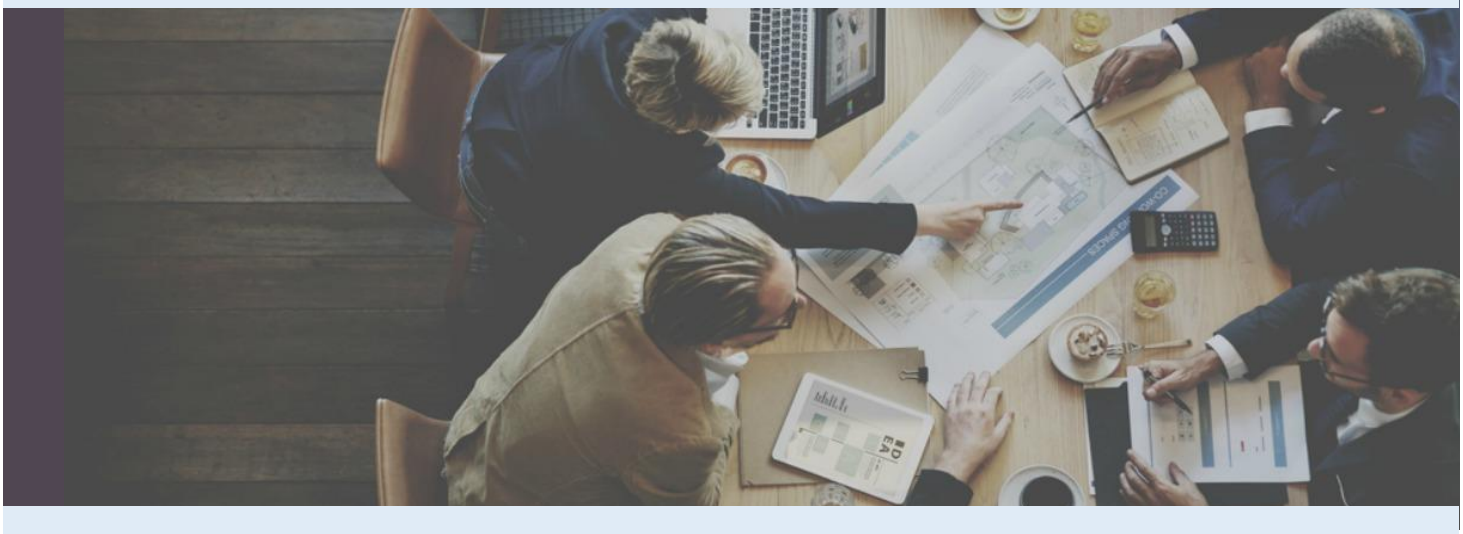
VERSION 1.0

FEBRUARY 19, 2018

IMPLEMENTING CONTROLS IN THE PAYROLL SYSTEM



Prepared by CompanyX
RYAN NYE, UNIVERSITY OF SAN DIEGO
CSOL 510 MODULE 7

1 IMPLEMENTING CONTOLS IN THE PAYROLL SYSTEM

WRITTED BY:	**Ryan Nye, Security Architect, Informatics, Inc**
	(MS CSOL Student)
REVIEWED BY:	**Donald F. Biedermann Jr., Manager of CompanyX.**
	(Professor)

SUBJECT:	**Implementation Proposal**
Start Date:	February 12, 2018
Published Date:	February 19, 2018
Questions:	T4lesfromthecrypto@gmail.com

PROJECT ASSUMPTIONS:	**Details**
Budget:	Large to accompany new systems and hardware
Size of Company:	Global, located in 84 countries

Disclaimer: The chosen case scenario is for learning purposes only. The plan presented in the case scenario is fictitious and are not intended to be implemented without professional consultation. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S., State, or local governments and University of San Diego. The information and statements shall not be used for the purposes of advertising.

