eBook

Autotask®

PROCESS FOCUS

GUIDE TO A BALANCED IT SECURITY STRATEGY

CHAPTER 1

The three pillars of security

The concept of the three pillars of cybersecurity — technology, people and process — is not new. However, the focus on each pillar has shifted over time, with different eras spotlighting different aspects as the key elements of security strategy. A balanced approach, integrating all three pillars effectively, is crucial for a robust defense against an ever-evolving threat landscape.

Technology: The traditional backbone of security

Historically, technology has been the cornerstone of cybersecurity defenses. This focus is largely due to the rapid development of digital infrastructure, necessitating an equally rapid development of defensive technologies. From the early days of simple firewalls and limited antivirus software to today's complex systems involving multifactor authentication (MFA), penetration testing, endpoint detection and response (EDR), managed security operations centers (SOCs) and AI-driven email security, the toolkit for cybersecurity professionals has expanded exponentially.

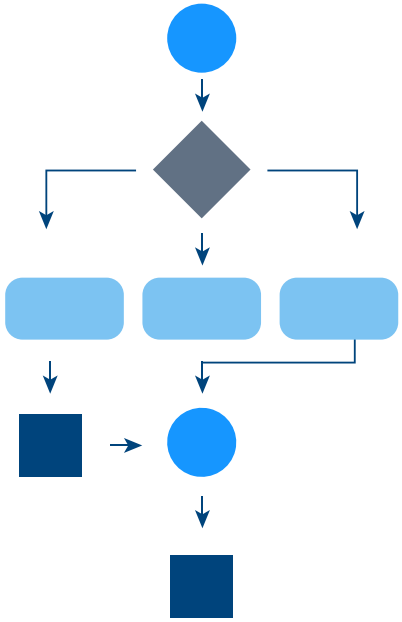
This pillar has seen significant investment as organizations have raced to keep up with sophisticated cyberthreats. Each new wave of technology — from cloud computing to the Internet of Things (IoT) — has brought with it new vulnerabilities and required new solutions. Consequently, the cybersecurity industry has witnessed an explosion of tools designed to protect these technologies, often leading to complex, layered defense strategies.

People: The essential element

While technology has often been the first line of defense, the people pillar has always been a close second. It encompasses not only the cybersecurity professionals who design and maintain security systems but also the end users who interact with these systems daily.

Initially, the focus within this pillar was primarily on acquiring talented cybersecurity professionals capable of managing and advancing security technologies. However, as the threat landscape evolved, it became apparent that end users could unintentionally become the weakest links in cybersecurity defenses. Incidents involving social engineering, phishing and other forms of manipulation demonstrated that user behavior could easily undermine even the most sophisticated technologies.

Recognizing this, the cybersecurity community has increasingly emphasized the need for comprehensive user training programs. These programs are designed to educate users on the risks of malicious emails, the importance of secure password practices, and the need to adhere to company policies on data security. This shift marks a crucial expansion of the people pillar from focusing solely on professionals to encompassing every individual within an organization.



Process: The underappreciated framework

The process pillar, despite its critical importance, has historically received less attention than technology and people. This pillar involves the frameworks, policies and procedures that govern the use of technology and the behavior of people within an organization. It is the structure that ensures consistency, efficiency and adaptability in an organization's security strategy.

