Final Internship Paper

Date: April 23, 2025
Name: Muhammad Rabiu
Employer: Charlotte Kimbro
Company/Agency: Old Dominion University - ITS
Internship Class: CYSE 368 – Internship
Term: Spring 2025

Table of Contents

1. Introduction

Choosing to intern with Old Dominion University's Information Technology Services (ITS) department was not only a strategic decision but a personal one. As a cybersecurity major with a growing interest in IT systems management and network security, I sought an environment that would bridge my academic learning with tangible, high-impact experience. The ITS department offered more than a student job—it provided access to a functioning support system that maintains the digital backbone of the university.

My first objective was to deepen my practical knowledge of enterprise-level IT support systems, especially ServiceNow, Microsoft Endpoint Manager, and network diagnostics tools. I wanted to see how these tools were used in real-time environments. Second, I aimed to enhance my cybersecurity decision-making, applying the NIST framework principles to real-world technical issues and service requests. Finally, I hoped to develop soft skills critical to the field, such as user communication, time prioritization, and documentation, all of which are vital to successful incident response and security operations.

This paper captures the progression of those goals. It covers every aspect of the 300-hour experience with the ITS Desktop Support Group, including the initial onboarding and adjustment period, as well as the main duties, difficulties, successes, and lessons learned. Every segment showcases a different aspect of development, emphasizing the improved technical and social abilities as well as the connections made between academia and real-world applications throughout the internship.

2. Business Overview and Internship Start

I worked as an intern in the Desktop Support Group of Old Dominion University's Information Technology Services (ITS) division. In higher education, ODU, a public research university in Norfolk, Virginia, has a long history of being innovative and approachable. The university was founded in 1930 and now has over 20,000 diverse students enrolled. The ITS department is responsible for maintaining campus-wide network infrastructure, providing technical support, and ensuring cybersecurity compliance. I worked in the Desktop Support Group during my internship, which was in charge of maintaining endpoint devices (such as PCs and laptops), fixing technical issues, and helping staff, students, and teachers with security configurations.

An organized orientation marked the start of my position as an ITS Student Worker. I went to a training session during the first week that covered the team's operational processes, communication protocols, and usage of internal tools such as Microsoft Endpoint Configuration Manager and ServiceNow. Security procedures, password management, customer service manners, and system escalation routes were all highlighted in the training. I was given access credentials after passing basic security awareness training and completing simulations to familiarize myself with remote assistance tools and documentation processes.

My first thoughts were conflicted. On the one hand, ODU's IT infrastructure's size and professionalism pleased me. I really liked how teamwork and lifelong learning were emphasized. But I soon discovered how flexible and erratic IT help might be. Issues would range from forgotten passwords to network reconfigurations and OS-level bugs. Each required rapid response, patience, and clear communication skills I had some experience in but would need to sharpen significantly.

From the outset, the environment challenged me to adapt quickly. I was not just observing professionals; I was expected to function like one. And this immediate responsibility gave me a sense of ownership that transformed this internship into something more than just a resume item. It became a proving ground for the skills I had spent years developing, both academically and personally.

3. Management Environment

The management structure at the Desktop Support Group within ODU's Information Technology Services was practical, hierarchical, and collaborative. My direct supervisor was Charlotte Kimbro, who managed day-to-day operations and task delegation. She balanced providing guidance and allowing interns to develop autonomy. Her leadership style was accessible. She encouraged us to ask questions but also expected initiative and follow-through. Weekly check-ins were scheduled to monitor progress and clarify expectations, but beyond that, most communication happened through a shared Microsoft Teams workspace and ServiceNow ticketing queues.

Above her, there were senior analysts and IT engineers responsible for larger-scale rollouts and security protocols. Their presence set the tone for a high-performance culture. Even though I didn't report to them directly, I observed how team leads made infrastructure decisions, prioritized support requests based on impact levels, and collaborated with security teams to enforce compliance. The level of coordination between the support staff and the cybersecurity division was something I had only previously encountered in theory. Here, I saw it live—policy trickled down through channels, and team members knew exactly how to implement changes without redundancy or confusion.

