

## State of Cloud Services in the U.S. Federal Government

Prepared by Dr. Larry Ponemon, September 5, 2011

The following tables summarize the results for all survey questions. The audited data is presented in three categories: the overall sample, IT sample and non-IT sample. This web-based survey was completed in September 2011. All respondents have bona fide credentials and are employed by U.S. federal organizations.

<b>Sample response</b>	Overall	IT	Non-IT
Sampling frame	12,916	6,455	6,461
Invitations	12,152	6,071	6,081
Total returns	585	296	289
Rejected surveys	55	29	26
Final sample before screening	530	267	263
Screened surveys	98	48	50
Final sample after screening	432	219	213
Response rate	3.3%	3.4%	3.3%
Sample weighting	100%	51%	49%

<b>Part 1. Screening Questions</b>			
Q1a. Does your organization use cloud applications or resources?	Overall	IT	Non-IT
Yes	281	145	136
No	249	122	127
Total	530	267	263

Q1b. If no, do you believe your organization will utilize cloud services in the next 12 months?	Overall	IT	Non-IT
Yes	151	74	77
No (stop after Q1c)	98	48	50
Total	249	122	127

Q1c. If no, why doesn't you organization deploy cloud services?	Overall	IT	Non-IT
Lack of suitable applications or services	42%	41%	43%
Lack of funding to move to the cloud environment	9%	10%	8%
Can't decide what applications to move to the cloud	13%	11%	16%
Concerns about safety and security	35%	36%	33%
Other	1%	2%	0%
Total	100%	100%	100%

<b>Part 2. Survey Questions</b>			
<b>Q2a. How familiar are you with the “Cloud First” policy?</b>	<b>Overall</b>	<b>IT</b>	<b>Non-IT</b>
Very familiar	36%	45%	26%
Somewhat familiar	37%	46%	28%
Not familiar	21%	7%	35%
No knowledge (go to Q3)	6%	2%	11%
Total	100%	100%	100%
<b>Q2b. What best describes your organization’s compliance (as of today) with the “Cloud First” policy in terms of identifying three “must move” services?</b>	<b>Overall</b>	<b>IT</b>	<b>Non-IT</b>
Full compliance, we identified all three cloud services	29%	30%	28%
Partial compliance, we only identified less than three cloud services	54%	56%	52%
Not yet in compliance	11%	10%	13%
Unsure	5%	4%	7%
Total	100%	100%	100%
<b>Q2c. What best describes your organization’s compliance (as of today) with the “Cloud First” policy in terms of moving at least one service from on-premises to the cloud during 2011?</b>	<b>Overall</b>	<b>IT</b>	<b>Non-IT</b>
Full compliance, we already moved one or more services to the cloud	25%	27%	23%
Partial compliance, we started the process of moving one or more services to the cloud	47%	45%	48%
Not yet in compliance	15%	11%	19%
Unsure	14%	17%	10%
Total	100%	100%	100%
<b>Q2d. In your opinion, is the “Cloud First” requirement to move three services to the cloud in an 18-month period a reasonable timeframe?</b>	<b>Overall</b>	<b>IT</b>	<b>Non-IT</b>
Yes, this timeframe is okay	22%	18%	26%
No, this timeframe is too fast	59%	69%	47%
No, this timeframe is too slow	14%	11%	18%
Unsure	5%	2%	9%
Total	100%	100%	100%
<b>Q3a. What types of cloud services does your organization use today</b>	<b>Overall</b>	<b>IT</b>	<b>Non-IT</b>
Private cloud – only your organization can use it	12%	13%	12%
Semi-public cloud shared with a limited number of US federal government organizations	25%	28%	21%
Semi-public cloud shared with any other federal, state or local government organization	33%	29%	38%
Public cloud shared with all customers of the cloud provider	30%	30%	30%
Total	100%	100%	100%