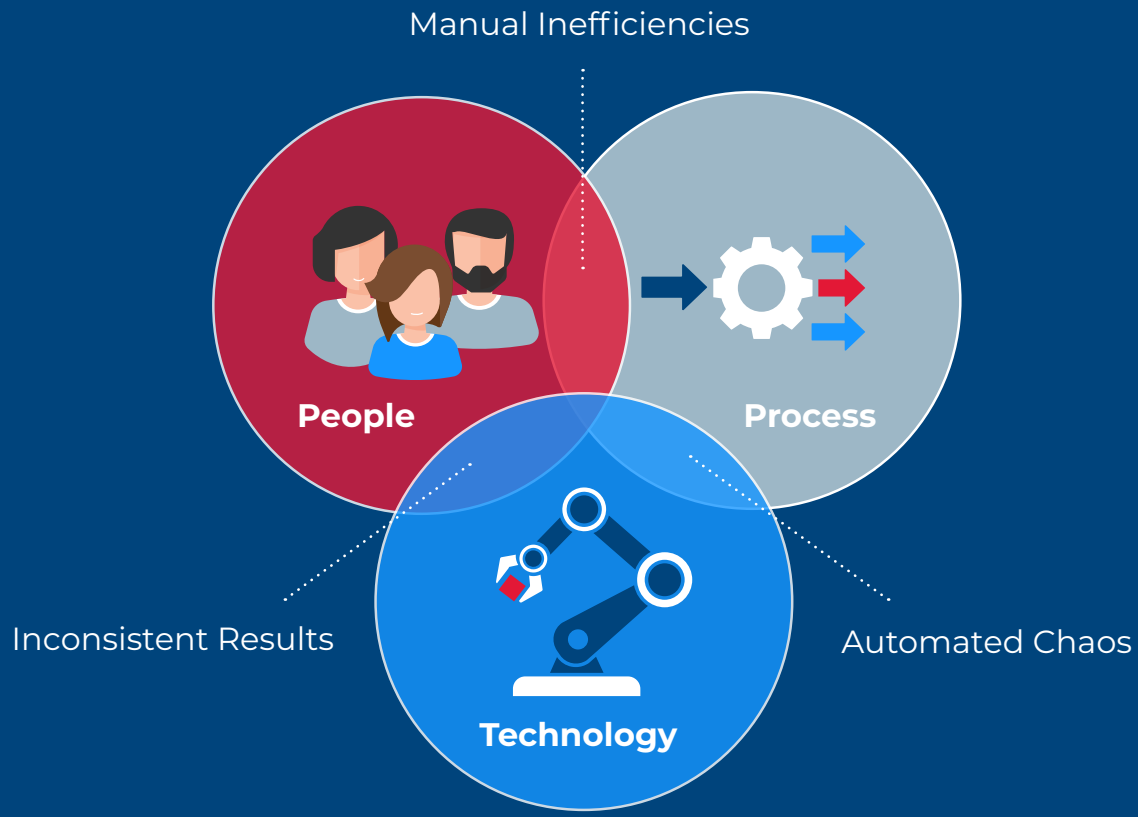
However, there is a growing recognition of its importance among cybersecurity professionals. As attacks have become more sophisticated and pervasive, the need for robust, scalable processes has become undeniable. These processes govern everything from how software updates are deployed to how incidents are managed and reported. Without strong processes, organizations find themselves reacting to threats rather than proactively managing them.

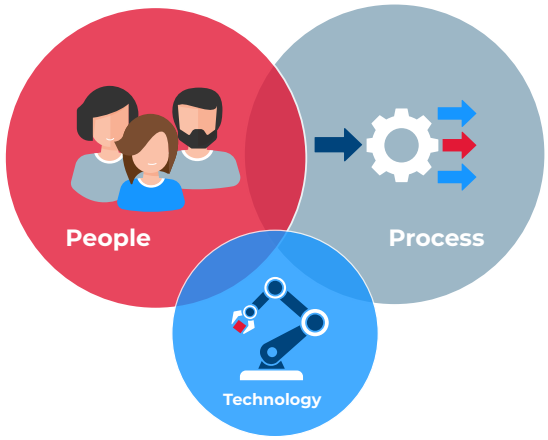
Organizational and leadership governance, service desk management and incident response are just a few of the areas where process plays a crucial role. As cybersecurity matures from a technical specialty to a strategic business imperative, processes that enhance governance, risk management, and compliance have taken center stage. This alignment is critical not only for enhancing security but also for achieving business objectives and maintaining regulatory compliance.

CHAPTER 2

The consequences of imbalanced security pillars

A comprehensive cybersecurity strategy requires a balanced approach that effectively incorporates technology, people and process. Neglecting any one of these pillars can lead to vulnerabilities, inefficiencies and a compromised security posture. This chapter explores the potential consequences of such imbalances by examining scenarios where only two of the three pillars are emphasized.