2 CONTENTS

3 EXECUTIVE SUMMARY

CompanyX strives to provide a sound security architecture to maintain security costs and increasing usability for end-users. We take a holistic, enterprise-wide view when designing the system to make sure the systems run as smooth as before. One of our principles is consistency across the network to reduce complexity and simplify tasks for management. We first discuss minimum controls as outlined in FIPS 199, then provide tailored controls from NIST SP 800-53 for payroll through the lens of the CIA/AIC triad of Confidentiality, Integrity, and Availability of the payroll system and network. We simplified the control implementation process for payroll and provided Appendixes to further guide decision makers.

3.1 MINIMUM REQUIREMENTS

The minimum requirements involve 17 controls. Below we have recommended the key minimum controls for the payroll system. All controls should be defined in policy by the organization.

REQUIREMENT	IMPLEMENTATION
Access Control (AC)	Payroll domain to remain segregated from other networks. Access control list for IP addresses to be used (whitelist) Active Directory (AD) to define users with HR privileges
Awareness and Training (AT)	HR/Payroll to sign-off on security training for payroll duties
Audit and Accountability (AU)	Use recommendations of auditors to improve accountability
Certification, Accreditation, and Security Assessments (CA)	Accredited penetration tester to test controls and connections of payroll system.
Configuration Management (CM)	Set a policy for dual authorization for configuration changes.
Contingency Planning (CP)	Continuous and off-site backup of payroll data using secure and proven cloud technologies and security middleware
Identification and Authentication (IA)	Utilize Windows Active Directory to identify users and devices
Incident Response (IR)	Purchase network management middleware: Track network anomalies that surpass the network firewall.
Maintenance (MA)	Data sanitization (disk destruction) for devices used in payroll no longer in service.
Media Protection (MP)	Develop, maintain, disseminate policy for how payroll data will be stored and transported (never uploaded to USB)
Physical and Environmental Protection (PE)	Locked room (key card/fob) accessible to only specified management and support personnel (those support personnel with a demonstrated need for access). Entrance door is identified and marked. Payroll systems (internal or external) are housed in area free of environmental hazards (e.g. electrical surge, flooding, magnetic interference) and include appropriate climate controls (NIST, n.d.).

Planning (PL)	Access to Payroll domain defined in detail in IT architecture plans.
Personnel Security (PS)	Revoke user access to payroll systems when personnel has moved to another department or left organization.
Risk Assessment (RA)	Vulnerability scanning by accredited third party to check for unauthorized access to payroll network and system.
System and Services Acquisition (SA)	Use sound procurement methodologies that enable both performance and security of the organization; using service reviews.
System and Communications Protection (SC)	Cryptographic technologies and key management mythologies from reliable and secure products and services; use service reviews.
System and Information Integrity (SI)	IDS Middleware to detect threats targeting the payroll system.

3.2 TAILORED CONTROL FOR CONFIDENTIALITY

Confidentiality objective is achieved with encryption which covers both confidentiality and integrity. We can refer to NIST 800-53 Table D for Protection of Information at Rest SC-28 baselines and extended controls for low to moderate-impact information.

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
PROTECTION OF INFORMATION AT REST	MOD	SC-28	PROTECTION OF INFORMATION AT REST
	MOD	SC-28(1)	CRYPTOGRAPHIC PROTECTION
	Not Required	SC-28(2)	OFF-LINE STORAGE

For full table regarding control content, supplemental detail, and related controls see Appendix I.

3.2.1 IMPLEMENTATION

Windows for Business users can take advantage of BitLocker, a program that encrypts the disk drive of desktops and laptops. This prevents data from being viewed in the case the device is lost or stolen. The data will remain hidden according to the lifetime strength of encryption algorithms. Therefore, it is recommended that organizations use products with at least AES 256 with SHA-2 hashing functions. One program using AES 256 for data at rest is DropBox for file encryption. Drop box secures all files sent from desktop, mobile, API, and web through a TLS connection using AES 128. With these two technologies, a business can meet Protection at rest controls SC-28, (1), and (2).

