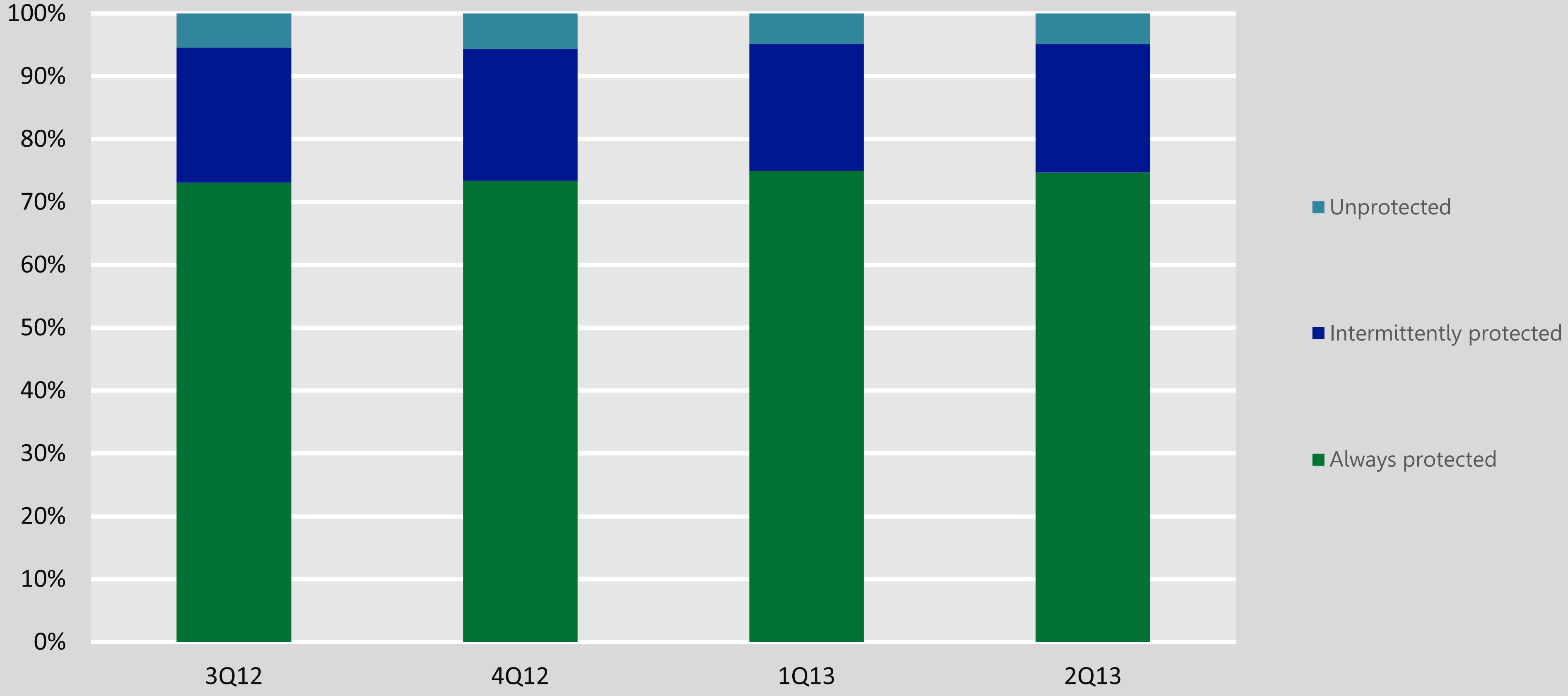
Antivirus / antimalware software (Enterprise)



Antivirus / antimalware software (SMB)



