State of Michigan
Civil Service Commission

Capitol Commons Center, P.O. Box 30002
Lansing, MI 48909

Position Code
1. DEPSPL2

POSITION DESCRIPTION

This position description serves as the official classification document of record for this position. Please complete the information as accurately as you can as the position description is used to determine the proper classification of the position.

2. Employee's Name (Last, First, M.I.)	**8. Department/Agency** MDHHS-COM HEALTH CENTRAL OFF
3. Employee Identification Number	**9. Bureau (Institution, Board, or Commission)** Compliance and Data Governance Bureau
4. Civil Service Position Code Description Departmental Specialist-2	**10. Division** Privacy, Security and Data Governance
5. Working Title (What the agency calls the position) Departmental Specialist	**11. Section** Data Protection & Management Section
6. Name and Position Code Description of Direct Supervisor VISSER, LAURA M; STATE ADMINISTRATIVE MANAGER-1	**12. Unit**
7. Name and Position Code Description of Second Level Supervisor BOWEN, JAMES R; STATE DIVISION ADMINISTRATOR	**13. Work Location (City and Address)/Hours of Work** 235 S. Grand Ave, Lansing, MI 48933 / Monday-Friday 8:00am-5:00pm

14. General Summary of Function/Purpose of Position

This position serves as the Security Specialist responsible for the development, implementation, coordination, and evaluation of security, privacy, and regulatory compliance activities required to ensure MDHHS adherence to federal and state standards, including NIST SP 800-53, IRS Publication 1075, and other applicable frameworks. Responsibilities include conducting and overseeing System and Organization Controls (SOC) report reviews; coordinating and participating in onsite security and compliance audits; evaluating application security scanning results; and managing all associated Plan of Action and Milestones (POAM) in Keylight to ensure required remediation is completed in accordance with established timelines. The position develops and maintains departmental security policies, procedures, and standards; assesses audit findings and risk evaluations; and recommends corrective actions to enhance internal controls and strengthen agency compliance posture. The incumbent also develops and delivers security, privacy, and compliance training and provides expert guidance to MDHHS leadership, program areas, and technical staff regarding security requirements, risk mitigation, and regulatory obligations.

15. Please describe the assigned duties, percent of time spent performing each duty, and what is done to complete each duty.

List the duties from most important to least important. The total percentage of all duties performed must equal 100 percent.

Duty 1

General Summary: **Percentage:** **50**

Security Specialist responsible for departmental program oversight by conducting detailed reviews of System and Organization Control (SOC) reports and coordinating onsite audits of vendors, systems, and internal programs to ensure compliance with state and federal security, privacy, and regulatory requirements. The position evaluates operational practices, verifies implementation of required controls, identifies risks, and provides recommendations to strengthen internal controls, inform policy decisions, and maintain program compliance.

Individual tasks related to the duty:

- Reviews and analyzes SOC 1 and SOC 2 reports for completeness, accuracy, and adherence to established security and compliance standards, collecting and maintaining program data necessary for reporting, evaluation, and audit readiness.
- Plans, schedules, and conducts onsite audits of vendors, systems, and internal programs to evaluate adherence to required security, privacy, and regulatory standards.
- Reviews documentation and verifies the implementation of required controls, analyzing ongoing program operations and recommending modifications to policies, procedures, and internal control practices to improve compliance.
- Identifies control gaps, exceptions, and areas requiring corrective action, documenting audit observations, findings, and recommendations to support program decision-making and compliance monitoring.
- Assists business areas in reviewing and completing end-user controls and supports preparation for state, federal, and partner agency audits by gathering required documentation and ensuring program readiness.
- Collaborates with internal and external partners to validate compliance requirements, clarify security obligations, and assess compatibility of vendor and system practices with state objectives and standards.
- Follows up on audit findings to ensure appropriate corrective actions are implemented, serving as a liaison among state program areas, vendors, auditors, and federal partners to coordinate compliance efforts and program oversight.
- Conducts special reviews and targeted analyses of security documentation and operational practices, providing expert recommendations to strengthen controls and reduce organizational risk.

Duty 2

General Summary: **Percentage:** **25**

Provides leadership and expert guidance in developing, updating, and maintaining departmental security policies, procedures, and standards. Conducts advanced research, evaluates emerging regulatory and security requirements, and advises executive leadership on strategic direction. This role ensures policies align with statewide objectives, federal mandates, and industry best practices, and serves as the department's subject-matter expert on security governance.