3.3 TAILORED CONTROL FOR INTEGRITY

The foundation of integrity is encryption. Due to the nature of modern networks using cloud technology, protecting against remote attacks and encrypting data in transit to-and-from cloud source are critical. We can refer to NIST 800-53 Table D for Remote Access AC-17(2) baselines and extended controls for low to moderate-impact information:

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
Remote Access	LOW	AC-17	REMOTE ACCESS
	MOD	AC-17 (1)	AUTOMATED MONITORING AND CONTROL
		AC-17 (2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION
		AC-17 (3)	MANAGED ACCESS CONTROL POINTS
		AC-17 (4)	PRIVILEGED COMMANDS AND ACCESS

For full table regarding control content, supplemental detail, and related controls see Appendix I.

3.3.1 IMPLEMENTATION

Establishing remote access restriction policy to the network is priority when keeping the organization's data confidential. Rules include the following: which remote accounts and devices in the directory may have access to local applications. The organization can make use of an intranet to allow third parties submit work without being on the primary local network. The network as whole can include IP white lists and black lists on Cisco networks known as access control lists (ACLs). An organization may use a combination of VPN, token generator, and certificate to provide multi-authentication of remote users. Implementing these controls take care of AC-17, (2), (3), (4).

Modern network hardware provides interfaces for the administrator to view all internal and external connections to the network. Additional automated monitoring tools are critical to provide visibility to brute force attempts and rogue devices on the network. For example, Qualys automated monitoring suite allows the system administrative to view brute force login attempts on a cloud server allowing the administrator to respond to the threat (e.g. blacklisting IP address). Automated monitoring tools should be researched thoroughly and phased in to make sure tools are compatible and do not affect system performance. Implementing this control completes AC-17 (1) requirement.

One of the frauds in payroll involve "ghost employees" or users who have elevated privileges in the payroll system. We can refer to NIST 800-53 Table D for Identity Spoofing baselines and extended controls for low to moderate-impact information:

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS

Identity Spoofing	LOW	IA-12	IDENTITY PROOFING
		IA-12(1)	SUPERVISOR AUTHORIZATION
	MOD	IA-12(2)	IDENTITY EVIDENCE
		IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION
		IA-12(5)	ADDRESS CONFIRMATION

For full table regarding control content, supplemental detail, and related controls see Appendix X.

3.3.2 IMPLEMENTATION

All employees and contractors who have access to payroll systems should be identified and tracked by management. This can be achieved by a print-out or screenshot of the access control list from the software used when accessed in administrator mode and matched to their physical identity. Before the system administrator designates an employee to HR and provides access to HR systems, this should be approved by a supervisor before the addition is made. This request, should be written down in the organizations policy and communicated to the appropriate personnel.

To verify the user, pre-assigned pins, biometric, and traditional license/passport information can be analyzed to ensure the correct personnel is being registered. The job role should be clearly defined internally by the organizations on paper to prevent the user from elevating privileges on the spot with staff. To confirm identities during remote requests, address conformations (physical or digital) can be used. This is essentially multi-factor authentication. The user or HR representative can receive materials sent to the physical address or previously confirmed email address for access. Examples:

- Mailing temporary enrollment code to employee's physical address for employee benefits
- Emailing picture of yourself holding up license with request note, and date for password reset requests
- Bills that show name and address can be used for additional assurance for identity registration remotely

3.4 TAILORED CONTROL FOR AVAILABILITY

One threat that has gained tracking is records being no longer available due to ransomware. To ensure the availability of the payroll system data we will need a quick backup solution that can be used when existing records are no longer available. We can refer to NIST 800-53 Table D for system backup baselines and extended controls for low to moderate-impact information:

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
System Backup	LOW	CP-9	SYSTEM BACKUP
	MOD	CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY
		CP-9(8)	CRYPTOGRAPHIC PROTECTION

For full table regarding control content, supplemental detail, and related controls see Appendix I.