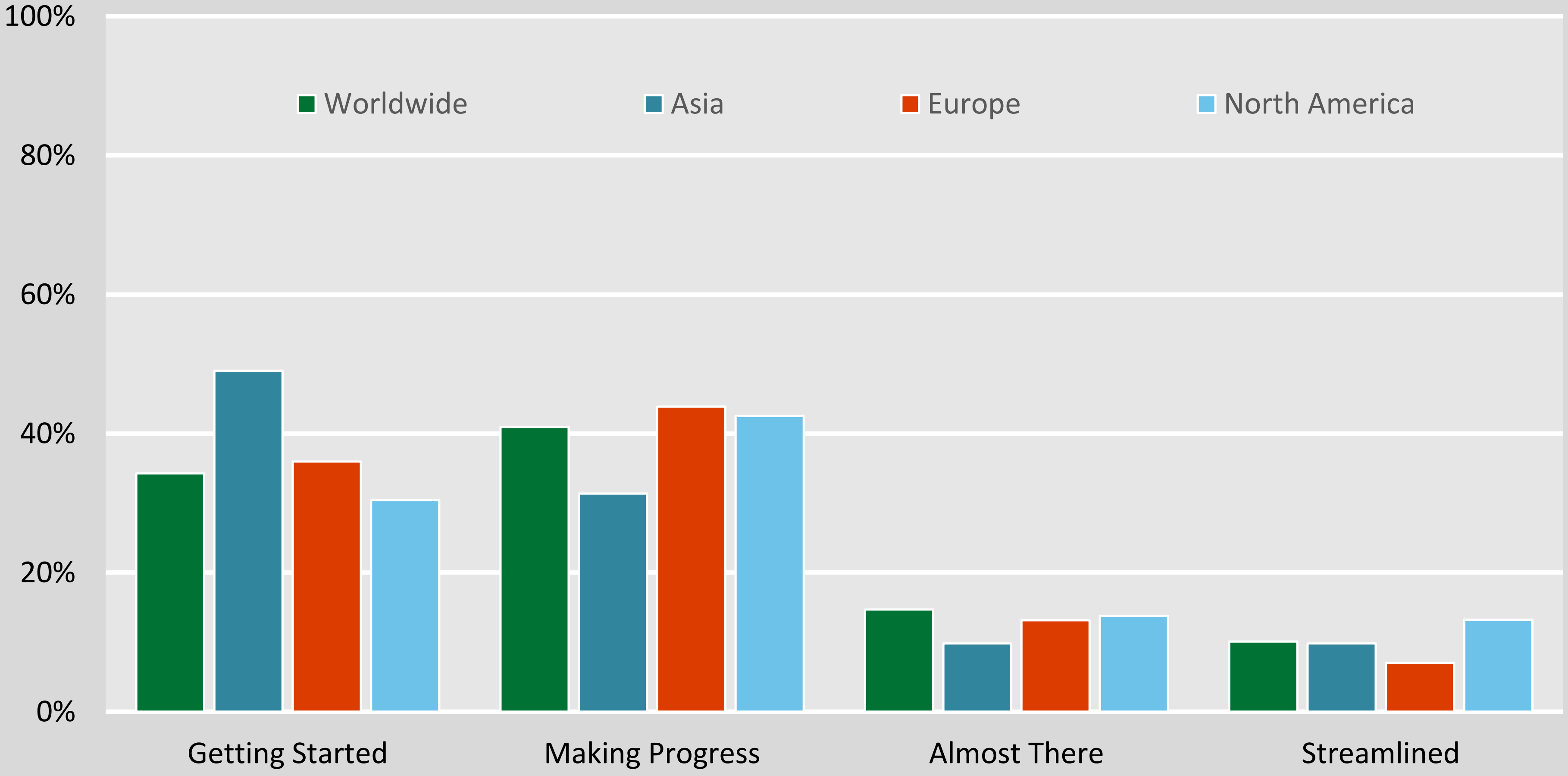
Computers with antimalware protection (SIR v15)



Which of these statements best describes your organization's nondisclosure agreement (NDA) requirements?

Getting Started	Paper NDAs are often signed.
Making Progress	Paper NDAs are signed and standardized across the organization.
Almost there	A mandatory electronic nondisclosure agreement process has been implemented.
Streamlined	A comprehensive, mandatory, regularly audited electronic nondisclosure agreement process exists.

