Week 10 Assignment – Course Project – Final Version

William Slater

CYBR 610 – Risk Management Studies

Bellevue University

Recognizing and Mitigating the Risks Associated with Teleworking Employees

Ronald Woerner, M.S. - Instructor

August 11, 2012

Abstract

In the last 10 to 12 years, the advent and rapid evolution of technologies related to communications, collaboration, document generation and handling, networking, the Internet, remote administration, and security have all given rise to the gradual acceptance of teleworking as a viable work alternative for workers. In fact, teleworking has become a common alternative especially for knowledge workers and those involved in the development of work products related to software development and system administration. This document will examine teleworking as an accepted fact, but also as a way of working that is different from managing office workers, and as such it has its own set of unique risks. Therefore different tools and management techniques must be used to effectively mitigate these risks.

Outline

I. Introduction to Teleworking and Its Associated Risks

II. Teleworking and the Law

III. Typical Teleworker Risks and Mitigations

IV. Essential Teleworking Management Tools

V. Case Study: Comparison between Best Practices in Telework Management and Teleworking Practices on a Recent Program

VI. A Checklist for Telework Security Policy Notes

VII. Conclusion

VIII. References

IX. Appendix A – Summary of Telework Fundamentals for Managers, developed by Government Services Administration (GSA) and the U.S. Office of Personnel Management (OPM)

Recognizing and Mitigating the Risks Associated with Teleworking

In the last 10 to 12 years, the advent and rapid evolution of technologies related to communications, collaboration, document generation and handling, and security have given rise to the acceptance of teleworking as a viable work alternative for workers, and especially for knowledge workers and those involved in software development. This document looks at teleworking as an accepted fact, but also as a way of working that is different from managing office workers, and so therefore, different tools and management techniques are involved. While this document does not do an exhaustive job of covering all aspects of management of teleworkers, it does summarize and cover the more important tools required for best practices in managing teleworkers. It also summarizes some of the unique risks involved in teleworking and the risks related to the absence of these basic teleworking management tools.

Teleworking and the Law

The Telework Enhancement Act of 2010 was passed by Congress and signed into law by President Obama. It effectively authorizes agencies of the U.S. Federal Government to create programs that would legally empower Federal workers to be able to telecommute at the discretion of their management, as the responsibilities of their jobs permitted. This law also stipulated that annual agency progress reports would be submitted to Congress to explain the state of teleworking among Federal employees.

Typical Teleworking Risks and Mitigations

Due to the unique nature of teleworking, the typical teleworker, and teleworking manager in or outside the government, both face risks that are unique and different than those associated

with the traditional office working environment. The table below lists some of those unique risks and their suggested mitigations.

Telework Risk	Mitigation	Comments	Recommendation
Data breach	Policies Training Network Security controls such as VPN, strong passwords	See **Mitigating Teleworking Risks** (SANS, 2001)	Implement: Policies Training Network Security controls such as VPN, strong passwords
Network security breach	Policies Training Security inspections Network Security controls such as VPN, strong passwords	See **Mitigating Teleworking Risks** (SANS, 2001)	Policies Training Security inspections Network Security controls such as VPN, strong passwords
Missing employees and unproductive behaviors	Policies Training Teleworking Management Tools (OPM and GSA, 2011).		Policies Training Teleworking Management Tools
Lack of Telework Policies	Do analysis and design work and create Telework Policies (OPM and GSA, 2011).	Should be placed in place on the organizations's intranet website in the How Do I Section? Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Policies
Lack of Telework Agreement	Do analysis and design work and create Telework Agreement (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Agreement
Lack of Telework Schedule	Do analysis and design work and create Telework Schedule (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Schedule

Telework Risk	Mitigation	Comments	Recommendation
Lack of Telework Communications Plan	Do analysis and design work and create Telework Communications Plan (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Communications Plan
Lack of Telework Work Plan	Do analysis and design work and create Telework Work Plan (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Work Plan
Lack of Telework Training	Do analysis and design work and create Telework Training (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Training
Lack of Telework Security Plan	Do analysis and design work and create Telework Security Plan (OPM and GSA, 2011).	Required if you are going to have a strong and productive Telework program.	Do analysis and design work and create Telework Security Plan Refer to NIST SP 800-46 rev 1 and NIST SP 800-114
Risk of unauthorized physical access to corporate information stored on a remote PC	Use of locks and home alarm systems.	See **Mitigating Teleworking Risks** (SANS, 2001)	Use good locks and home alarm systems. CCTV surveillance is also good with DVR machine.
An "always on connection" can be a likely target for attackers and malware.	Use of Internet firewall devices and laptop firewall programs.	See **Mitigating Teleworking Risks** (SANS, 2001)	Use of Internet firewall devices and laptop firewall programs.
Teleworker behavior associated with downloading of unauthorized programs.	Use of written policies and Windows group policy objects that are deployed on the equipment used to perform telework. Also the regular updating of Windows software and antivirus program software and signatures.	See **Mitigating Teleworking Risks** (SANS, 2001)	Use of written policies and Windows group policy objects that are deployed on the equipment used to perform telework. Also the regular updating of Windows software and antivirus program software and signatures.