3.4.1 IMPLEMENTATION

Implementation depends upon the size of the business. Small business that can track employees on an excel spreadsheet with stand alone HR software. They can backup and encrypt data faster using simple tools available online. For example, for backup, they can use a cloud backup solution such as Microsoft OneDrive for Business (includes encryption) (Pcmag.com, n.d.). With a system like OneDrive, the business fulfills two out of three requirements: CP-9 and CP-9(8) shown above. The business can meet the CP-9(1) requirement of testing for reliability by scheduling tests throughout the year on another computer to check the data is still operational. Placing personal deadlines, policies, dates, reminders on when to conduct the tests will help enforce the CP-9(1).

For larger organizations, the backup solution may be tailored to the specific software or database type (e.g. SQL). In today's business, we see the current trend to outsource many functions to various cloud networks such as Office 365, AWS, and private clouds located on-site. Once practical solution for backup is Veeam, which offers off-site (for disaster recovery requirements) and on-site backup for the modern multi-cloud business. For payroll data being processed on one of Microsoft's cloud programs, Veeam will be able to copy the data as frequent that the user wants within its specifications to off-site or on-site location to be available instantly. With the built-in AES 256 bit encryption and error checking functions, Veam fulfills all three requirements CP-9, CP-9(1), and CP-9(8). It's important that the system administrator makes sure that the backup solution is compatible with the system they intend on backing up.

Some software may have their own backup and encryption solution running on the dedicated server. For example, some SQL databases may have their own backup scripts to create backup copies on a daily or weekly basis. To avoid performance issues of the database, most backups are scheduled during off hours as backing up can take up to a few hours (depending on size of database). To run these programs, the system administrator can use task scheduler to schedule the backup program to run at the most convenient time. It's important to note:

- No other CPU heavy tasks run at the same time of the backup
- Server is disconnected from the internet (security issue of backups and data)
- Opt-in to notifications from the vendor when backups are not running (fulfills CP-9(1))

4 APPENDIX I: MINIMUM REQUIREMENTS

REQUIREMENT	DESCRIPTION	IMPLEMENTATION
Access Control (AC)	Limit information access to authorized users and devices.	Develop, maintain, disseminate an access control policy. Use existing policy templates from open source. Payroll domain to remain segregated from other networks. Access control list for IP addresses to be used (whitelist) Active Directory (AD) to define users with HR privileges
Awareness and Training (AT)	Awareness of security risks and trained on information security responsibilities	Develop, maintain, disseminate a security and privacy policy. Use existing policy templates from open source. HR/Payroll to sign-off on security training for payroll duties
Audit and Accountability (AU)	Maintain auditability and ensure users can be uniquely traced in the system.	Use existing audit program policy and follow recommendations by auditors to improve existing program. Use recommendations of auditors to improve accountability
Certification, Accreditation, and Security Assessments (CA)	Periodically assess security of systems.	Develop, maintain, disseminate privacy assessment, authorization, and monitoring policy (from open source). Accredited penetration tester to test controls and connections of payroll system.
Configuration Management (CM)	Establish and maintain baseline hardware, software, firmware, and documentation.	Develop, maintain, disseminate configuration management policy (from open source). Set a policy for dual authorization for configuration changes.
Contingency Planning (CP)	Planning for emergency response and backup.	Develop, maintain, disseminate contingency planning policy (from open source). Continuous and off-site backup of payroll data using secure and proven cloud technologies and security middleware
Identification and Authentication (IA)	Identify users, processes, and devices.	Develop, maintain, disseminate identification and authentication policy (from open source). Utilize Windows Active Directory to identify users and devices
Incident Response (IR)	Detection, analysis, containment, and recovery.	Develop, maintain, disseminate identification an incident response policy (from open source).