Overemphasis on people and process

In organizations that focus heavily on people and process while neglecting technology, the security infrastructure may fail to keep pace with technological advancements and emerging threat vectors. This often results in:

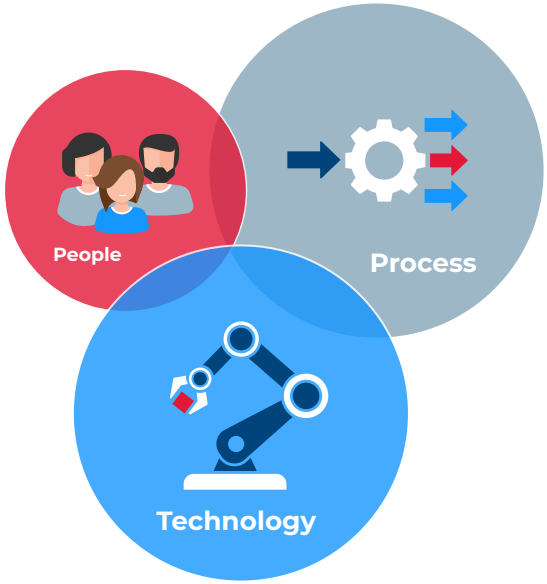
Resource inefficiency: Without the latest technological tools, cybersecurity professionals may find themselves overburdened, compensating for outdated systems with manual processes that are not only inefficient but also error-prone.

Lack of expertise: The cybersecurity talent shortage often makes it difficult and expensive for businesses to find and employ people with cybersecurity expertise, resulting in a team that may lack the needed skills to adequately maintain a secure environment.

Increased burnout: Continuous reliance on human intervention and rigorous processes can lead to employee burnout, particularly when staff must handle repetitive tasks that could be automated.

Security gaps: Lacking advanced technological defenses like AI-driven threat detection or automated security monitoring, the organization remains vulnerable to sophisticated cyberattacks that require technological solutions to identify and mitigate.

This imbalance highlights the critical need for technological investment to complement human expertise and refined processes, ensuring that the security infrastructure is both robust and resilient.



Overemphasis on technology and process

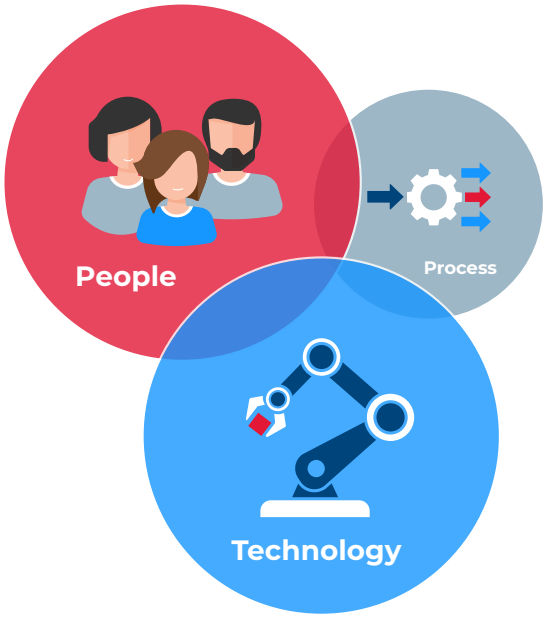
When organizations invest heavily in technology and process but skimp on people, they encounter a different set of challenges:

Automated chaos: High-tech solutions and detailed processes are in place, but there are insufficient skilled personnel to oversee these systems. This can lead to situations where automated systems operate without adequate oversight, potentially overlooking false positives or unusual patterns that a trained professional would catch.

Lack of adaptability: Although newer AI-enabled technology and processes can be automatically updated through machine learning, certain outdated technologies that are not continuously updated or informed by human insight may fail to adapt to new threats. Cybersecurity is as much about anticipating threats as it is about responding to them, and human expertise is irreplaceable in this context.

Knowledge silos: With a lack of emphasis on training and retaining skilled personnel, organizations may find that knowledge is not effectively transferred within the team, leading to dependency on a few individuals or external vendors.

This scenario demonstrates that technology and process efficiencies are only as good as the people who manage and optimize them.



Overemphasis on people and technology

This is the most common scenario, where organizations have invested in people and technology but have weak or non-existent processes.

Inconsistent results: Without standardized processes, the same security tasks may be performed differently across the organization, leading to inconsistent security postures and potential vulnerabilities.

Reactive rather than proactive security: In the absence of solid processes, organizations tend to react to security incidents as they occur, rather than proactively preventing them through established guidelines and protocols.

Difficulty in scaling: Scaling security operations becomes challenging without processes that standardize responses and ensure uniform implementation of security measures across all units and new expansions.

This lack of process can undermine the effectiveness of the technology in place and the capabilities of the people involved, emphasizing the need for well-defined procedures.