Telework Risk	Mitigation	Comments	Recommendation
Exposure of remote PC on Internet.	Direct exposure can be mitigated by strong identification, authentication and authorization at the corporate firewall or DMZ and the use of encryption technology to protect data integrity and confidentiality. (Typically, a virtual private network [VPN] is employed to provide aspects of all of the above.)	See **Mitigating Teleworking Risks** (SANS, 2001)	Use strong identification, authentication and authorization at the corporate firewall or DMZ and the use of encryption technology to protect data integrity and confidentiality. (Typically, a virtual private network [VPN] is employed to provide aspects of all of the above.)
	Indirect exposure can be mitigated by protecting the remote PC by deploying standard security measures on the PC but, as discussed above, the security status of the remote PC cannot be guaranteed and hence the corporate network must be protected against a compromised remote PC.	See **Mitigating Teleworking Risks** (SANS, 2001)	Protect the remote PC or laptop by deploying standard security measures on the PC but, as discussed above, the security status of the remote PC cannot be guaranteed and hence the corporate network must be protected against a compromised remote PC.
Bridging networks from remote Home Networks to Corporate Networks creates the opportunity for Zombies, botnets and other serious malware.	Use of written policies and Windows group policy objects that are deployed on the equipment used to perform telework. Also the regular updating of Windows software and antivirus program software and signatures. Direct exposure can be mitigated by strong identification, authentication and authorization at the corporate firewall or DMZ and the use of encryption technology to protect data integrity and confidentiality.	See **Mitigating Teleworking Risks** (SANS, 2001)	Use written policies and Windows group policy objects that are deployed on the equipment used to perform telework. Also regularly update of Windows software and antivirus program software and signatures. Use strong identification, authentication and authorization at the corporate firewall or DMZ and the use of encryption technology to protect data integrity and confidentiality.

Essential Teleworking Management Tools

The following table contains a list of teleworking management tools that were taken from the TELEWORK.gov website (OPM and GSA, 2011).

Teleworking Management Tool	Description
Telework Policies (OPM and GSA, 2011).	Written policies
Telework Agreement (OPM and GSA, 2011).	Signed, written agreement between teleworker and management to establish the ground rules on teleworking.
Telework Schedule (OPM and GSA, 2011).	Written schedule accurately reflects the work hours that the teleworker will be available for work assignments. Copies will be provided to the teleworker's management, team leads, and the teleworker. The schedule must be reviewed and agreed upon by both the teleworker and their management.
Telework Communications Plan (OPM and GSA, 2011).	Written communications plan that reflects the how the teleworker will communicate and the expectations for responding to communications. Forms of communication may include phone, cell phone, e-mail, FAX, instant chat communication, smart phone, and/or SKYPE, etc. The communications plan must be reviewed and agreed upon by both the teleworker and their management. Copies will be provided to the teleworker's management, team leads, and the teleworker.
Telework Work Plan (OPM and GSA, 2011).	Written work plan that reflects the what the teleworker will work on and the expectations for type and format of deliverables, quality, quantity, work delivery, type and frequency of review for approval and/or revision. The work plan must be reviewed and agreed upon by both the teleworker and their management. Copies will be provided to the teleworker's management, team leads, and the teleworker.

Teleworking Management Tool	Description
Telework Training (OPM and GSA, 2011).	All teleworkers should complete teleworker training every 12 months. Teleworking managers should complete both the teleworker employee training and the telework management training. Teleworker training should be formal, structured, interactive, and online. It will define teleworking and management expectations regarding this method of working. It also includes the definitions and explanations regarding the various teleworking management tools. 1. Teleworking Policies 2. Teleworker Agreement 3. Telework Schedule 4. Telework Communications Plan 5. Telework Work Plan 6. Telework Security Plan Managers of teleworker should complete both the telework employee training and telework training for managers. It also includes the definitions and explanations regarding the various teleworking management tools: 1. Teleworking Policies 2. Teleworker Agreement 3. Telework Schedule 4. Telework Communications Plan 5. Telework Work Plan 6. Telework Security Plan A copy of the certificate completion of teleworker training must be provided to the provided to the teleworker's management, team leads, the teleworker, and the training coordinator.