Q3b. What types of cloud services will your organization use in the next 12-18 months?	Overall	IT	Non-IT
Private cloud – only your organization can use it	20%	26%	15%
Semi-public cloud shared with a limited number of US federal government organizations	38%	44%	32%
Semi-public cloud shared with any other federal, state or local government organization	28%	20%	36%
Public cloud shared with all customers of the cloud provider	14%	10%	17%
Total	100%	100%	100%

Q4. <b>OVERALL:</b> In your opinion, who is <b>most responsible</b> for security in cloud environments used by your organization? Please define your answer in the context of each cloud type..	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
My organization is most responsible	48%	43%	39%	19%
Our cloud providers are most responsible	32%	36%	40%	55%
My organization and our cloud providers are equally responsible	20%	21%	21%	26%

Q4. <b>IT SAMPLE:</b> In your opinion, who is <b>most responsible</b> for security in cloud environments used by your organization? Please define your answer in the context of each cloud type..	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
My organization is most responsible	45%	46%	42%	20%
Our cloud providers are most responsible	30%	33%	38%	48%
My organization and our cloud providers are equally responsible	25%	21%	20%	32%

Q4. <b>NON-IT SAMPLE:</b> In your opinion, who is <b>most responsible</b> for security in cloud environments used by your organization? Please define your answer in the context of each cloud type..	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
My organization is most responsible	51%	40%	36%	18%
Our cloud providers are most responsible	34%	39%	42%	63%
My organization and our cloud providers are equally responsible	14%	21%	22%	19%

Q5. To date, which of the following federal security standards has your organization made active use of in planning or implementing cloud services? Please select all that apply.	Overall	IT	Non-IT
FISMA	56%	61%	51%
Fed Ramp	50%	54%	45%
NIST	39%	42%	36%
None of the above	20%	8%	31%
Other	6%	10%	1%
Total	170%	175%	165%

Q6. How confident are you about the overall data protection and security features of your current or prospective cloud service providers?	Overall	IT	Non-IT
Very confident	17%	13%	21%
Confident	26%	21%	30%
Not confident	45%	54%	36%
Unsure	12%	12%	13%
Total	100%	100%	100%

Q7. How does your organization determine if a given cloud provider has an adequate security posture?	Overall	IT	Non-IT
We conduct our own evaluation of each cloud provider using FISMA criteria	41%	50%	32%
We use Fed RAMP, which means we rely on a pre-determined assessment conducted by GSA and another federal agency.	23%	32%	15%
Other	8%	9%	7%
Unsure	28%	9%	47%
Total	100%	100%	100%

Q8. Please rate the following five statements using the scale below each item. Strongly agree and agree response.	SA & A, Overall	SA & A, IT Sample	SA & A, Non-IT Sample
Q8a. Cloud service providers used by my organization are compliant with FISMA requirements.	44%	38%	50%
Q8b. Cloud service providers used by my organization are compliant with Fed Ramp requirements.	39%	33%	45%
Q8c. Cloud services used by my organization are just as secure as on-premises IT services previously used.	38%	22%	54%
Q8d. My organization has applications and data that are too sensitive to move to the cloud environment.	62%	73%	51%
Q8e. The pressure to move to the cloud inadvertently creates security risks for my organization.	56%	71%	41%

Q9. How confident are you that your organization understands the <b>true long-term cost</b> of migrating on-premise applications and data to the cloud environment?	Overall	IT	Non-IT
Very confident	11%	8%	14%
Confident	29%	19%	39%
Not confident	53%	65%	40%
Unsure	7%	8%	7%
Total	100%	100%	100%

Q10. In your opinion, what do you believe is the <b>true long-term cost</b> impact to your organization as it moves from on-premises to cloud environments?	Overall	IT	Non-IT
Significant cost saving	12%	6%	18%
Some cost saving	30%	21%	39%
Neutral, no impact on cost	33%	39%	27%
Some cost increase	19%	24%	13%
Significant cost increase	6%	10%	3%
Total	100%	100%	100%