CHAPTER 3

People challenges and solutions

People challenges

End users: Research has shown that end users are often the weakest security link due to lack of awareness and training. In fact,

97% of employees cannot spot a sophisticated phishing email without training.

Lack of IT professionals: The U.S. National Institute of Standards in Technology (NIST) estimates that there was a

deficit of 3.4 million cybersecurity professionals worldwide.

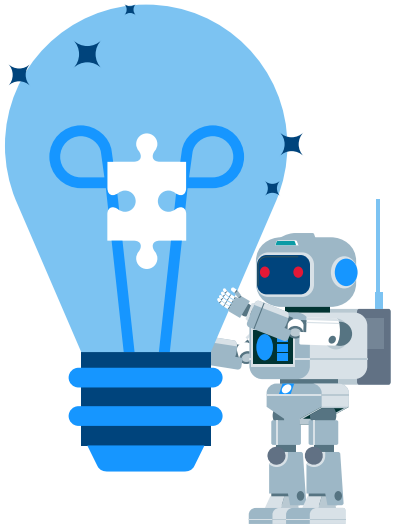
This global shortage of cybersecurity experts places increasing pressure on existing staff and resources.

People solutions

Security awareness training: Implement regular, comprehensive training sessions for all levels of the organization, from the CEO to interns. Incorporate phishing simulations to prepare employees for real-world threats.

Building a security culture: Instill best practices, such as never leaving computers unattended and reporting suspicious activities.
Lead by example: Senior management must adhere to and champion security protocols to reinforce their importance.

Expertise and response: Employ managed detection and response (MDR) or managed security operations center (SOC) services to ensure round-the-clock security monitoring.
Focus on retaining skilled security personnel by providing continuous training and favorable working conditions.



CHAPTER 4

Technology challenges and solutions

Technology challenges

Rapid evolution: The pace of new threats requires continual updates and adaptations in cybersecurity technologies.

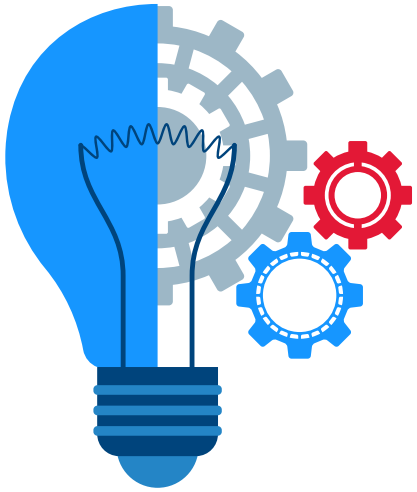
SMB adoption lag: Small- and medium-sized businesses often lag in adopting the latest security technologies, increasing their vulnerability.

Technology solutions

Modern security tools: Transition from basic security measures like firewalls and antivirus to advanced solutions such as multifactor authentication, Datto EDR and penetration testing. Implement Zero Trust network access, data backup and recovery, DNS filtering and dark web monitoring.

Comprehensive cybersecurity model: NIST maintains a cybersecurity framework (CSF) that is considered an industry standard. It is comprised of the steps "Identify," "Protect," "Detect," "Respond" and "Recover." It can be used as a guide for implementing technological tools that help improve your organization's cybersecurity:

- **Identify:** Tools like DarkWeb ID and Network Detective Pro help organizations understand their security landscape.
- **Protect:** Use advanced tools like Datto AV and Graphus for proactive defense.
- **Detect:** Solutions like Cyber Hawk and Datto EDR identify breaches that slip past initial defenses.
- **Respond and recover:** Tools like RocketCyber for response and Datto Unified Community for recovery ensure resilience and continuity.



CHAPTER 5

Process challenges and solutions

Process challenges

Inconsistency in execution: Variability in how security processes are applied can lead to gaps in defense.

Technician burnout: High demands and constant vigilance can lead to high turnover and reduced effectiveness.

Scalability issues: Processes that are not well-defined or adaptable can hinder the growth and responsiveness of security operations.

Process solutions

Standardizing operations: Implement comprehensive service desk management tools for handling access requests, triage processes and common request runbooks.

Develop, drill and enforce incident response plans that include centralized alert management and crisis communications.

Organizational leadership and governance: Focus on compliance management, risk identification and systematic reporting to maintain oversight and control.