Teleworking Management Tool	Description
Teleworker Security Plan (OPM and GSA, 2011).	The Teleworker Security Plan includes the technical details about how to securely connect with and communicate with the organization. Such details will include: 1. Acceptable use guidelines 2. Requirements for home networking and Internet connections 3. Requirements for security on home networking and Internet connections 4. Requirements for security in the organization's infrastructure 5. Password use and protection 6. Use of protocols and configurations 7. Encryption requirements, uses and configuration techniques 8. A list of threats and vulnerabilities 9. Requirements for antivirus protections 10. Requirements for security and etiquette in all forms of electronic communication 11. Other requirements for working securely, such as restrictions on unauthorized software installation and making copies of and/or transmitting data.

Case Study: Comparison between Best Practices in Telework Management and Teleworking Practices on a Recent Program

From July 2011 – March 2012, I worked in an organization where the work environment of every position on this 48-person team was 100% telework, across four U.S. Time Zones (Eastern, Central, Mountain, and Pacific). This primary purpose of this program was to develop systems that facilitated the use of electronic medical records.

It is unknown if there were data breaches and security breaches with the workers and work performed on this program, however, there were at least two known instances of subcontractor workers taking advantage of the nature of telework and disappearing while they were supposed to be working. When the infractions were finally discovered, each subcontractor was immediately terminated from the program. In the first instance, the subcontractor was never available and never responded to attempts to communicate with him after the first week when he joined the team. In fact, it was later discovered that the rogue subcontractor had secured employment at another company, while he was supposedly a member of our team. His immediate supervisor did not accept full responsibility for this issue, saying that she was already overworked and that she was focused on project deadlines and providing focus and attention on the primary senior developers that worked for her.

The table below shows a comparison between the recommended best practices in teleworking described by the training at TELEWORK.gov and state of that organization's teleworking management practices.

Telework Fundamentals Training	**CACI NwHIN - U.S. Department of Veterans Affairs Telework**	**Comments**	**Recommendation**
Telework Policies (OPM and GSA, 2011).	Yes	Available on the organizations VLER Website under "How Do I"	Disseminate information about these policies and have employees and have employees acknowledge receipt, reading and understanding.

Telework Fundamentals Training	CACI NwHIN - U.S. Department of Veterans Affairs Telework	Comments	Recommendation
Telework Agreement (OPM and GSA, 2011).	Nonexistent	Should have been written. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written. Disseminate information about this agreement and have employees and have employees acknowledge receipt, reading and understanding.
Telework Schedule (OPM and GSA, 2011).	Nonexistent	Should have been written. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written, published and available to the Team.
Telework Communications Plan (OPM and GSA, 2011).	Nonexistent	Should have been written, specifying types of communication, frequency, and expectations for responses. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written, published and available to the Team.
Telework Work Plan	Nonexistent	Should have been written, specifying deliverables, quantity, quality, type of review, frequency of review, feedback, etc. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written. Bothe the Manager and the Teleworker should agree to the creation and execution of this plan.
Teleworker Training (OPM and GSA, 2011).	Nonexistent	Should have been written. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written, and completed annually.
Teleworker Security Plan (OPM and GSA, 2011).	Nonexistent	Should have been written. Lack of this introduced unnecessary risks into the teleworking environment.	Should be written, and training should include the details of this security plan.

A Checklist for Telework Security Policy Notes

"As every good security program begins with the security policy. Security policy must cover telecommuting/teleworking. In particular it should consider:

- "- who may telework - identify the roles/jobs which may be considered for teleworking
- "- services available to teleworkers - the types of network and application services which may be provided to teleworkers
- "- Information restrictions - are there classified information types which should not be made available to teleworkers?
- "- Identification/authentication/authorization - how should teleworkers be identified, authenticated and authorized before accessing corporate resources
- "- Equipment and software specifications - are there any specific equipment or software products which must be deployed on the teleworker's PC? (e.g., firewall or encryption software)
- "- Integrity and confidentiality - consider how the connection to the remote PC should be protected (i.e., VPN) and how data on the machine should be protected
- "- Maintenance guidelines - how should the teleworker's PC configuration be protected, updated and monitored?
- "- User guidelines - clarify the user's role in protecting corporate resources - e.g., appropriate use of resources; user should not modify security configurations; use of anti-virus software; storage of corporate data on local drives; use of encryption tools
- "- User education - ensure that users understand the possible information risks associated with teleworking, how those risks are addressed, and the user's role in minimizing the risks (SANS, 2001).