One standout feature of this environment was its hybrid style of supervision. Early tasks were micro-managed, ensuring we didn't make avoidable mistakes. But as time progressed, supervisors allowed for more independence. By week four, I was resolving tickets end-to-end with minimal oversight, submitting reports, and being trusted to communicate directly with faculty members to schedule hardware servicing or security patches. This gradual scaling of responsibility helped me build confidence, and it also exposed me to real-world management protocols: escalation chains, prioritization models, and customer satisfaction tracking.

What made the environment so effective was not just the hierarchy—it was how mentorship was embedded into every layer. Senior workers didn't just fix issues—they explained their logic, walked me through their diagnostic thought processes, and often followed up to make sure I understood. That mentorship mindset turned the job into a developmental space. I wasn't just a student worker—I was part of the structure, learning the language, pace, and culture of enterprise-level IT.

4. Work Duties and Assignments

As an ITS Student Worker within ODU's Desktop Support Group, my core responsibilities revolved around technical support, system maintenance, and service ticket resolution. From my first day, I was integrated into the ServiceNow platform, the university's centralized IT support system. My duties began with managing Level 1 tickets—password resets, basic connectivity issues, and peripheral setup. But as I gained trust, I moved into more complex assignments, including software installations, endpoint compliance audits, and configuration of networked devices.

One recurring task involved preparing university-owned laptops for new hires or lab environments. This included imaging systems using Windows Deployment Services (WDS), installing required academic software like SPSS or MATLAB, and configuring user accounts with proper permissions under Active Directory. These tasks weren't isolated—they were tied to academic calendar cycles, meaning that deadlines were strict and errors had immediate consequences for department productivity.

Another critical project was helping implement security compliance checks during random audits. I worked with team members to confirm that all devices were encrypted, running the latest security patches, and compliant with the university's endpoint protection policies. In one case, we discovered that a batch of faculty desktops had not received the most recent Microsoft Defender update due to a Group Policy misconfiguration. I assisted in drafting a mini-report and executing a fix that ensured compliance across over 50 machines.

Network troubleshooting was another component. Using basic diagnostic tools (ping, ipconfig, nslookup), I addressed Wi-Fi connectivity issues, IP conflicts, and DNS resolution problems. These tasks gave me first-hand experience in understanding how physical network layers interact with policy-driven security environments—something that textbooks only hint at.

During the midterm push, I helped configure and troubleshoot Zoom and hybrid classroom tech setups. These responsibilities were essential not just for user satisfaction but for academic continuity. The pressure was real—if a system failed mid-lecture, faculty relied on our team to restore function immediately.

I also created documentation: step-by-step setup guides for student labs, onboarding checklists for new users, and quick reference sheets for common troubleshooting steps. This improved support consistency and reduced repetitive inquiries.

Every assignment I touched connected directly to organizational operations. Without the configurations, patches, and issue resolutions we performed, classroom sessions would halt, research data could be compromised, and systems would lose efficiency. My work wasn’t auxiliary—it was foundational.

5. Cybersecurity Skills Utilization

Cybersecurity wasn't just a background principle during my internship—it was embedded in nearly every action I took. From handling faculty login requests to installing endpoint security updates, I was consistently applying security concepts learned in class. The work I performed wasn't theoretical. Each click had real-world implications: data confidentiality, device integrity, and user access control.

I entered this internship with a strong foundation in core cybersecurity principles—CIA triad, secure configurations, authentication protocols, and awareness of compliance standards like NIST. This helped me hit the ground running. For instance, when provisioning systems, I made sure user privileges followed the principle of least privilege. It would've been easier to assign blanket administrative rights to faculty systems, but we enforced tiered access to reduce risk vectors.

I also applied my understanding of patch management. I remember identifying a vulnerability flagged in a ServiceNow ticket where a user's system hadn't updated Adobe Reader for several cycles. Instead of simply executing the update, I traced the source of the delay and found that their machine was excluded from the auto-update group policy. That small discovery led to a wider audit, which exposed six other similar cases. Resolving them wasn't just about patching—it was about tightening administrative gaps.