Promote collaboration and communication to ensure all team members are aligned and informed.

CHAPTER 6

Connecting to NIST CSF 2.0

In February 2024, NIST released a significant update to its CSF, marking the first major revision since its inception in 2014. NIST CSF 2.0 reflects a shifting cybersecurity landscape and a greater emphasis on a holistic approach to organizational security, where governance plays a central role.

Key updates in NIST CSF 2.0:

Broadened scope: Originally designed for critical infrastructure, the CSF now extends its guidance to all sectors, urging a standardized approach to managing and reducing security risks.

Enhanced focus on governance: The addition of "Govern" as a key category of the framework emphasizes the importance of governance in cybersecurity, advocating for a strategic integration of security considerations from the operational level up to the boardroom.

Cherilyn Pascoe's insight: Echoing the expanded scope of governance, Cherilyn Pascoe, Director of the National Cybersecurity Center of Excellence (NCCoE) at NIST noted, "The CSF has always been intended to be used from the server room to the boardroom, and as server rooms are now no longer on-prem, the boardroom becomes even more important." This statement highlights the necessity for governance to permeate all levels of the organization.

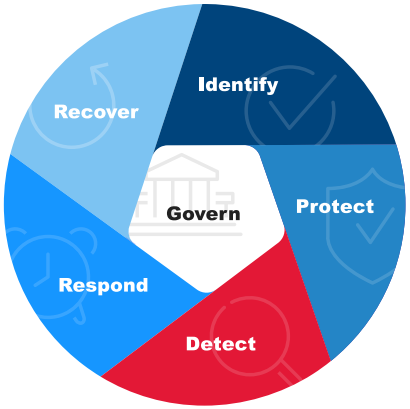
CHAPTER 7

What does Governance in NIST mean?

Governance refers to the systems, processes and policies through which an organization is directed, controlled and held accountable to achieve its goals. It involves oversight, policy-making and the ensuring of compliance with both internal and external standards.

In the context of NIST CSF 2.0, governance relates to the alignment and management of security efforts across an organization. It ensures that security practices are not only consistent and compliant with regulations but also strategically aligned with organizational goals.

In IT, examples of governance include defining clear roles and responsibilities for cybersecurity, establishing security policies that guide staff actions and implementing regular audits to assess compliance and effectiveness of security measures. These elements help an organization manage and mitigate risks associated with its information systems and technology.



"Govern" acts as the glue binding the other elements of the framework — Identify, Protect, Detect, Respond, and Recover — organizations are encouraged to view governance as a foundational aspect of their cybersecurity strategy.

CHAPTER 8

Embedding policies and procedures in everyday operations

In response to the updated NIST CSF 2.0, policies and procedures must be actively implemented and continuously updated, not merely documented and forgotten. This active integration ensures that governance is a living part of the daily operations.

Professional Services Automation (PSA) tools like Autotask are pivotal in this transformation, turning static policies into dynamic workflows and processes that drive governance. By integrating these tools into service delivery systems, organizations can ensure that governance is not only a compliance checkbox but a core component of operational efficiency. Autotask facilitates this integration through advanced service desk management, sophisticated workflow automation and thorough documentation capabilities, ensuring that every aspect of service delivery aligns with stringent governance standards.