Q11. Which one of the following attributes or features do you view as the <b>most important</b> reasons for moving to the cloud? Please select only two top choices.	Overall	IT	Non-IT
Cost savings	55%	35%	76%
Political mandate	59%	69%	48%
Interoperability	28%	34%	22%
Improved efficiency	33%	31%	35%
Increased security	18%	8%	29%
Other	3%	4%	2%
Total	196%	181%	212%

Q12. <b>OVERALL:</b> What percent of cloud services used in your organization today (or in the next 12 months) are provided from private, semi-public or public cloud environments? Your best guess is welcome.	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
None	45%	26%	19%	15%
1 to10%	16%	20%	18%	12%
11 to 25%	14%	16%	23%	28%
26 to 50%	8%	21%	20%	24%
51 to 75%	3%	6%	8%	5%
76 to 100%	14%	11%	12%	16%
Total	100%	100%	100%	100%
Extrapolated average	20%	25%	28%	32%

Q12. <b>IT SAMPLE:</b> What percent of cloud services used in your organization today (or in the next 12 months) are provided from private, semi-public or public cloud environments? Your best guess is welcome.	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
None	48%	27%	21%	14%
1 to10%	15%	19%	19%	13%
11 to 25%	13%	14%	15%	29%
26 to 50%	7%	22%	21%	22%
51 to 75%	2%	6%	8%	6%
76 to 100%	15%	12%	16%	16%
Total	100%	100%	100%	100%
Extrapolated average	20%	26%	30%	32%

Q12. <b>NON-IT SAMPLE:</b> What percent of cloud services used in your organization today (or in the next 12 months) are provided from private, semi-public or public cloud environments? Your best guess is welcome.	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
None	42%	25%	17%	16%
1 to 10%	17%	21%	17%	11%
11 to 25%	15%	18%	32%	27%
26 to 50%	9%	20%	19%	26%
51 to 75%	4%	6%	8%	4%
76 to 100%	13%	10%	7%	16%
Total	100%	100%	100%	100%
Extrapolated average	21%	24%	25%	32%

Q13. <b>OVERALL:</b> In your opinion, how safe are each of these cloud types for your organization's applications?	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
Very safe	19%	18%	16%	10%
Somewhat safe	45%	43%	38%	25%
Somewhat unsafe	26%	30%	34%	45%
Very unsafe	10%	9%	12%	20%
Total	100%	100%	100%	100%

Q13. <b>IT SAMPLE:</b> In your opinion, how safe are each of these cloud types for your organization's applications?	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
Very safe	17%	17%	14%	6%
Somewhat safe	35%	33%	28%	24%
Somewhat unsafe	36%	35%	39%	55%
Very unsafe	12%	15%	19%	15%
Total	100%	100%	100%	100%

Q13. <b>NON-IT SAMPLE:</b> In your opinion, how safe are each of these cloud types for your organization's applications?	Private cloud – only your organization can use it	Semi-public cloud shared with a limited number of US federal government organizations	Semi-public cloud shared with any other federal, state or local government organization	Public cloud shared with all customers of the cloud provider
Very safe	21%	19%	18%	15%
Somewhat safe	56%	54%	49%	26%
Somewhat unsafe	15%	24%	28%	34%
Very unsafe	8%	2%	4%	26%
Total	100%	100%	100%	100%

Q14a. For your organization, how important is it for cloud service providers to perform these physical security steps? Please use the following scale::1 = Very important, 2 = Important, 3 = Not important and 4 = Irrelevant	VI & I, Overall	VI & I, IT sample	VI & I, Non-IT sample
Physically isolate your organization's services and data storage from all others	52%	63%	41%
Physically isolate all government services and data storage from all others	61%	73%	49%
Locate all servers in the United States	65%	78%	52%
Require cloud custodians who have access to your services to pass rigorous background checks	59%	70%	48%
Require cloud custodians who have access to your services to be U.S. citizens	41%	51%	31%
Average	56%	67%	44%