Applying a Risk Management Framework to Manage and Mitigate Teleworking Risks

There are several well-defined, structured risk management frameworks that can help organizations manage risk in a structured manner. Since I am very familiar with the ISO 27001 framework for performing risk management, I chose it. Appendix B shows a sample minimum set of policies that would be required to help mitigate the risks of teleworking in an organization.

These policies are specifically required under ISO 27001 Annex A item 11.7.2. However, in reality, if the teleworker is working in an ISO 27001 certified organization, many more sections of Annex A would apply to ensure that all potential risks were recognized and mitigated. The results of the analysis that I performed are shown in Appendix C of this document. The results show that nearly all of the ISO 27001 Annex A items would apply, with the exception of some policies under Annex A section 9.

As a matter of cost-savings or convenience, it may be possible to ignore the application of these ISO 27001 Annex A security controls for the teleworker, but to do so introduces risks that these ISO 27001 Annex A security controls were designed to mitigate. It would also introduce the risk of failing an ISO 27001 audit if the ISO 27001 Audit Team is savvy enough to ask the right questions and understand the manner in which the organization's employees and contractors perform their work. Failing an ISO 27001 certification audit is both an expensive and risky proposition: Failing an ISO 27001 certification audit could jeopardize business revenues from companies that require ISO 27001 certification as a condition of doing business, and it could damage an organization's credibility, reputation, and business relationships in the long term.

Conclusion

This paper has shown that while teleworking has now become a widely accepted practice very different from working and managing in a traditional office environment, it also has special risks that can present special challenges to employees and management. Because telework is different than a traditional office environment, it requires special training, tools, and an

awareness of the new risks that are inherent to teleworking. Some of these tools that can be used to mitigate these risks include:

Effective Telework Policies

Teleworker Agreements

Teleworker Training

Teleworker Schedule

Teleworker Communications Plan

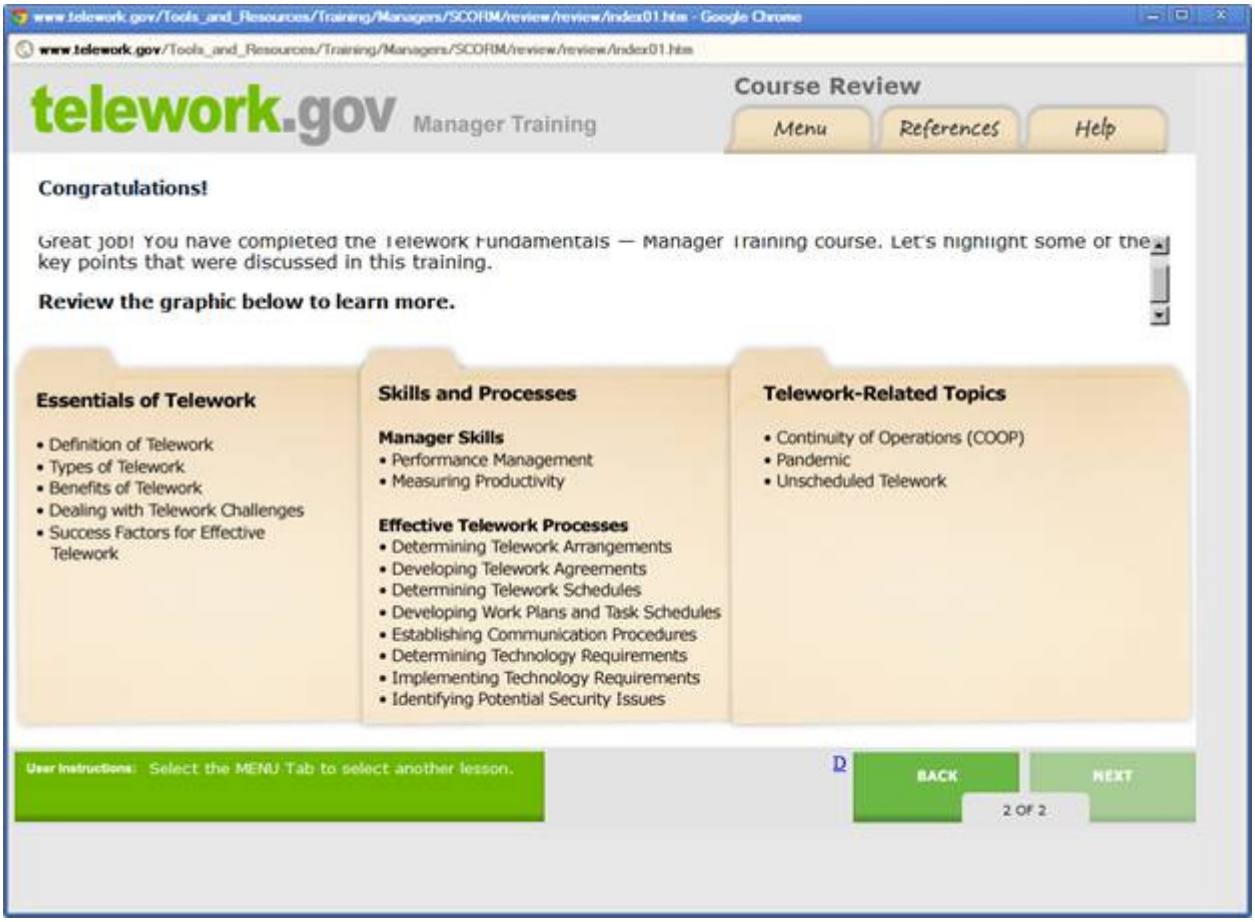
Teleworker Work Plan

Teleworker Security Assessment and Security Plan

It is absolutely essential for every manager who implements a teleworking program to understand and proactively plan to mitigate the risks associated with this organizational transition, so that they reduce risks to acceptable levels, ensure secure work environments, and maximize productivity, for the employees and for the organization as a whole.

One final observation related to teleworking is the recent surge of smart phones and tablet computing. It has created a related phenomenon in the U.S. called, Bring Your Own Device (BYOD) in which employees want to connect their personal mobile devices to their organization's network. This BYOD phenomenon will likely also greatly impact teleworking practices to change the very nature of work as we know it in most organizations within the next five years. In the very near future, one can predict with great certainty that the rapid adoption of BYOD and teleworking will greatly increase the importance understanding, planning, and effectively mitigating the risks associated with these modern phenomenon.

Appendix A – Summary of Telework Fundamentals for Managers, developed by Government Services Administration (GSA) and the U.S. Office of Personnel Management (OPM)



(OPM and GSA, 2011)

Appendix B – Sample Information Security Policies Recommended For Teleworkers to Fulfill the Requirements of ISO 27001 A 11.7.2

11.7 MOBILE COMPUTING AND TELEWORKING » 11.7.2 Teleworking

» **1. Telecommuting Data Entry Operators**

All Acme Widget data entry operators must employ thin clients as configured by the Information Systems Department as well as download the software for their work at the beginning of each business day.

» **2. Telecommuting Equipment**

Employees working on Acme Widget business at alternative work sites must use Acme Widget-provided computer and network equipment, unless other equipment has been approved by the Help Desk as compatible with Acme Widget information systems and controls.

» **3. Telecommuter Working Environments**

To retain the privilege of doing off-site work, all telecommuters must structure their remote working environment so that it is in compliance with all Acme Widget policies and standards.

» **4. Security Requirements For Telecommuters**

Before a telecommuting arrangement can begin, the worker's manager must be satisfied that an alternative work site is appropriate for the Acme Widget work performed by the involved worker.

» **5. Telecommuter Information Security Procedures**

Telecommuters must follow all remote system security policies and procedures including, but not limited to, compliance with software license agreements, performance of regular backups, and use of shredders to dispose of sensitive paper-resident information.

» **6. Inspections Of Telecommuter Environments**

Acme Widget maintains the right to conduct inspections of telecommuter offices with one or more days advance notice.

» **7. Remote Workers Required to Sign Specific Policy**

All Acme Widget employees who are approved to work from remote locations must sign an agreement to abide by specific remote worker policies. The agreement should be reviewed annually.

» **8. Lockable Metal Furniture**

All workers who must keep sensitive Acme Widget information at their homes in order to do their work, must receive from Acme Widget or otherwise provide lockable furniture for the proper storage of this information.

» **9. Security Standard for Home User Computers**

The Acme Widget Information Security Department must issue a standard for the security configuration of home computers which employees use for remote access to Acme Widget networks. The standard must include a list of required and prohibited software packages

» **10. Clock Synchronization of Remote Systems**

Telecommuting workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time.

» **11. Third-Party Network Access Control**

When accessing a Acme Widget computer or communications system through a third-party network teleworkers must use the secure remote access solution provided by the organization.

» **12. Teleworker Password Controls**

Teleworkers must maintain the self-selected passwords used to access all teleworking equipment and networks including that which is personally owned using the Acme Widget password policies and standards.

» **13. Applications on Personally-Owned Equipment**

Workers must install and properly maintain only approved communications and productivity applications on any personally-owned equipment used to access a Acme Widget computer or communications system.

» **14. Teleworker Software Updates**

Teleworkers must check for updates and apply them periodically, as explained in the manufacturer's documentation, either automatically or manually, for all equipment used to communicate with Acme Widget computer and communications systems.