		Purchase network management middleware: Track network anomalies that surpass the network firewall.
Maintenance (MA)	Effective controls on tools, techniques, mechanisms, and personnel used to conduct maintenance.	Develop, maintain, disseminate identification a system maintenance policy (from open source). Data sanitization (disk destruction) for devices used in payroll no longer in service.
Media Protection (MP)	Protection of both paper and digital media, sensitization and techniques before disposal or release for reuse.	Develop, maintain, disseminate identify a media protection policy (from open source). Develop, maintain, disseminate policy for how payroll data will be stored and transported (never uploaded to USB)
Physical and Environmental Protection (PE)	Limit physical access to IT systems and protect against environment hazards.	Develop, maintain, disseminate identification a physical access and environmental policy (from open source). Locked room (key card/fob) accessible to only specified management and support personnel (those support personnel with a demonstrated need for access). Entrance door is identified and marked. Payroll systems (internal or external) are housed in area free of environmental hazards (e.g. electrical surge, flooding, magnetic interference) and include appropriate climate controls (NIST, n.d.).
Planning (PL)	Develop, update, and implement security plans and rules.	Develop, maintain, disseminate identification an architectural planning policy (from open source). Access to Payroll domain defined in detail in IT architecture plans.
Personnel Security (PS)	Ensure individuals are occupying positions of responsibility are trustworthy.	Develop, maintain, disseminate identification a personnel security policy (from open source). Revoke user access to payroll systems when personnel has moved to another department or left organization.
Risk Assessment (RA)	Assess risk to operations (includes mission, functions, image, and reputation), assets and individuals.	Develop, maintain, disseminate identification a risk assessment policy (from open source). Vulnerability scanning by accredited third party to check for unauthorized access to payroll network and system.
System and Services Acquisition (SA)	SDLC consideration and restrictions for software	Develop, maintain, disseminate identification a system and service acquisition policy (from open source).

	usage and installation including third parties.	Use sound procurement methodologies that enable both performance and security of the organization; using service reviews.
System and Communications Protection (SC)	Architectural designs, development techniques, and engineering principles for system boundaries.	Develop, maintain, disseminate identification an encryption policy (from open source). Cryptographic technologies and key management mythologies from reliable and secure products and services; use service reviews.
System and Information Integrity (SI)	Protection against system flaws.	Develop, maintain, disseminate identification a system and information integrity policy (from open source). IDS Middleware to detect threats targeting the payroll system.

CONTROL ACTIVITY	DESCRIPTION	CONTROL ITEM
Hiring	Written process for hiring employees.	Approval of the position from a budget perspective
		Authorization to advertise job position
		Receipt of appropriate application information
		Participation in an established selection process
		Offering of position with letter from chief executive that includes annual salary or hourly rate, benefits, status (full vs part time) and classification according to the Fair Labor Standards Act (exempt vs. non-exempt).
Documentation	Proper documentation should be completed and authorized by the employee. Deductions (other than state and federal taxes) should not be withheld without a properly completed form from the employee.	Personal data that includes identifying information
		Form I-9, employment eligibility verification, determines eligibility to work in the United States. Employers should verify information using E-Verify system.
		Form W-4, Federal Withholding
		Form G-4, State Tax Withholding

		Benefits forms including health, dental and other plans
		Retirement plan forms
	Online document submission is properly secured.	Transmission of data is secured, with user requirement of login name and password
		Direct deposit registration requires a cancelled check along with an authorization form
Authorization	Ensure only valid transactions are entered in the payroll system, all transactions should be properly authorized.	Time sheets: employee should certify the time recorded was the time actually worked. Supervisor should approve the time sheets and signature serves as authorization to pay employee. If any leave is taken, the supervisor is to properly record leave dates.
		Payroll: Payroll checks and direct deposit should not be generated until a supervisor has authorized the payroll. Supervisor should verify all supporting documentation is present prior to approving the payroll. The payroll may have tailored controls if payroll is manual or electronically approved.
Reconciliation	Accurate reconciliation of amounts and accounts.	Hours Worked:
		Adjusted Gross Salary:
		Taxable Wages:
		Retirement Contributions:
		Flexible Spending Account Deductions:
(Development District Association of Appalachia [DDAA], n.d.)		