Q14b. How confident are you that your cloud service providers perform these physical security steps? Please use the following scale: 1 = Very confident, 2 = Confident, 3 = Not confident and 4 = Unsure	VC & C, Overall	VC & C, IT sample	VC & C, Non-IT sample
Physically isolate your organization's services and data storage from all others	50%	45%	55%
Physically isolate all government services and data storage from all others	48%	42%	54%
Locate all servers in the United States	49%	40%	58%
Require cloud custodians who have access to your services to pass background checks	48%	44%	52%
Require cloud custodians who have access to your services to be U.S. citizens	30%	23%	37%
Average	45%	39%	51%

Q15a. What applications or services are <b>most suitable</b> for cloud deployment by your organization? Please check only your top three choices.	Overall	IT	Non-IT
Email	73%	66%	80%
Word processing	72%	68%	76%
Spreadsheets	68%	57%	80%
Presentation tools	65%	61%	70%
Group collaboration	63%	54%	73%
Internal portal (employee-facing)	56%	46%	66%
External portal (public-facing)	50%	40%	61%
Finance & budget	33%	30%	36%
Human resources including payroll	43%	42%	44%
Backup and disaster recovery	60%	54%	66%
Organization's core domain-specific applications	34%	33%	36%
Law enforcement applications	13%	5%	22%
National security applications	12%	0%	24%
Other	3%	0%	5%
Average	46%	40%	53%

Q15b. What applications or services are <b>least suitable</b> for cloud deployment by your organization? Please check only your top three choices.	Overall	IT	Non-IT
Email	21%	30%	13%
Word processing	22%	34%	10%
Spreadsheets	21%	33%	9%
Presentation tools	25%	32%	17%
Group collaboration	26%	33%	18%
Internal portal (employee-facing)	35%	39%	31%
External portal (public-facing)	26%	33%	20%
Finance & budget	33%	42%	23%
Human resources including payroll	39%	47%	31%
Backup and disaster recovery	23%	25%	20%
Organization's core domain-specific applications	49%	58%	39%
Law enforcement applications	75%	81%	69%
National security applications	83%	93%	74%
Other	3%	8%	0%
Average	34%	42%	27%

Q16. How confident are you that your organization knows all privileged users who have access to the servers and data storage devices operated by your cloud service providers?	Overall	IT	Non-IT
Very confident	23%	15%	31%
Confident	29%	22%	36%
Not confident	43%	62%	23%
Unsure	5%	1%	9%
Total	100%	100%	100%

Q17a. Does your organization encrypt sensitive or confidential information stored in the cloud environment?	Overall	IT	Non-IT
Yes, all data	9%	8%	10%
Yes, some data	23%	25%	22%
No	46%	52%	40%
Unsure	21%	15%	28%
Total	100%	100%	100%

Q17b. If yes, does your cloud service provider have access to encryption keys?	Overall	IT	Non-IT
Yes, full access	33%	39%	27%
Yes, partial or supervised access	30%	44%	15%
No access	8%	5%	12%
Unsure	29%	12%	46%
Total	100%	100%	100%

Q18. To the best of your knowledge, did any one of your cloud service providers suffer a security breach sometime over the past 12 months?	Overall	IT	Non-IT
Yes	11%	20%	2%
No	45%	40%	51%
Unsure	43%	40%	47%
Total	100%	100%	100%

Q19a. In your opinion, what is the likelihood that your organization will suffer a security breach as a result of an insecure cloud service provider sometime over the next 12 months?	Overall	IT	Non-IT
Already happened	11%	20%	1%
Very likely	24%	25%	23%
Likely	22%	29%	15%
Not likely	27%	20%	34%
No chance	16%	6%	26%
Total	100%	100%	100%

Q19b. In your opinion, what is the likelihood that a U.S. federal agency or department (other than your organization) will suffer a security breach as a result of an insecure cloud service provider sometime over the next 12 months?	Overall	IT	Non-IT
Already happened	11%	20%	2%
Very likely	24%	27%	21%
Likely	39%	34%	45%
Not likely	18%	15%	22%
No chance	7%	4%	10%
Total	100%	100%	100%