Individual tasks related to the duty:

- Leads the drafting, revision, and publication of departmental security policies, procedures, and standards to ensure alignment with state and federal requirements, emerging best practices, and strategic program goals.
- Conducts high-level research and analysis of emerging security frameworks, regulatory changes, and national best practices, recommending updates to departmental policy and security governance models.
- Provides expert consultation to internal leadership, program managers, and technical teams on the interpretation and application of security policies, regulatory obligations, and risk impacts.
- Reviews existing departmental policies and enterprise security controls to identify policy gaps, areas of inconsistency, and opportunities to strengthen governance structures.
- Evaluates the effectiveness of implemented policies and standards, recommending strategic modifications to improve internal controls, strengthen compliance posture, and support organizational risk reduction.

Duty 3

General Summary: **Percentage:** **15**

Authoritative reviewer for Microsoft Teams workspaces, SharePoint sites, and software/application solution requests. Evaluates, approves, and governs the use of collaboration platforms and technologies to ensure compliance with departmental security, privacy, and data governance requirements. This role exercises expert-level judgment, interprets complex security standards, advises leadership, and ensures technology decisions align with departmental strategy and enterprise architecture.

Individual tasks related to the duty:

- Reviews and evaluates requests for new Microsoft Teams workspaces and SharePoint sites to ensure alignment with security, privacy, data governance, and enterprise architecture requirements.
- Performs advanced evaluation of software and application requests, assessing security controls, data handling requirements, interoperability, access management, and technical risk.
- Approves, denies, or conditionally approves requests based on authoritative interpretation of regulatory requirements, departmental policy, risk tolerance, and operational impact.
- Coordinates with statewide IT, enterprise security, architecture teams, and business area leadership to validate business needs, assess risks, and ensure technology solutions align with statewide and departmental priorities.
- Documents all review decisions, required corrective actions, risk mitigation steps, and communications in accordance with departmental procedures and audit requirements.
- Conducts special studies or targeted analyses related to collaboration platform governance, emerging risks, or process improvements, providing expert recommendations to executive leadership.

Duty 4

General Summary: **Percentage:** **10**

Oversees and manages the Plan of Action and Milestones (POAM) program. Provides expert leadership in ensuring timely, accurate, and compliant remediation of security, audit, and regulatory findings. This role interprets complex federal and state requirements, establishes governance standards, advises executive leadership, and ensures that remediation activities align with departmental risk management strategy and statewide security frameworks.

Individual tasks related to the duty:

- Leads the creation, maintenance, and governance of POAMs for vulnerabilities, audit findings, compliance gaps, and issues identified through security assessments, SOC reviews, application scanning, or oversight entities.
- Monitors remediation progress across all program areas, validates completion, and ensures corrective actions meet state and federal regulatory requirements, including NIST and IRS Publication 1075.
- Ensures all POAM entries meet federal and state documentation standards, including required descriptions, risk assessments, milestones, justifications, due dates, and evidence of closure.
- Provides expert consultation to system owners, program leadership, and technical teams regarding remediation expectations, regulatory requirements, timelines, and risk implications.
- Coordinates cross-departmental collaboration by gathering updates, addressing delays, resolving barriers to remediation, and advising leadership on corrective action strategies.
- Prepares, analyzes, and delivers comprehensive POAM status reports for departmental leadership, auditors, regulatory agencies, and oversight bodies, ensuring accuracy and readiness for review.
- Escalates overdue, high-risk, or non-compliant POAMs to senior leadership and recommends risk mitigation strategies to maintain adherence to statewide security policies and federal regulations.

16. Describe the types of decisions made independently in this position and tell who or what is affected by those decisions.

The position evaluates and makes decisions regarding the review and approval of SOC reports, onsite audit findings, and technology requests, including Microsoft Teams workspaces, SharePoint sites, and software/application requests. Decisions include determining whether vendors, systems, and requested tools meet departmental security, privacy, and compliance standards; identifying risks and required mitigation; and approving, denying, or conditionally approving requests based on technical and regulatory requirements. The position also determines the need for updates to policies and procedures and identifies staff training requirements to address gaps in compliance or knowledge.

17. Describe the types of decisions that require the supervisor's review.

Decisions that require supervisory approval include those involving policy changes that have department-wide impact, significant deviations from established security or compliance standards, or situations where guidance is unclear or conflicting across regulatory frameworks. Requests that require new resources, budget considerations, procurement activities, or commitments on behalf of the department are also referred to the supervisor.

Additionally, issues involving high-risk audit findings, unresolved vendor non-compliance, or decisions that could affect federal reporting requirements, funding eligibility, or interagency agreements are escalated for supervisory review. Matters involving sensitive political, legal, or executive-level implications, as well as decisions outside the established scope of authority for a Specialist 13, must also be brought forward for supervisory direction.