(Policy Shield, 2011)

Appendix C – IS0 27001 Controls that Would Apply to Teleworkers in an ISO 27001 Certified Organization

Control Seq. No.	ISO 27001 Annex A Control Name and Annex Reference Designation	Does It Apply to Teleworkers?
1	A.5.1.1 Information Security Policy Document	**Yes**
2	A.5.1.2 Review Of The Information Security Policy	**Yes**
3	A.6.1.1 Management Commitment To Information Security	**Yes**
4	A.6.1.2 Information Security Coordination	**Yes**
5	A.6.1.3 Allocation Of Information Security Responsibilities	**Yes**
6	A.6.1.4 Authorization Process For Information Processing Facilities	**No**
7	A.6.1.5 Confidentiality Agreements	**Yes**
8	A.6.1.6 Contact With Authorities	**Yes**
9	A.6.1.7 Contact With Special Interest Groups	**Yes**
10	A.6.1.8 Independent Review Of Information Security	**Yes**
11	A.6.2.1 Identification Of Risks Related To External Parties	**Yes**
12	A.6.2.2 Addressing Security When Dealing With Customers	**Yes**
13	A.6.2.3 Addressing Security In Third Party Agreements	**Yes**
14	A.7.1.1 Inventory Of Assets	**Yes**
15	A.7.1.2 Ownership Of Assets	**Yes**
16	A.7.1.3 Acceptable Use Of Assets	**Yes**
17	A.7.2.1 Classification Guidelines	**Yes**
18	A.7.2.2 Information Labeling And Handling	**Yes**
19	A.8.1.1 Roles And Responsibilities	**Yes**
20	A.8.1.2 Screening	**Yes**
21	A.8.1.3 Terms And Conditions Of Employment	**Yes**
22	A.8.2.1 Management Responsibilities	**Yes**
23	A.8.2.2 Awareness, Education, And Training	**Yes**
24	A.8.2.3 Disciplinary Process	**Yes**
25	A.8.3.1 Termination Responsibilities	**Yes**
26	A.8.3.2 Return Of Assets	**Yes**
27	A.8.3.3 Removal Of Access Rights	**Yes**

Control Seq. No.	ISO 27001 Annex A Control Name and Annex Reference Designation	Does It Apply to Teleworkers?
28	A.9.1.1 Physical Security Perimeter	**No**
29	A.9.1.2 Physical Entry Controls	**No**
30	A.9.1.3 Securing Offices, Rooms, Facilities	**Yes**
31	A.9.1.4 Protecting Against External And Environmental Threats	**Yes**
32	A.9.1.5 Working In Secure Areas	**Yes**
33	A.9.1.6 Public Access, Delivery And Loading Areas	**No**
34	A.9.2.1 Equipment Siting And Protection	**No**
35	A.9.2.2 Supporting Utilities	**Yes**
36	A.9.2.3 Cabling Security	**No**
37	A.9.2.4 Equipment Maintenance	**No**
38	A.9.2.5 Security Of Equipment Off-Premises	**Yes**
39	A.9.2.6 Secure Disposal Or Re-Use Of Equipment	**Yes**
40	A.9.2.7 Removal Of Property	**Yes**
41	A.10.1.1 Documented Operating Procedures	**Yes**
42	A.10.1.2 Change Management	**Yes**
43	A.10.1.3 Segregation Of Duties	**Yes**
44	A.10.1.4 Separation Of Development, Test And Operational Facilities	**Yes**
45	A.10.2.1 Service Delivery	**Yes**
46	A.10.2.2 Monitoring And Review Of Third Party Services	**Yes**
47	A.10.2.3 Managing Changes To Third Party Services	**Yes**
48	A.10.3.1 Capacity Management	**Yes**
49	A.10.3.2 System Acceptance	**Yes**
50	A.10.4.1 Controls Against Malicious Code	**Yes**
51	A.10.4.2 Controls Against Mobile Code	**Yes**
52	A.10.5.1 Information Back-Up	**Yes**
53	A.10.6.1 Network Controls	**Yes**
54	A.10.6.2 Security Of Network Services	**Yes**
55	A.10.7.1 Management Of Removable Media	**Yes**
56	A.10.7.2 Disposal Of Media	**Yes**
57	A.10.7.3 Information Handling Procedures	**Yes**