5 APPENDIX II: NIST 800-53 CONTROLS

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
PROTECTION OF INFORMATION AT REST	MOD	SC-28	PROTECTION OF INFORMATION AT REST Protect the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information] at rest.
			SUPPLEMENTAL This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of this control is not on the type of storage device or frequency of access but rather the state of the information. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection and prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other security controls including, for example, frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage.
			RELATED CONTROLS AC-3, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5,PE-3, SC-8, SC-13, SC-34, SI-3, SI-7, SI-16.
		SC-28(1)	CRYPTOGRAPHIC PROTECTION Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] when at rest on [Assignment: organization-defined system components].
			SUPPLEMENTAL This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage. It also applies to limited quantities of media generally

			associated with system components in operational environments including, for example, portable storage devices, notebook computers, and mobile devices. Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt all information on storage devices or encrypt specific data structures including, for example, files, records, or fields. Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.
			RELATED CONTROLS AC-19, SC-12
	Not Required	SC-28(2)	OFF-LINE STORAGE Remove the following information from online storage and store off-line in a secure location: [Assignment: organization-defined information].
			SUPPLEMENTAL Removing organizational information from online system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.
			RELATED CONTROLS None.

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
Remote Access	LOW	AC-17	REMOTE ACCESS
			SUPPLMENTAL Remote access is access to organizational systems (or processes acting on behalf of users) communicating through external networks such as the Internet. Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, Executive

			Orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.
			AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SI-4.
	MOD	AC-17 (1)	AUTOMATED MONITORING AND CONTROL Monitor and control remote access methods.
			SUPPLEMENTAL Automated monitoring and control of remote access methods allows organizations to detect attacks and ensure compliance with remote access policies by auditing connection activities of remote users on a variety of system components including, for example, servers, workstations, notebook computers, smart phones, and tablets.
			RELATED CONTROLS AU-2, AU-6, AU-12, AU-14
		AC-17 (2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
			SUPPLEMENTAL The encryption strength of mechanism is selected based on the security categorization of the information.
			RELATED CONTROLS SC-8, SC-12, SC-13
		AC-17 (3)	MANAGED ACCESS CONTROL POINTS Route all remote accesses through Assignment: organization-defined number] managed network access control points.
			SUPPLEMENTAL Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections initiative requirements for external network connections.

			RELATED CONTROLS SC-7
		AC-17 (4)	PRIVILEGED COMMANDS AND ACCESS (a) Authorize the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Document the rationale for such access in the security plan for the system.
			SUPPLEMENTAL None.
			RELATED CONTROLS AC-6
CONTROL NAME	**IMPACT LVL**	**CONTROL CODE**	**800-53 CONTROLS**
Identity Spoofing	LOW	IA-12	IDENTITY PROOFING a. Identity proof users that require Accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence
			SUPPLMENTAL Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system. This control is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include NIST Special Publications 800-63 and 800-63A.
			RELATED CONTROLS IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8
		IA-12(1)	SUPERVISOR AUTHORIZATION Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.
			SUPPLEMENTAL None.
			RELATED CONTROLS None.
	MOD	IA-12(2)	IDENTITY EVIDENCE Require evidence of individual identification be presented to the registration authority.
			SUPPLEMENTAL Requiring identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to

			establish an identity, or at least increases the work factor of potential adversaries. Acceptable forms of evidence are consistent with the risk to the systems, roles, and privileges associated with the user's account.
			RELATED CONTROLS None.
		IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].
			SUPPLMENTAL Validating and verifying identity evidence increases the assurance that that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic and that the data contained in the evidence is correct, current, and related to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the systems, roles, and privileges associated with the users account.
			RELATED CONTROLS None.
		IA-12(5)	ADDRESS CONFIRMATION Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.
			SUPPLMENTAL To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to increase assurance that the individual associated with an address of record was the same person that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts are obtained from records and not self-asserted by the user. The address can include a physical or a digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.
			RELATED CONTROLS IA-12