CHAPTER 9

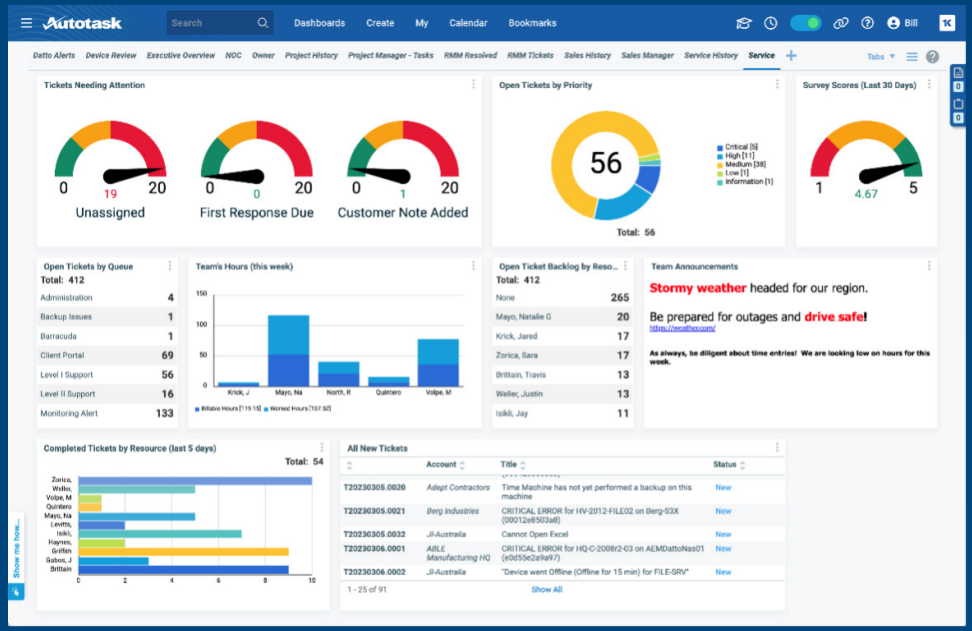
Autotask's role in governance

Autotask, as a comprehensive PSA tool, offers several features that help embed governance into the daily workflows of Managed Service Providers (MSPs) and internal IT teams.

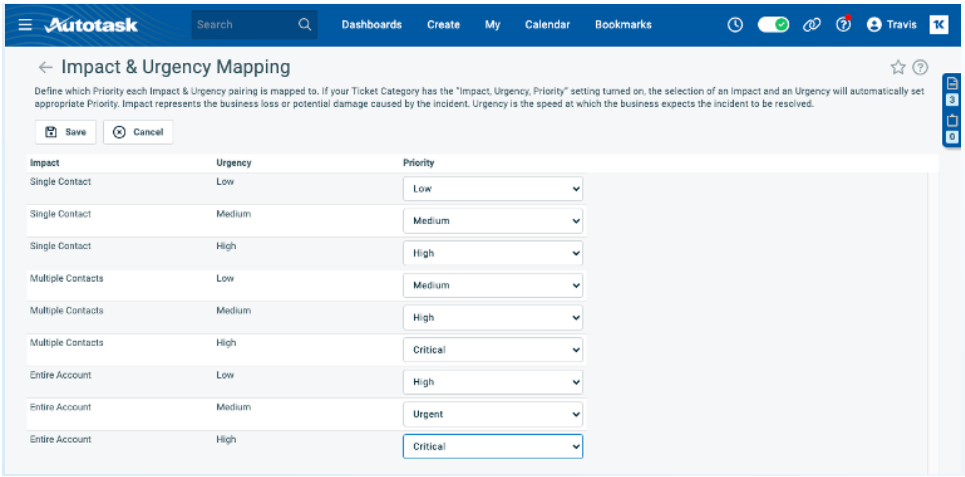
Autotask features for easy policy and procedure complian

1. Service desk enhancements

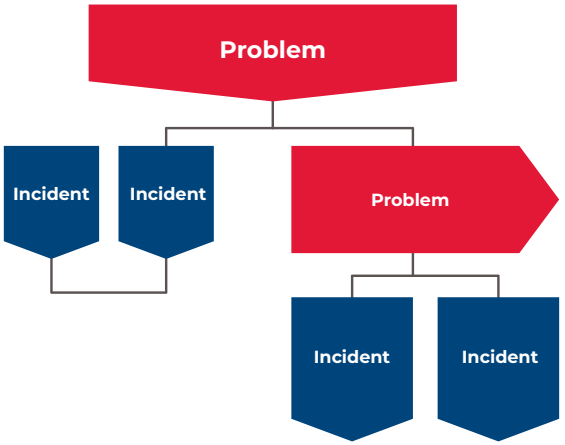
Queues and service level agreements (SLAs): Service requests are managed efficiently by ensuring they meet SLAs, aligning operational performance with your defined policies.



Urgency/Impact prioritization: The prioritization of incidents is automated to align with organizational policies, ensuring that critical issues are escalated appropriately.