Firewall settings and endpoint detection tools like Microsoft Defender and CrowdStrike were part of my daily exposure. One assignment involved assessing whether certain lab machines were reporting their logs correctly. We discovered that while the antivirus tool was installed, it hadn't been configured to communicate with the central dashboard. I collaborated with a full-time staff member to script a fix that enabled log forwarding across a batch of machines.

Password hygiene and multi-factor authentication (MFA) were also front and center. I assisted users in setting up MFA via Duo and explained why long, complex passphrases were more effective than frequent resets. Sometimes, I'd give mini-tutorials during support calls—bridging the gap between help desk support and cybersecurity awareness training.

I also developed soft cybersecurity instincts—recognizing when a user report may hint at phishing (e.g., "strange popups," "weird login prompts," etc.). While I wasn't part of the Security Operations Center, I documented these alerts and passed them to the appropriate teams.

The internship made cybersecurity real. In a classroom, you simulate breaches. On the job, you prevent them. That shift changed how I viewed the role of an analyst. You're not just scanning logs—you're protecting daily operations. You're invisible when everything works, but you're the front line when it doesn't.

6. ODU Curriculum Connection

The ODU curriculum, especially within the School of Cybersecurity, gave me the right skeleton, but the internship added the muscle. Many of the tools, concepts, and frameworks I encountered on the job had been introduced in theory through coursework like CYSE 200, CYSE 270, and CYSE 330. However, seeing those theories play out in a real-world university IT environment made all the difference.

For instance, my understanding of system architecture, layered security, and user access control was primarily formed in lecture halls. But in my role, I had to apply those principles with actual users, machines, and policies that didn't always align perfectly with the textbook. It forced me to adapt. A clear example was learning how Microsoft Endpoint worked alongside Group Policy—something not directly taught in any course, but made easier to grasp because of my foundation in secure system design.

Courses in risk management and cybersecurity policy were also helpful, especially when communicating with supervisors or users about potential issues. For example, when I identified machines that were excluded from automatic antivirus updates, I remembered our discussions on compliance gaps in CYSE 368 and 406. That gave me the language and confidence to report the issue without panic, just solutions.

What the curriculum lacked, however, was exposure to real ticketing systems like ServiceNow. My first few weeks navigating it were shaky. The system had its own logic: ticket categories, priority levels, and internal vs. external notes. It wasn't complicated, but it was unfamiliar. Still, because ODU taught me how to learn quickly—especially through labs and capstone-style projects—I adjusted.

Another area I had to pick up on the job was soft skills: how to walk into a professor's office, listen patiently, and resolve tech issues while explaining things in non-technical terms. No amount of group projects or simulated presentations prepared me for that fully. But they gave me the confidence to try, mess up, and improve.

So, did ODU prepare me? Yes, but only to a point. The classroom showed me the road. The internship made me drive it, with passengers, deadlines, and speed bumps. And in that way, both worked together better than either would have alone.

7. Learning Outcomes Fulfillment

In the introduction, I outlined three main goals for my internship: improving real-world technical troubleshooting, gaining experience with IT service management systems, and applying cybersecurity principles to active university infrastructure. Now that I've completed over 300 hours, I can reflect clearly on how each was met—and how they evolved.

First, real-world technical troubleshooting.

This was the most consistent part of my daily tasks. From day one, I had to diagnose issues across a wide range of systems—some were simple (like printer errors), others layered (like profile corruption across network logins). My goal wasn't just to fix problems, but to develop a logic and rhythm. Over time, I learned to isolate issues faster by using keyboard shortcuts, running quick diagnostics, and asking the right user questions. The skill isn't just technical—it's in managing time and temperament, especially when users are stressed.

Second, experience with IT service management systems.

I had never worked with an enterprise tool like ServiceNow before. At first, I felt lost—fields everywhere, acronyms I didn't recognize, escalation rules I had to memorize. But this quickly turned into a strength. I now understand how structured ticketing systems contribute to accountability, transparency, and priority-setting in a large organization. I learned to properly log tickets, avoid redundancy, and monitor issue trends for systemic problems. This was a direct win in terms of learning goal fulfillment.

Third, applying cybersecurity principles in practice.