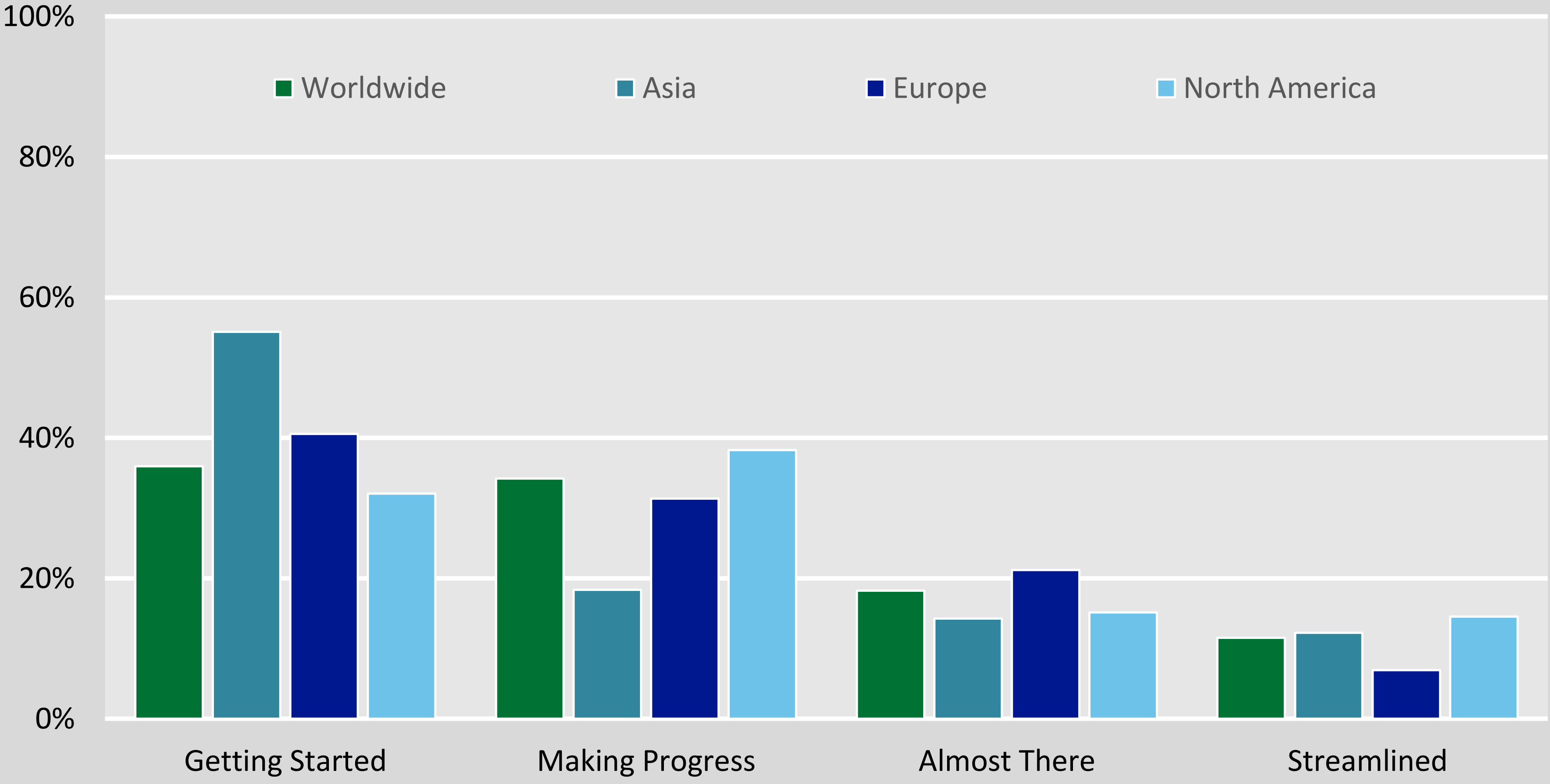
Human resources - Employment agreements



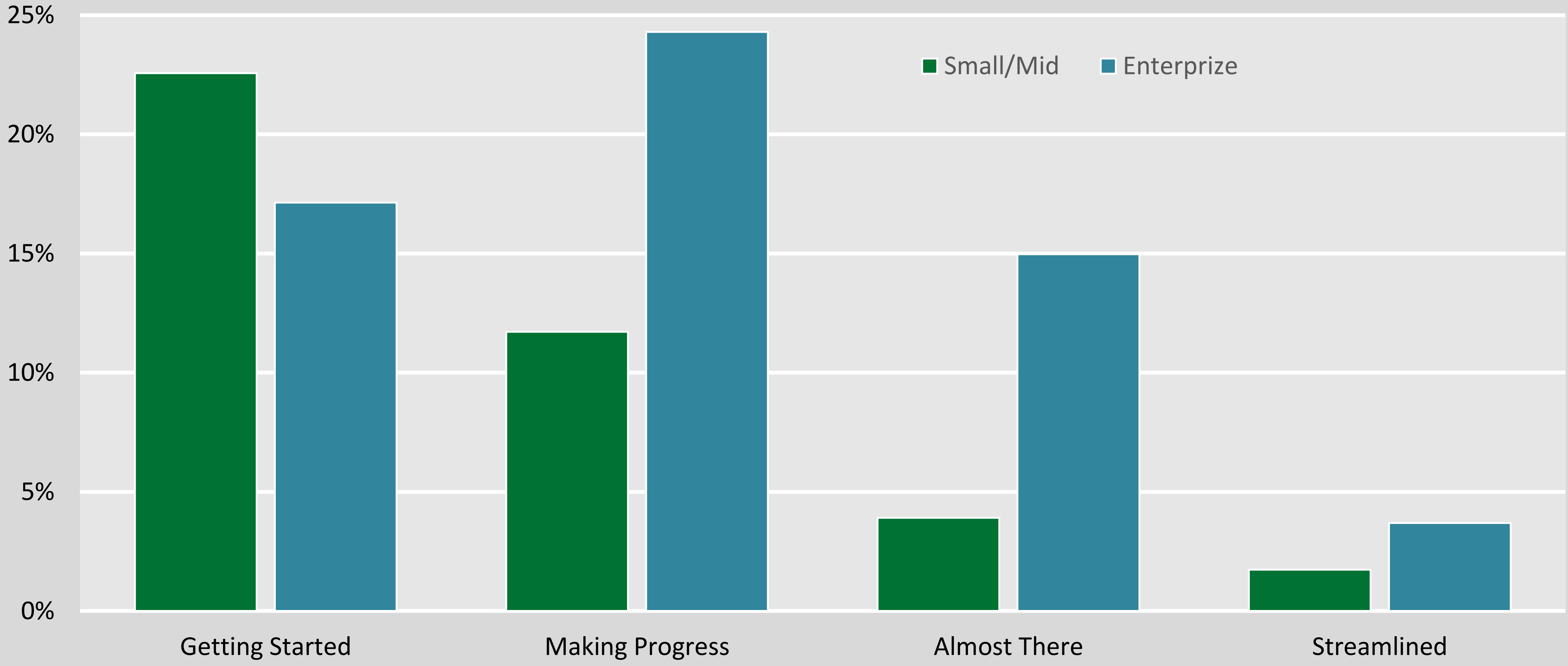
Which of these statements best describes your organization's capacity planning efforts?

Getting Started	The organization increases capacity when there is a capacity shortage.
Making Progress	No formal capacity planning process exists. Some projects include usage and growth estimation.
Almost there	A formal capacity planning process exists. Most IT projects plan for capacity growth using a validated formula.
Streamlined	A formal capacity planning process exists with a data life cycle plan, which is regularly reviewed for capacity compensation.