Control Seq. No.	ISO 27001 Annex A Control Name and Annex Reference Designation	Does It Apply to Teleworkers?
58	A.10.7.4 Security Of System Documentation	**Yes**
59	A.10.8.1 Information Exchange Policies And Procedures	**Yes**
60	A.10.8.2 Exchange Agreements	**Yes**
61	A.10.8.3 Physical Media In Transit	**Yes**
62	A.10.8.4 Electronic Messaging	**Yes**
63	A.10.8.5 Business Information Systems	**Yes**
64	A.10.9.1 Electronic Commerce	**Yes**
65	A.10.9.2 On-Line Transactions	**Yes**
66	A.10.9.3 Publicly Available Information	**Yes**
67	A.10.10.1 Audit Logging	**Yes**
68	A.10.10.2 Monitoring System Use	**Yes**
69	A.10.10.3 Protection Of Log Information	**Yes**
70	A.10.10.4 Administrator And Operator Logs	**Yes**
71	A.10.10.5 Fault Logging	**Yes**
72	A.10.10.6 Clock Synchronization	**Yes**
73	A.11.1.1 Access Control Policy	**Yes**
74	A.11.2.1 User Registration	**Yes**
75	A.11.2.2 Privilege Management	**Yes**
76	A.11.2.3 User Password Management	**Yes**
77	A.11.2.4 Review Of User Access Rights	**Yes**
78	A.11.3.1 Password Use	**Yes**
79	A.11.3.2 Unattended User Equipment	**Yes**
80	A.11.3.3 Clear Desk And Clear Screen Policy	**Yes**
81	A.11.4.1 Policy On Use Of Network Services	**Yes**
82	A.11.4.2 User Authentication For External Connections	**Yes**
83	A.11.4.3 Equipment Identification In Networks	**Yes**
84	A.11.4.4 Remote Diagnostic And Configuration Port Protection	**Yes**
85	A.11.4.5 Segregation In Networks	**Yes**
86	A.11.4.6 Network Connection Control	**Yes**
87	A.11.4.7 Network Routing Control	**Yes**

Control Seq. No.	ISO 27001 Annex A Control Name and Annex Reference Designation	Does It Apply to Teleworkers?
88	A.11.5.1 Secure Log-On Procedures	**Yes**
89	A.11.5.2 User Identification And Authentication	**Yes**
90	A.11.5.3 Password Management System	**Yes**
91	A.11.5.4 Use Of System Utilities	**Yes**
92	A.11.5.5 Session Time-Out	**Yes**
93	A.11.5.6 Limitation Of Connection Time	**Yes**
94	A.11.6.1 Information Access Restriction	**Yes**
95	A.11.6.2 Sensitive System Isolation	**Yes**
96	A.11.7.1 Mobile Computing And Communications	**Yes**
97	A.11.7.2 Teleworking	**Yes**
98	A.12.1.1 Security Requirements Analysis And Specification	**Yes**
99	A.12.2.1 Input Data Validation	**Yes**
100	A.12.2.2 Control Of Internal Processing	**Yes**
101	A.12.2.3 Message Integrity	**Yes**
102	A.12.2.4 Output Data Validation	**Yes**
103	A.12.3.1 Policy On The Use Of Cryptographic Controls	**Yes**
104	A.12.3.2 Key Management	**Yes**
105	A.12.4.1 Control Of Operational Software	**Yes**
106	A.12.4.2 Protection Of System Test Data	**Yes**
107	A.12.4.3 Access Control To Program Source Code	**Yes**
108	A.12.5.1 Change Control Procedures	**Yes**
109	A.12.5.2 Technical Review Of Applications After Operating System Changes	**Yes**
110	A.12.5.3 Restrictions On Changes To Software Packages	**Yes**
111	A.12.5.4 Information Leakage	**Yes**
112	A.12.5.5 Outsourced Software Development	**Yes**
113	A.12.6.1 Control Of Technical Vulnerabilities	**Yes**
114	A.13.1.1 Reporting Information Security Events	**Yes**
115	A.13.1.2 Reporting Security Weaknesses	**Yes**
116	A.13.2.1 Responsibilities And Procedures	**Yes**
117	A.13.2.2 Learning From Information Security Incidents	**Yes**