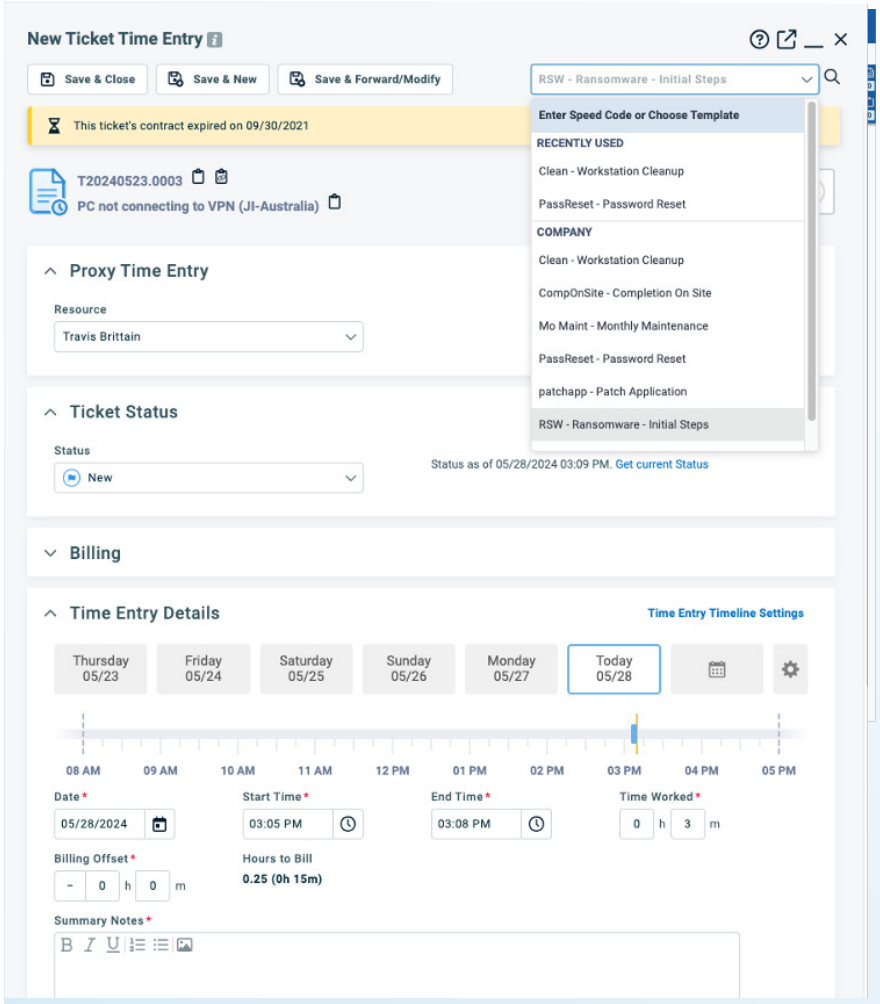


Incident and problem management: Standardized management processes are utilized to help maintain compliance and governance through consistent handling of incidents.