Operations management - Capacity planning



Resilience Europe



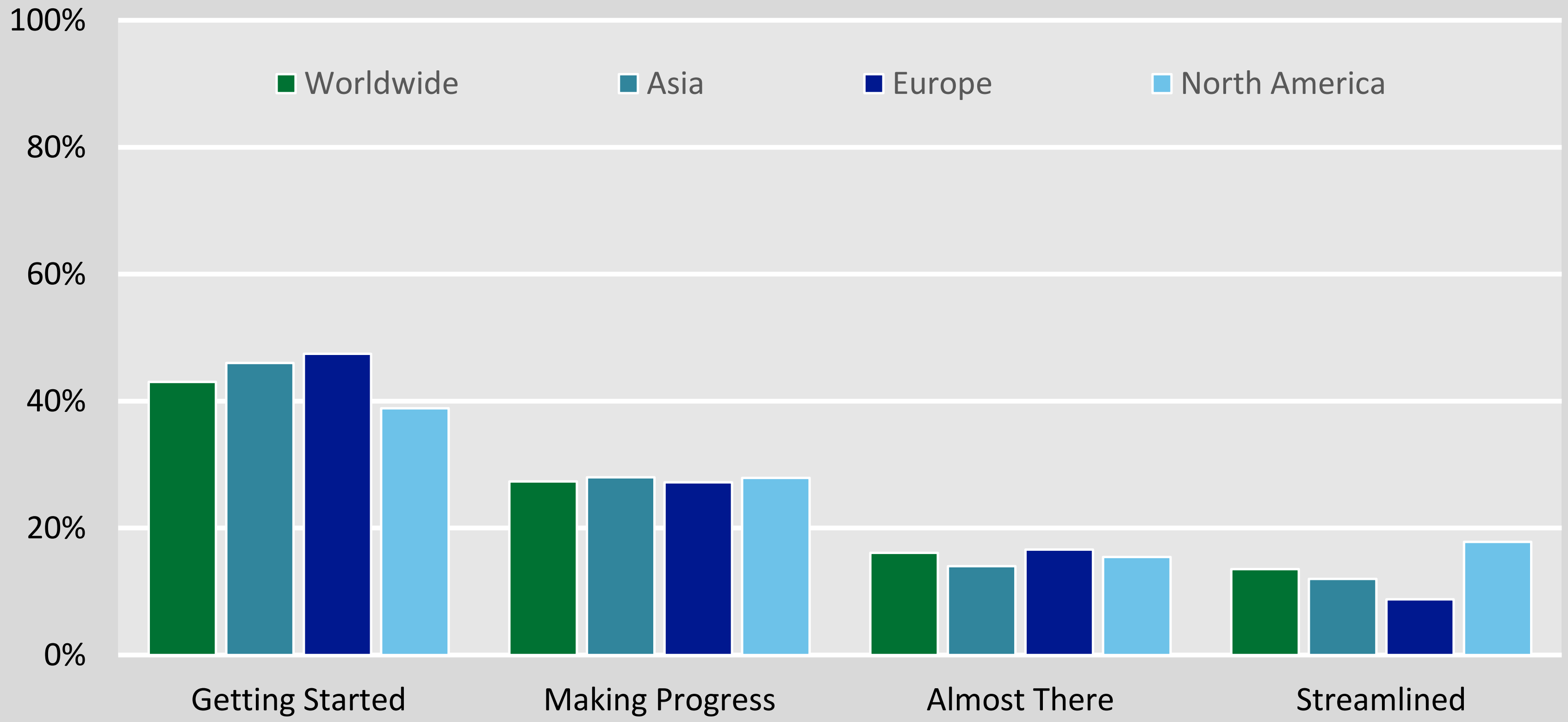
Control /question

security policies and procedures?	employee change/termination process?	security policies and procedures?	capacity planning efforts?
security policies review process?	physical security access method?	staging to production requirements?	selects its data center location(s)?
security program is updated?	equipment support contracts?	application testing using customer data?	redundancy if utility service outages should occur?
personnel background checks?	data classification efforts?	asset inventory program?	patch management processes?
(NDA) requirements?	grants access to data?	conducts risk assessments?	antivirus efforts?
physical access by role?	data retention and recovery program?	responds to an incident ?	firewalls to protect data?
security policies and procedures?	destroys data?	disaster recovery plan?	time setting policies?