Control Seq. No.	ISO 27001 Annex A Control Name and Annex Reference Designation	Does It Apply to Teleworkers?
118	A.13.2.3 Collection Of Evidence	**Yes**
119	A.14.1.1 Including Information Security In The Business Continuity Management Process	**Yes**
120	A.14.1.2 Business Continuity And Risk Assessment	**Yes**
121	A.14.1.3 Developing And Implementing Continuity Plans Including Information Security	**Yes**
122	A.14.1.4 Business Continuity Planning Framework	**Yes**
123	A.14.1.5 Testing, Maintaining And Reassessing Business Continuity Plans	**Yes**
124	A.15.1.1 Identification Of Applicable Legislation	**Yes**
125	A.15.1.2 Intellectual Property Rights (IPR)	**Yes**
126	A.15.1.3 Protection Of Organizational Records	**Yes**
127	A.15.1.4 Data Protection And Privacy Of Personal Information	**Yes**
128	A.15.1.5 Prevention Of Misuse Of Information Processing Facilities	**Yes**
129	A.15.1.6 Regulation Of Cryptographic Controls	**Yes**
130	A.15.2.1 Compliance With Security Policies And Standards	**Yes**
131	A.15.2.2 Technical Compliance Checking	**Yes**
132	A.15.3.1 Information Systems Audit Controls	**Yes**
133	A.15.3.2 Protection Of Information Systems Audit Tools	**Yes**

(ISO, 2005).

References

Amigoni, M. and Gurvis, S. (2009). Managing the Telecommuting Employee: Set Goals, Monitor Progress, and Maximize Profit and Productivity. Avon, MA: Adams Media.

Brewer, D. and Nash, M. (2010). Insights into the ISO/IEC 27001 Annex A. Retrieved from the web at Retrieved from the web at https://buildsecurityin.us-cert.gov/swa/downloads/McCumber.pdf on August 1, 2012.

Chickowski, E. (2008). Telework Tips: 4 Strategies for Leading Remote Workers. An article published at the Baseline.com website on June 25, 2008. Retrieved from http://www.baselinemag.com/c/a/IT-Management/Telework-Tips-4-Strategies-for-Leading-Remote-Workers/ on June 25, 2012.

Congress. (2010). Telework Enhancement Act of 2010. Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1722enr/pdf/BILLS-111hr1722enr.pdf on June 25, 2012.

Dinnocenzo, D. (2006). How to Lead from a Distance: Building Bridges in the Virtual Workplace. Flower Mound, TX: The WALK THE TALK Company.

Fischer, K. (2000). The Distance Manager: A Hands On Guide to Managing Off-Site Employees and Virtual Teams. New York, NY: McGraw-Hill.

Froggatt, C. C. (2001). Work Naked: Eight Essential Principles for Peak Performance in the Virtual Workplace. New York, NY. Jossey-Bass Business & Management.

Gilbert, J. (2008). 10 signs that you aren't cut out to be a telecommuter. An article published on January 8, 2008 at TechRepublic.com. Retrieved from

http://www.techrepublic.com/blog/10things/10-signs-that-you-arent-cut-out-to-be-a-telecommuter/290?tag=content;siu-container on June 25. 2012.

ISO. (2005) "Information technology – Security techniques – Information security management systems – Requirements", ISO/IEC 27001:2005.

Lojeski, K. S., and Reilly, R. R. (2008). Uniting the Virtual Workforce: Tranforming Leadership and Innovation in the Globally Integrated Enterprise. Redmond, WA: Microsoft Corporation.

Nilles, J. M. (1998). Managing Telework: Strategies for Managing the Virtual Workforce. New York, NY: John Wiley & Sons.

OPM and GSA. (2011). Teleworking fundamentals for Managers. Retrieved from http://www.telework.gov/tools_and_resources/training/managers/index.aspx on June 25, 2012.

OPM and GSA. Annual Report of Teleworking – 2012. Retrieved from http://www.telework.gov/Reports_and_Studies/Annual_Reports/2012teleworkreport.pdf on July 12, 2012.

Policy Shield. (2011). Information Security Policies Written to Mitigate Risk Under the ISO 27001 Security Complicance Framework. Retreived from http://www.informationshield.com on March 15, 2011.

SANS. (2001). Mitigating Teleworking Risks. Retrieved from http://www.sans.org/reading_room/whitepapers/telecommunting/mitigating-teleworking-risks_314 on June 25, 2012.

Scarfone, K. and Souppaya, M. (2007). NIST SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access. NIST: Washington, DC. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf on June 25, 2012.

Scarfone, K.,et al. (2009). NIST SP 800-46, rev 1 - Guide to Enterprise Telework and Remote Access Security. NIST: Washington, DC. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf on June 25, 2012.

Telework Collaborative. (2012). Managing Telework. An article published at the Retrieved from the web at the Telework Arizona website. Retrieved from http://www.teleworkarizona.com/mainfiles/supervisor/smanagingtelework.htm on June 25, 2012.

Tuutti, C. (2012). Why federal managers resist telework. An article published at the Federal Computer Week website (www.fcw.com). Retrieved from http://fcw.com/articles/2012/07/11/reasons-federal-managers-resist-telework.aspx?s=fcwdaily_120712 on July 12, 2012.