CONTROL NAME	IMPACT LVL	CONTROL CODE	800-53 CONTROLS
System Backup	LOW	CP-9	SYSTEM BACKUP a. Conduct backups of user-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conduct backups of system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protect the confidentiality, integrity, and availability of backup information at storage locations.
			SUPPLMENTAL System-level information includes, for example, system-state information, operating system software, application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed to protect the integrity of system backups include, for example, digital signatures and cryptographic hashes. Protection of backup information while in transit is beyond the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information
			RELATED CONTROLS CP-2, CP-6, CP-10, MP-4, MP-5, SC-13, SI-4, SI-13
	MOD	CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.
			SUPPLMENTAL None.
			RELATED CONTROLS CP-4
		CP-9(8)	CRYPTOGRAPHIC PROTECTION Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].
			SUPPLMENTAL

			The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to system backup information in storage at primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.
			RELATED CONTROLS SC-12, SC-13, SC-28

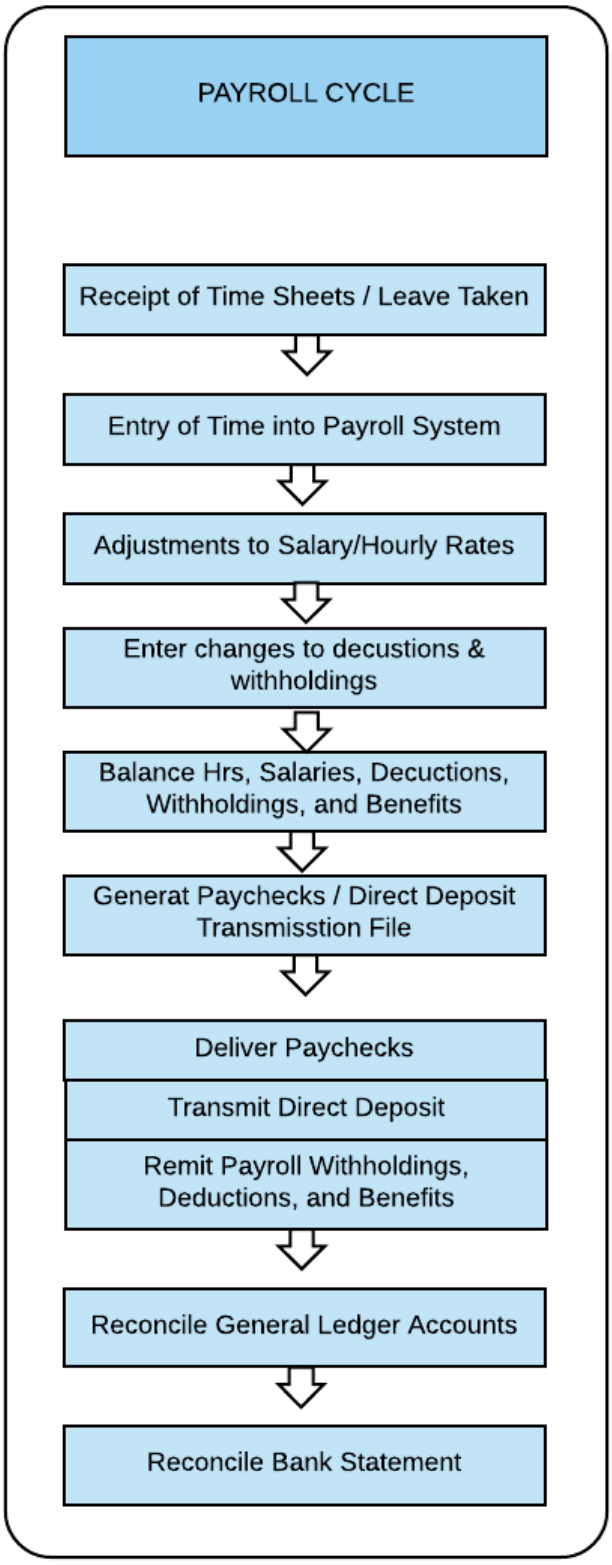
6 APPENDIX III: TYPES OF INFORMATION AND COMMUNICATION OF PAYROLL