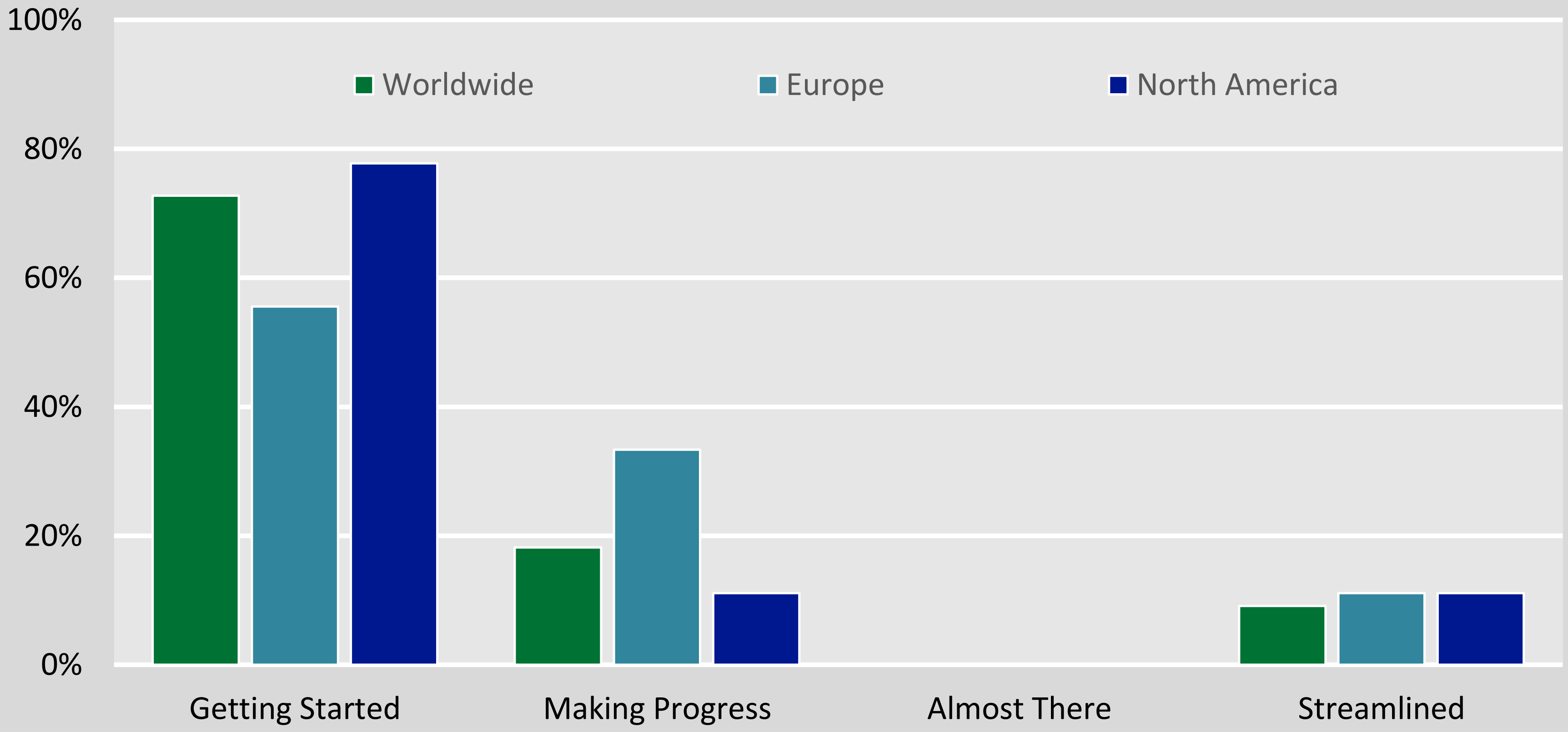
Which of these statements best describes how your organization responds to an incident ?