18. What kind of physical effort is used to perform this job? What environmental conditions in this position physically exposed to on the job? Indicate the amount of time and intensity of each activity and condition. Refer to instructions.

General Office Setting

19. List the names and position code descriptions of each classified employee whom this position immediately supervises or oversees on a full-time, on-going basis.

Additional Subordinates

20. This position's responsibilities for the above-listed employees includes the following (check as many as apply):

N	Complete and sign service ratings.	N	Assign work.
N	Provide formal written counseling.	N	Approve work.
N	Approve leave requests.	N	Review work.
N	Approve time and attendance.	N	Provide guidance on work methods.
N	Orally reprimand.	N	Train employees in the work.

22. Do you agree with the responses for items 1 through 20? If not, which items do you disagree with and why?

Yes

23. What are the essential functions of this position?

The essential functions of this position include serving as the specialist for security and compliance activities within the department. This includes independently conducting SOC report reviews, coordinating and performing onsite audits, evaluating security and privacy risks, and making recommendations to ensure departmental compliance with state and federal requirements. The position is responsible for developing, updating, and maintaining security and compliance policies and procedures, as well as creating and delivering training to ensure staff understand and adhere to established standards.

The position also independently reviews and approves Microsoft Teams workspaces, SharePoint sites, and software/application requests to ensure alignment with security, privacy, and governance requirements. Additional essential functions include collaborating with internal and external stakeholders, supporting audit readiness activities, analyzing complex regulatory information, and providing expert guidance to program areas. These duties require regular communication, critical thinking, and the ability to work effectively with others.

24. Indicate specifically how the position's duties and responsibilities have changed since the position was last reviewed.

New establishment.

25. What is the function of the work area and how does this position fit into that function?

The function of this position is to serve as the specialist for security, privacy, and compliance activities within the department. The position independently conducts SOC report reviews, performs onsite audits, evaluates security risks, and ensures departmental compliance with state and federal regulations. The employee develops and maintains security and compliance policies, creates and delivers staff training, and provides expert-level guidance on matters involving data protection, IT governance, and regulatory standards.

The position also functions as the primary reviewer and approver for Microsoft Teams workspaces, SharePoint sites, and software/application requests, ensuring alignment with departmental security, privacy, and governance requirements. Through these activities, the position supports operational readiness, audit preparedness, and the protection of departmental data assets.

26. What are the minimum education and experience qualifications needed to perform the essential functions of this position.

EDUCATION:

Possession of a bachelor’s degree in any major.

EXPERIENCE:

Departmental Specialist 13 - 15
Four years of professional experience, including two years equivalent to the experienced (P11) level or one year equivalent to the advanced (12) level.

KNOWLEDGE, SKILLS, AND ABILITIES:

As listed on the Civil Service job specification. In addition:

- Ability to develop and maintain positive, strong, and credible professional and interpersonal relationships with all
- parties associated with MDHHS projects, and represents the best interests of MDHHS at all times.
- Critical thinking and the ability to problem solve through analytical methods and creative thinking.
- Highly organized and disciplined.
- In-depth knowledge of the national security requirements and technology laws including NIST, HIPAA, IRS, SSA,
- CJIS, FERPA, etc.
- Knowledge of other industry information security standards and programs including FISMA, FFIEC, COBIT, SOX GLB,
- PCI, ISO 27001, Fedramp, etc.
- Outstanding interpersonal and communication skills.
- Must possess a high degree of integrity and trust along with the ability to work independently.
- Excellent written communication skills (A writing sample should be provided as part of your application packet.)
- Proficiency in presentation software (e.g., Microsoft PowerPoint) or the demonstrated ability to learn quickly.
- Ability to weigh business risks and enforce appropriate information security measures.
- Technically savvy and interested in emerging technology, able to quickly evaluate technology for information security
- risk.

The MDHHS mission is to provide opportunities, services, and programs that promote a healthy, safe, and stable environment for residents to be self-sufficient. We are committed to ensuring a diverse workforce and a work environment whereby all employees are treated with dignity, respect, and fairness.

CERTIFICATES, LICENSES, REGISTRATIONS:

None

NOTE: Civil Service approval does not constitute agreement with or acceptance of the desired qualifications of this position.

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

Supervisor **Date**

TO BE FILLED OUT BY APPOINTING AUTHORITY

Indicate any exceptions or additions to the statements of employee or supervisors.

None

I certify that the entries on these pages are accurate and complete.

HILLARY PLATTE 7/13/2026

Appointing Authority **Date**

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

Employee **Date**