This one surprised me. While I assumed my internship would be more IT-focused, I ended up engaging with cybersecurity far more than I expected. Tasks like identifying machines that hadn't updated antivirus definitions, setting BIOS-level restrictions, or flagging suspicious logins taught me how security works beneath the surface. I used my prior classroom knowledge—threat modeling, risk matrices, NIST principles—to inform decisions or ask better questions. More than anything, this taught me that cybersecurity isn't a separate department—it's baked into every system support role, whether users realize it or not.

Each of these objectives was met, stretched, and grounded in ways I didn't anticipate. They gave the internship structure, but the experience gave them depth.

8. Most Motivating Aspects

What energized me most during this internship wasn’t a single task, but a shift. The moment I realized I could independently solve problems that once made me hesitate. At first, I relied on team members for second opinions. I would pause, double-check settings, and mentally rehearse what I would say before approaching a user. But by the midpoint, something changed. Confidence started showing up not as bravado, but quiet efficiency.

One moment that stands out: I was assigned a support ticket for a faculty member whose laptop wouldn’t authenticate on the secure Wi-Fi network. They were clearly frustrated—it was interrupting a class livestream. My initial scan of the issue revealed nothing. But I remembered a niche configuration bug I had seen weeks prior. I checked their network profile settings, reissued the security certificate, and reset their DNS cache. It worked. What made this exciting wasn’t the fix itself—it was that I didn’t need to escalate. I was trusted. That trust, earned over time, was deeply motivating.

Another motivating factor was the rhythm of problem-solving. Each day brought a new blend of hardware quirks, software failures, miscommunications, or policy gaps. I enjoy puzzles, and the internship turned technical issues into live puzzles with real consequences. Fixing something meant someone's day continued. That connection between technical action and human outcome fueled me more than expected.

Beyond that, being part of a professional IT team had an energizing effect. Seeing how documentation was managed, how protocols were enforced, and how subtle professionalism played out in hallway check-ins and Slack threads—those things left an imprint. They made me want to level up—not just technically, but interpersonally and operationally.

9. Most Discouraging Aspects

The most discouraging aspect wasn't about the workload—it was the slow realization that not every environment values innovation as much as it claims to. In a university setting, especially one with legacy systems and constrained budgets, change is slow. Sometimes painfully so. I'd find ways to streamline processes, only to have them shelved for "later discussion." Or I'd point out recurring issues in ServiceNow tickets that could be resolved upstream—just to see them resurface again and again. There's a quiet resistance in institutional IT, born from years of navigating red tape. And as an intern, my position didn't come with the authority to challenge that flow.

At times, that made the work feel repetitive. It wasn't the technical work itself—it was the knowledge that some problems were fixable, yet intentionally allowed to persist. It taught me something about patience, about influence without authority. But it also revealed how bureaucracy can dull innovation when left unchecked.

Additionally, there were depressing instances where communication failed. On a few occasions, I would show up prepared to start work only to discover that it had been rescheduled, cancelled, or deprioritized without informing me. I sat there for a while, thinking if I should wait it out or follow up. I eventually learned to be proactive, but that limbo state felt like a waste of potential.

Still, these moments didn't crush morale. They became data points. Indicators of how real-world environments operate—sometimes clunky, often political, always human. And in hindsight, those challenges helped refine a more grounded professional mindset. Not every obstacle is technical. Not every win is visible. But each one shapes how you navigate the systems you're placed in.

10. Most Challenging Aspects

Learning how to maintain momentum when the pace around me slowed down was the most difficult part of my internship, not any one project or occasion.

I discovered early on that things don't always go quickly in settings like IT support, particularly in a big university. Approvals take a long time, yet tickets pile up. People ask for assistance and then vanish. After resolving one issue, you discover that it is a component of a larger one that no one is yet prepared to address. It's inertia, not anarchy. It was difficult to maintain mental acuity while working inside such a rhythm.

Another major challenge was triaging technical problems while maintaining user communication. Someone calls in stressed, systems down, expecting an immediate fix. Meanwhile, you're navigating outdated documentation, unfamiliar configurations, or dependencies outside your control. In some cases, I had to troubleshoot live while explaining the delay in real time, balancing technical clarity with user empathy. No script could prepare me for that blend of performance, patience, and problem-solving. I had to build it day by day.