Q20. How confident are you that your cloud service provider would inform your organization if it suffered from a security exploit or data breach involving your applications or data?	Overall	IT	Non-IT
Very confident	24%	10%	38%
Confident	25%	24%	26%
Not confident	31%	43%	19%
Unsure	20%	23%	17%
Total	100%	100%	100%

Q21. <b>OVERALL:</b> The following table lists six common security threats faced by many federal organizations. In your opinion, are these issues more likely, less likely or equally likely to occur in the cloud versus on-premise?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Negligent insiders	51%	15%	34%	100%
Malicious insiders	50%	18%	32%	100%
External cyber attacks	34%	29%	37%	100%
Vulnerable applications	56%	18%	26%	100%
Vulnerable endpoints	33%	32%	35%	100%
Insecure third-party relationships	21%	19%	60%	100%

Q21. <b>IT SAMPLE:</b> The following table lists six common security threats faced by many federal organizations. In your opinion, are these issues more likely, less likely or equally likely to occur in the cloud versus on-premise?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Negligent insiders	48%	11%	41%	100%
Malicious insiders	44%	13%	43%	100%
External cyber attacks	35%	33%	32%	100%
Vulnerable applications	48%	20%	32%	100%
Vulnerable endpoints	27%	36%	36%	100%
Insecure third-party relationships	24%	13%	63%	100%

Q21. <b>NON-IT SAMPLE:</b> The following table lists six common security threats faced by many federal organizations. In your opinion, are these issues more likely, less likely or equally likely to occur in the cloud versus on-premise?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Negligent insiders	54%	19%	26%	100%
Malicious insiders	57%	24%	20%	100%
External cyber attacks	33%	24%	43%	100%
Vulnerable applications	65%	16%	19%	100%
Vulnerable endpoints	39%	27%	34%	100%
Insecure third-party relationships	18%	26%	56%	100%

Q22. <b>OVERALL:</b> The following table lists five consequences of security failure experienced by many federal organizations. In your opinion, are these consequences more likely, less likely or equally likely to occur in the cloud versus the on-premise IT environment?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Unauthorized public disclosure of information assets	60%	16%	24%	100%
Corruption or loss of information assets	53%	17%	30%	100%
Compromise of government employees' privacy	36%	21%	43%	100%
Compromise of citizens' privacy	29%	19%	52%	100%
Disruption of department or agency's IT operations	34%	11%	55%	100%
Average	51%	15%	34%	100%

Q22. <b>IT SAMPLE:</b> The following table lists five consequences of security failure experienced by many federal organizations. In your opinion, are these consequences more likely, less likely or equally likely to occur in the cloud versus the on-premise IT environment?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Unauthorized public disclosure of information assets	65%	9%	26%	100%
Corruption or loss of information assets	50%	13%	37%	100%
Compromise of government employees' privacy	35%	23%	42%	100%
Compromise of citizens' privacy	23%	26%	51%	100%
Disruption of department or agency's IT operations	35%	5%	60%	100%
Average	51%	15%	34%	100%

Q22. <b>NON-IT SAMPLE:</b> The following table lists five consequences of security failure experienced by many federal organizations. In your opinion, are these consequences more likely, less likely or equally likely to occur in the cloud versus the on-premise IT environment?	More likely to occur in the cloud	Less likely to occur in the cloud	Equally likely	Total
Unauthorized public disclosure of information assets	55%	23%	22%	100%
Corruption or loss of information assets	56%	21%	23%	100%
Compromise of government employees' privacy	37%	19%	44%	100%
Compromise of citizens' privacy	36%	11%	53%	100%
Disruption of department or agency's IT operations	33%	18%	49%	100%
Average	51%	15%	34%	100%

Recently, Google reported that it was the victim of a cyber attack that allowed Chinese hackers to hijack gmail accounts by using malware and phishing scams that tricked users into sharing their passwords, or by using passwords obtained by hacking other websites. Other web-based email systems were also attacked including Hotmail. While most account hijackings were not very targeted, some attacks were targeted at specific individuals including senior U.S. government officials.