Getting Started	The organization responds to incidents in an ad-hoc manner as they are discovered.
Making Progress	Incident response is in accordance with documented policy, processes, and procedures.
Almost there	Incident response is in accordance with documented policy, processes, and procedures that are regularly updated and tested.
Streamlined	Incident response is in accordance with risk-based policy, processes, and procedures that are regularly updated, tested, and audited.

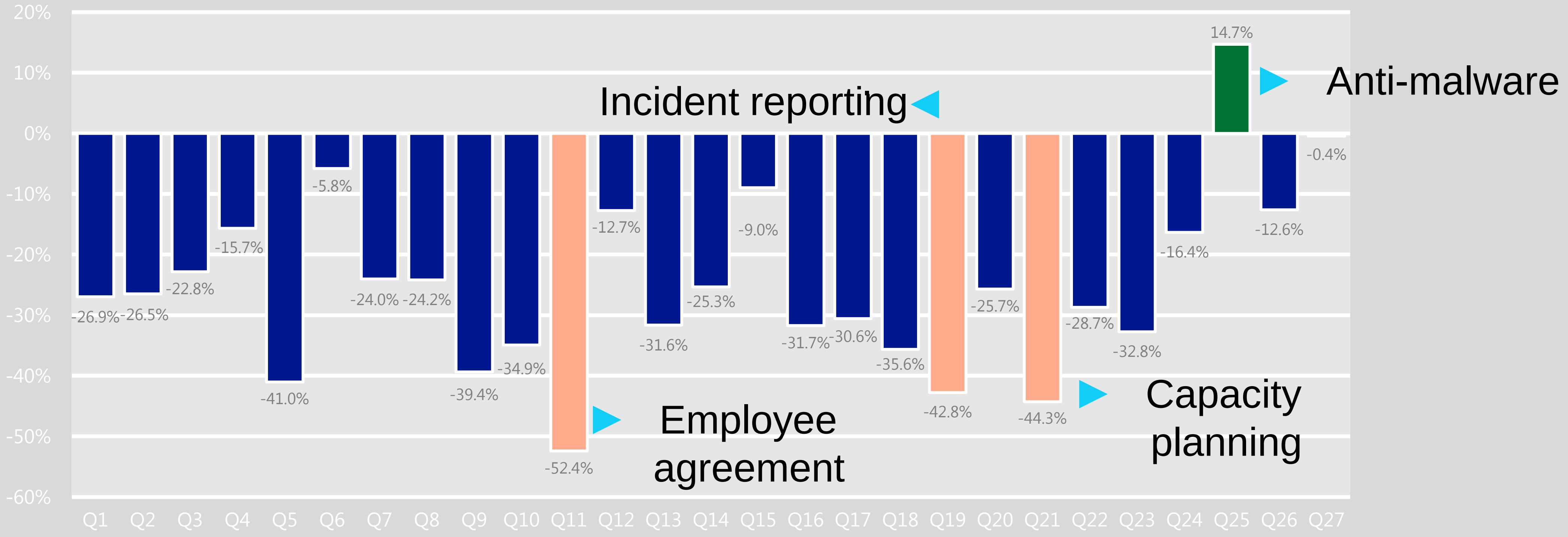
Q19 Information security - Incident reporting



Incident reporting (Non-profit/education)



What does this mean? (for Cloud adoption)



Incident reporting

Anti-malware

Employee agreement

Capacity planning

Values were assigned to each of the four possible answers for each question:

- If the answer was Almost There or Streamlined, a +1 value was assigned for maturity.
- If the answer was Getting Started or Making Progress, a -1 value was assigned for maturity.

What can I do?

The better you understand your people, processes, and technologies, the more you will be able to make informed comparisons and evaluate the benefits of the cloud.