INFORMATION	DESCRIPTION
Enrollment Periods for Benefits	Plan options and dates for enrollment
Pay Periods and Dates	Dates of pay period due date for time sheets, and pay date
Holidays	Scheduled paid holidays
Furlough days	Scheduled furloughed days to be communicated to employees
Personnel Policies and Procedures	Employees to have access to detailed policies and procedures related to employment with government.
Salary Information	Employees should receive annual notification of changes in pay rate or salary
Benefits Payment	Benefit providers must receive timely information regarding employee enrollments
Tax Withholding & Reports	Must be sent to federal and state government agencies.
(DDAA, n.d.)	

7 APPENDIX IV: MONITORING OF PAYROLL

MONITORING ACTIVITIES	DESCRIPTION
Regular management and supervisor activities	Traditional management activities of performance review and authorization.
Supervisor activities of Payroll	Supervisor should initial and date the face of the reconciliation and evidence of the review. Supervisor to review all changes to employee information by producing an employee addition & change report.
(DDAA, n.d.)	

8 APPENDIX V: PAYROLL CYCLE & SUMMARY



(Development District Association of Appalachia, n.d.)

9 APPENDIX V: RISK ASSESSMENT

OBJECTIVE	RISK EVENT
Authorization	Hiring an employee that was not approved or not eligible for employment.
	Overspending of budget from unauthorized hiring
	Appropriate supervisors make the final decision regarding the candidate's qualifications
	Incorrect employee classification for benefits eligibility and Fair Labor Standards Act status may occur if hiring does not follow the eligibility process
Safeguarding Assets	Intentional change or unintentional mistake in salary, wages, or withholdings.
	Failure to observe payroll deadlines may result in penalties and interest
	Fictitious employees added to payroll
	Employees may be improperly classified: Fair Labor Standards Laws and Internal Revenue Service Code require proper classification of employees
	Employee may not properly report leave taken
Accurate, Reliable, Timely Information	Employee's salary or pay rate may be incorrectly entered. Results in incorrect financial reports.
	Hours or pay period may be incorrectly entered. Results in overstatements of expenditures incurred and unrecorded liability for time worked but not paid.
	Deduction data may be improperly entered. Deductions of health, dental, life, retirement, require the vendor based on a predetermined schedule in order for coverage to be effective.
	Payroll may be generated but not posted to the general ledger. This created an understatement of expenditures and an overstatement of cash in the general ledger.

10 REFERENCES

Development District Association of Appalachia. (n.d.). *Chapter 4: Effective Internal Controls Over Payroll.* Ddaa-ldd.org. Retrieved February 16, 2018 from http://ddaaldd.org/documents/FY15_IC_Payroll_Chapter_4_Effective_IC_over_Payroll.pdf

Manageengine. (n.d.). *Network traffic monitoring software for in-depth traffic analysis*. manageengine.com. Retrieved February 19, 2018 from https://www.manageengine.com/products/netflow/

NIST. (n.d.). *Summary Privacy Impact Assessment (PIA).* NIST.gov. Retrieved February 18, 2018 from https://www.nist.gov/document-17608

PCMAG. (n.d.). *Business Software Index: Encryption*. Pcmag.com. Retrieved from https://www.pcmag.com/business/directory/encryption

Qualys. (n.d.). *Unparalleled visibility, end-to-end IT security and compliance for all your assets*. qualys.com. Retrieved February 19, 2018 from https://www.qualys.com/

Veeam. (n.d.). *#1 Availability for Multicloud Enterprise.* Veeam.com. Retrieved February 19, 2018 from https://www.veeam.com/backup-files-encryption.html