Q23. How familiar are you with this recent cyber attack?	Overall	IT	Non-IT
Very familiar	30%	32%	29%
Familiar	32%	36%	28%
Not familiar	26%	19%	34%
No knowledge (go to Part 3)	11%	13%	10%
Total	100%	100%	100%

Q24. How did this incident affect your confidence in the security of cloud services?	Overall	IT	Non-IT
No affect	14%	11%	18%
Minimal affect	18%	16%	20%
Some affect	37%	36%	39%
Significant affect	23%	33%	14%
Unsure	7%	4%	10%
Total	100%	100%	100%

Q25. How did this incident affect the adoption rate of cloud services by your organization?	Overall	IT	Non-IT
No affect	26%	21%	30%
Minimal affect	50%	44%	55%
Some affect	10%	16%	4%
Significant affect	8%	14%	1%
Unsure	7%	5%	9%
Total	100%	100%	100%

<b>Part 2. Organizational Characteristics</b>			
D1. What best describes your position or organizational level?	Overall	IT	Non-IT
Department head	5%	6%	5%
Executive	5%	7%	2%
Director	31%	29%	32%
Manager	36%	35%	37%
Supervisor	14%	13%	15%
Technician	4%	8%	0%
Staff	4%	2%	5%
Contractor	0%	0%	0%
Other	2%	0%	3%
Total	100%	100%	100%

D2. What is the name of the federal department or agency that employs you? Top ten:	Overall	IT	Non-IT
Defense, Civilian	14%	15%	12%
Defense, Military	7%	6%	8%
Justice	3%	4%	3%
Homeland Security	10%	8%	13%
Treasury	5%	6%	4%
State	2%	0%	5%
Transportation	4%	0%	8%
Commerce	5%	2%	9%
Labor	2%	0%	3%
Health & Human Services	9%	12%	6%
Energy	2%	4%	0%
Education	1%	0%	2%
Executive Branch	14%	15%	13%
DNI	5%	8%	3%
NASA	1%	2%	0%
US Postal Service	3%	5%	2%
All others	12%	13%	12%
Total	100%	100%	100%

D3. What best describes your organizational unit (within the federal agency or department)?	Overall	IT	Non-IT
General management	6%	5%	7%
Project management	5%	3%	8%
Human resources	1%	0%	2%
Compliance & audit	2%	2%	1%
Legal	2%	0%	4%
Security	8%	3%	12%
Public policy	5%	0%	10%
Media and communications	4%	0%	8%
Budget and finance	8%	0%	16%
Citizen and community outreach	4%	0%	7%
Research, training and education	9%	4%	14%
Information Technology (IT)	35%	68%	0%
Information security	8%	15%	2%
Other	5%	0%	9%
Total	100%	100%	100%

D4. Do you consider yourself an IT practitioner or professional?	Overall	IT	Non-IT
Yes	49%	100%	0%
No	51%	0%	100%
Total	100%	100%	100%

D5. Experience (mean years)	Overall	IT	Non-IT
D5a. How many years of relevant experience to you have?	11.6	10.9	12.2
D5b. How many years have to been in your present position?	5.1	5.0	5.2

D6. What the approximate headcount of your organization?	Overall	IT	Non-IT
Less than 1,000	17%	9%	25%
1,001 to 5,000	12%	11%	14%
5,001 to 10,000	32%	38%	25%
10,001 to 25,000	30%	26%	33%
25,001 to 50,000	4%	8%	0%
More than 50,000	5%	8%	3%
Total	100%	100%	100%

Respectfully,

*L.A. Ponemon*

Dr. Larry Ponemon  
Chairman & Founder

Please contact [research@ponemon.org](mailto:research@ponemon.org) or call us at 800.887.3118 if you have any questions.

### **Ponemon Institute**

*Advancing Responsible Information Management*

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict information confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.