Visit the Trustworthy Computing – Cloud TechCenter and its many resources:

The Cloud Security Readiness Tool

A free assessment to help you

evaluate the benefits of the cloud

create a plan for adoption

better understand your organization’s capabilities

www.microsoft.com/trustedcloud

Thank you!

Jeff Jones

Microsoft Trustworthy Computing

jrjones@microsoft.com

Frank Simorjay

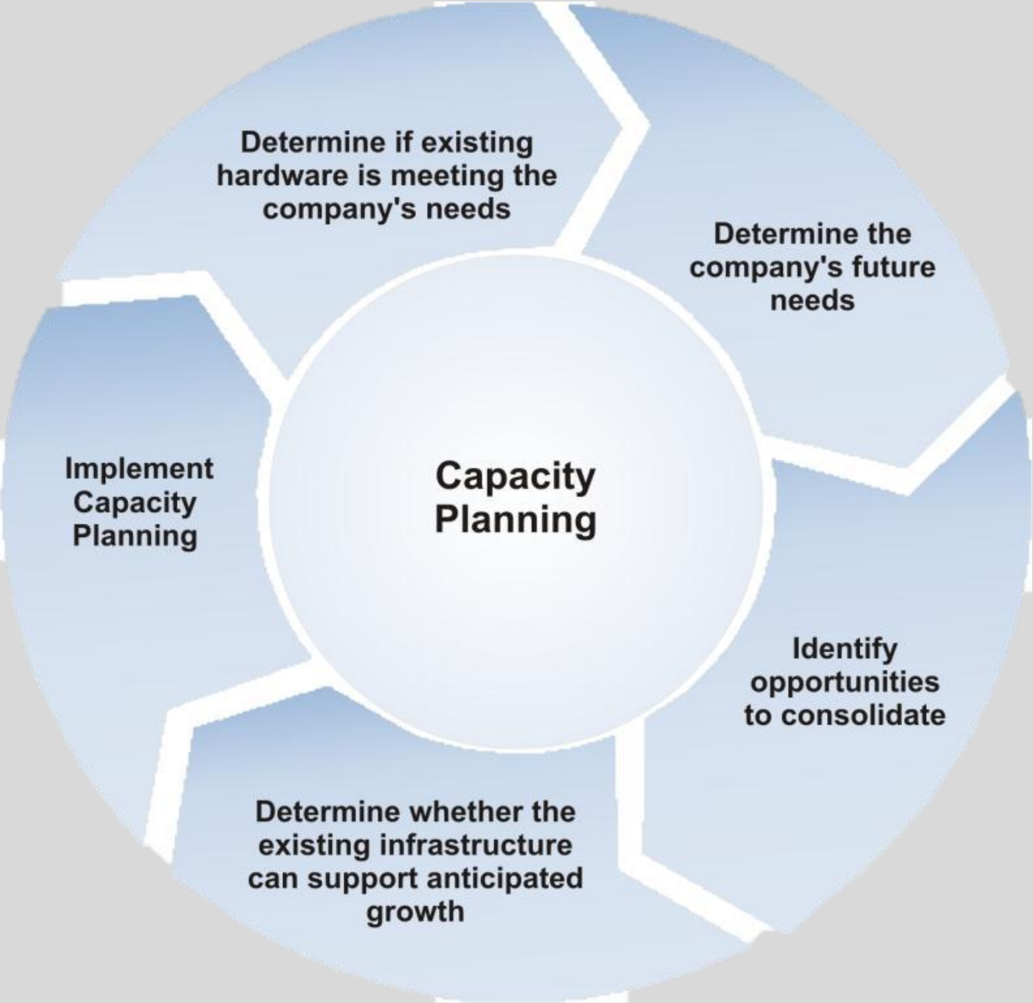
Microsoft Trustworthy Computing

frasim@microsoft.com

#RSAC

RSA CONFERENCE EUROPE 2013

Planning methodology



Capacity Planning

Determine if existing hardware is meeting the company's needs

Determine the company's future needs

Identify opportunities to consolidate

Determine whether the existing infrastructure can support anticipated growth

Implement Capacity Planning