Learning new tools on the fly was also a challenge I welcomed. Microsoft Endpoint Manager was familiar in theory but daunting in practice. Being trusted to manage system-wide configurations came with responsibility and risk. I triple-checked every change, knowing the wrong click could impact hundreds of users. The pressure forced me to think like an administrator, not just a student.

Lastly, navigating ServiceNow taught me more than just ticket categorization—it taught me about systems thinking. A single ticket wasn’t just a task; it was a signal. Learning how to see patterns across user reports, trace them to root causes, and suggest preventative measures meant pushing beyond surface-level solutions. That shift in thinking—from reactive to proactive—was tough but transformative.

The challenge wasn’t surviving the internship. It was learning how to evolve through it.

11. Recommendations for Future Interns

First: don’t just prepare for the work—prepare for the pace. In IT support, some days will move fast, and others will feel slow. Learn how to stay productive when no one’s assigning tasks. Take initiative. Check unresolved tickets, review system documentation, and observe how other team members handle problems. Use those quiet moments to sharpen your awareness—it’s how you’ll build trust.

Second: document everything. If you solve a ticket, log your steps. If you learn a new process, write it down. It’s not just for your memory—it’s for your team. Good documentation shows you’re thinking like a systems person, not just a support role. It also earns respect fast.

Third: know your tools. Before your first week, read about Microsoft Endpoint Manager and ServiceNow. Watch walkthroughs, learn the lingo, and get comfortable with how ticketing systems are structured. Even if your access is limited at first, this background knowledge will help you contribute early.

Fourth: soft skills matter more than you expect. You'll be face-to-face with users who are frustrated, confused, or rushing. Your ability to stay calm, listen, and explain tech in simple terms will define how successful you are. Practice patient communication. The goal is not just solving the issue—it’s making the user feel supported.

Fifth: build relationships. Say hello. Ask questions. Join team meetings. These small actions create opportunities. Most of my best learning moments came from spontaneous conversations with experienced team members who were willing to share because I had shown interest before.

Lastly, treat every task—even the small ones—as part of something bigger. Reimagining a device? You’re reinforcing security. Fixing a connection issue? You’re restoring someone’s ability to teach, research, or work. When you approach each assignment with purpose, even repetitive tasks become meaningful.

12. Conclusion

This internship wasn't just a checklist item for graduation—it shifted the way I see myself in the cybersecurity field. What started as a student job turned into a proving ground. Every ticket, every confused user, every unexpected error taught me something—not just about systems, but about showing up ready to solve problems when no one's watching.

The biggest takeaway? Cybersecurity is not just a technical field—it's human-centered. It's about trust, clarity, and consistency. I saw firsthand how quickly a system breakdown can ripple through departments, and how one well-executed fix can restore flow. That responsibility grounded me. It made the subject matter come alive.

As I return to the classroom for my final stretch at ODU, this experience reshapes how I engage. I'm more alert. More intentional. Concepts like endpoint protection and configuration management no longer feel abstract—they carry real-world weight. I've seen the backend of university infrastructure, the workflow of support teams, and the pressure points where things break. That insight will color how I approach my final projects and capstones.

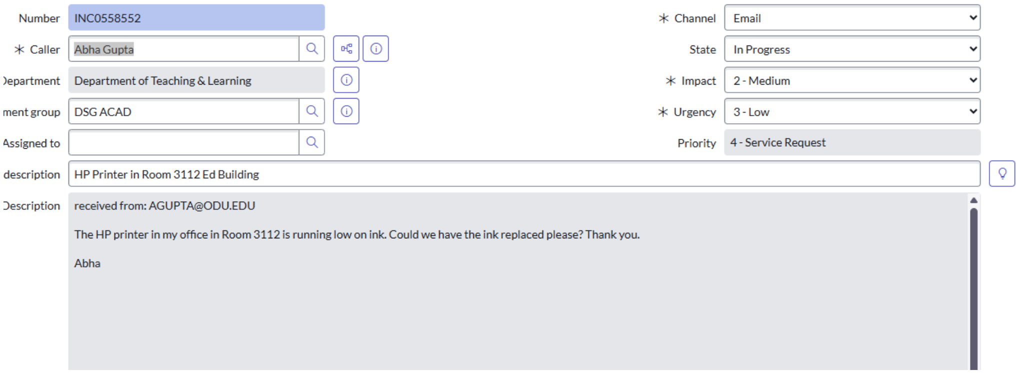
Looking ahead, this internship sharpened my focus. I'm no longer just interested in cybersecurity—I want to work at the intersection of IT operations and policy enforcement. Risk mitigation. Real-time response. Systems that serve people well. Whether I pursue graduate study in business analytics and AI or enter a GRC role, the clarity and discipline I've gained from this role will stay with me.

I've logged over 300 hours in this role, but the value of this internship goes far beyond time. It redefined how I approach problems, how I communicate under pressure, and how I see my potential in tech.

Appendices

Appendix A: Ticket Log Example

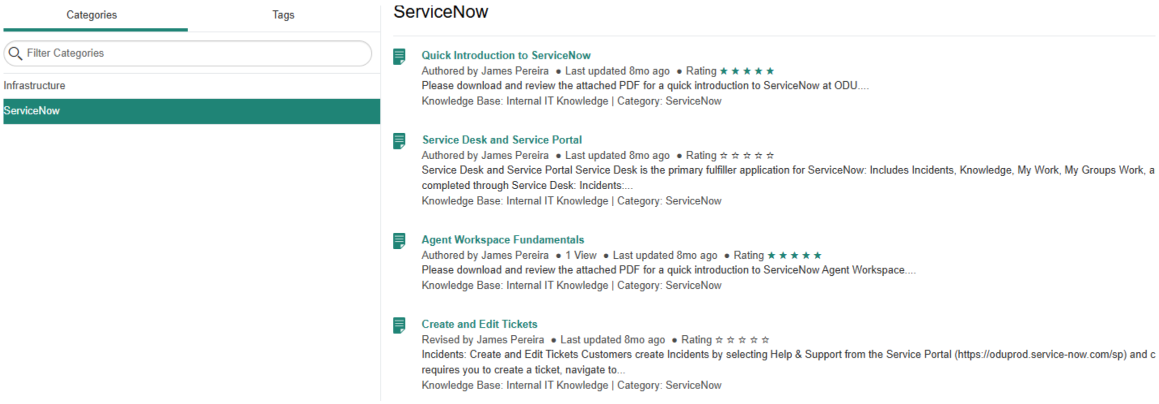
This screenshot displays a redacted example of a ServiceNow ticket log. It shows how technical issues were tracked, assigned, and resolved within the ITS environment.



Number	INC0558552	✱ Channel	Email
✱ Caller	Abha Gupta	State	In Progress
epartment	Department of Teaching & Learning	✱ Impact	2 - Medium
ment group	DSG ACAD	✱ Urgency	3 - Low
Assigned to		Priority	4 - Service Request
description	HP Printer in Room 3112 Ed Building		
escription	received from: AGUPTA@ODU.EDU The HP printer in my office in Room 3112 is running low on ink. Could we have the ink replaced please? Thank you. Abha		

Appendix B: Configuration Guide Sample

This sample is from a documentation I helped create to standardize the imaging and setup of new faculty laptops. It includes software checklist, configuration steps, and user credential policies.



ServiceNow

Quick Introduction to ServiceNow
Authored by James Pereira • Last updated 8mo ago • Rating ★★★★★
Please download and review the attached PDF for a quick introduction to ServiceNow at ODU....
Knowledge Base: Internal IT Knowledge | Category: ServiceNow

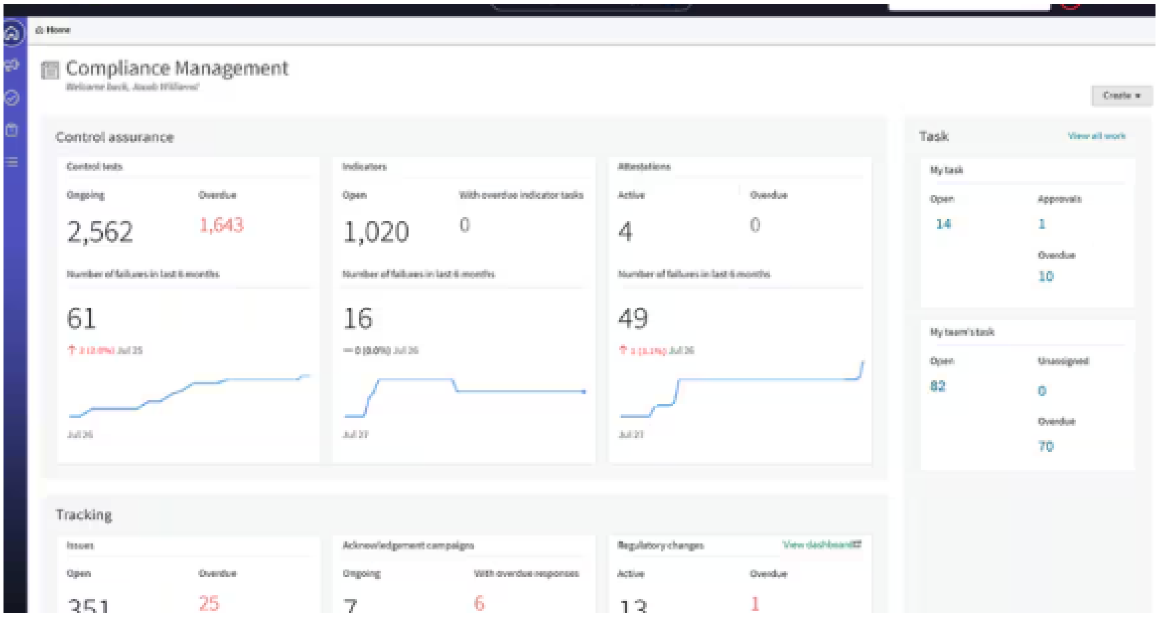
Service Desk and Service Portal
Authored by James Pereira • Last updated 8mo ago • Rating ☆☆☆☆☆
Service Desk and Service Portal Service Desk is the primary fulfiller application for ServiceNow: Includes Incidents, Knowledge, My Work, My Groups Work, a completed through Service Desk: Incidents:...
Knowledge Base: Internal IT Knowledge | Category: ServiceNow

Agent Workspace Fundamentals
Authored by James Pereira • 1 View • Last updated 8mo ago • Rating ★★★★★
Please download and review the attached PDF for a quick introduction to ServiceNow Agent Workspace....
Knowledge Base: Internal IT Knowledge | Category: ServiceNow

Create and Edit Tickets
Revised by James Pereira • Last updated 8mo ago • Rating ☆☆☆☆☆
Incidents: Create and Edit Tickets Customers create Incidents by selecting Help & Support from the Service Portal (https://oduprod.service-now.com/sp) and c requires you to create a ticket, navigate to...
Knowledge Base: Internal IT Knowledge | Category: ServiceNow

Appendix C: Endpoint Compliance Summary

This chart represents part of a compliance audit for Microsoft Defender deployments across various systems. I collaborated with senior staff to interpret this data and remediate non-compliant endpoints.



Compliance Management

Welcome back, Jacob Williams!

Control assurance

Control tests

Ongoing 2,562 Overdue 1,643

Number of failures in last 6 months

61

↑ 3 (2.0%) Jul 25

Jul 26

Indicators

Open 1,020 With overdue indicator tasks 0

Number of failures in last 6 months

16

— 0 (0.0%) Jul 26

Jul 27

Attestations

Active 4 Overdue 0

Number of failures in last 6 months

49

↑ 1 (2.1%) Jul 26

Jul 27

Task

My task

Open 14 Approvals 1

Overdue 10

My team's task

Open 82 Unassigned 0

Overdue 70

Tracking

Issues

Open 351 Overdue 25

Acknowledgement campaigns

Ongoing 7 With overdue responses 6

Regulatory changes

Active 13 Overdue 1