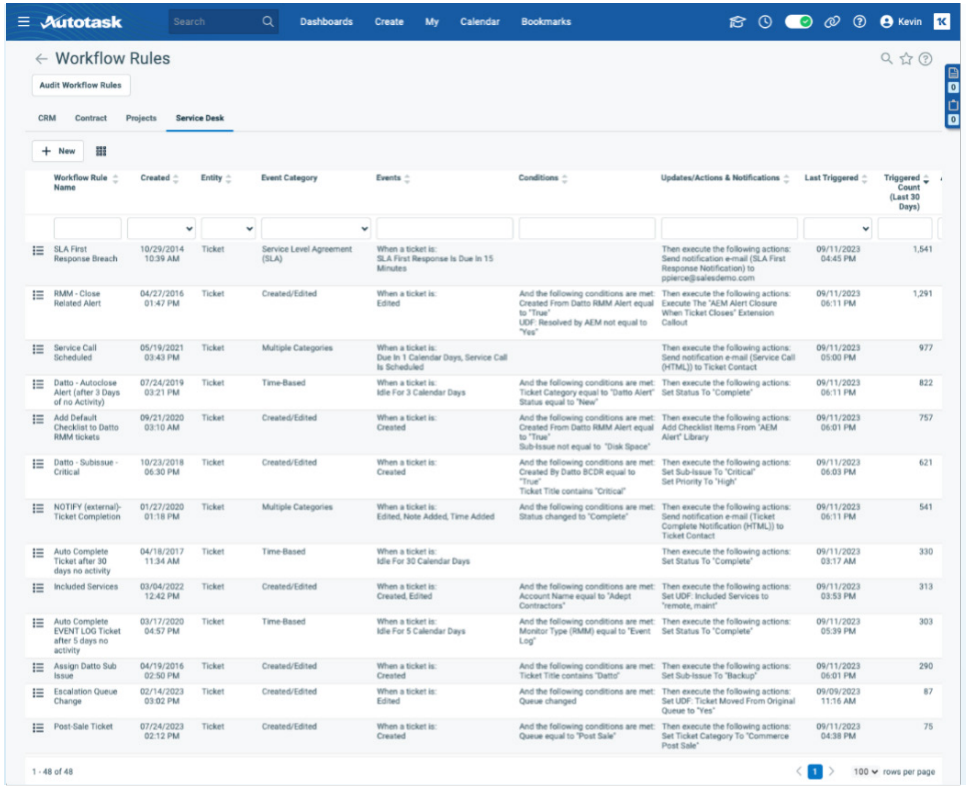


2. Workflow automation

Speed codes and integrated ticketing: Responses are streamlined and service delivery is standardized through the use of speed codes and integrated ticketing, reducing variability and ensuring adherence to procedural protocols.

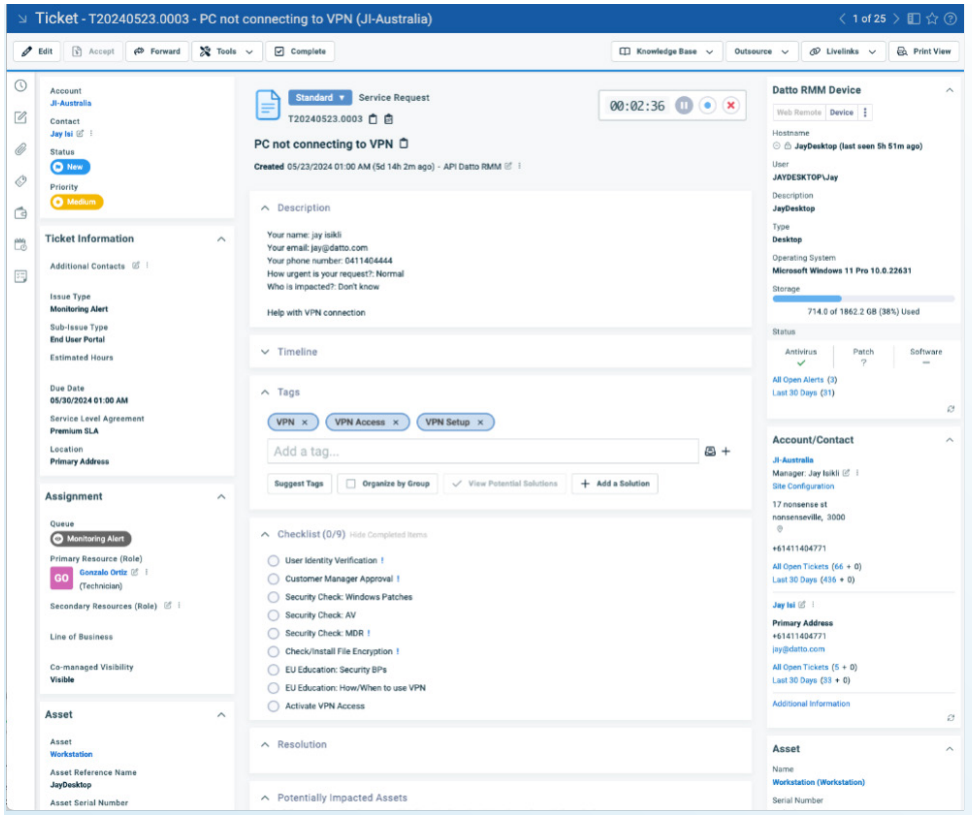


Enforcement of workflow rules: Policies are automatically enforced during service processes to ensure compliance and quick resolution of deviations.



3. Documentation and compliance management

Checklists: Autotask's checklists are used to maintain rigorous adherence to operational procedures and tags are utilized for easier audit and compliance tracking.



Activity logs: A detailed record of actions taken in Datto RMM remote control is logged to the ticket to ensure that all changes are documented to adhere to policies.

Example workflow

To illustrate the effectiveness of integrating governance through Autotask, we will explore a comprehensive example of how its features streamline service operations, enforce policy adherence and optimize efficiency. This workflow demonstrates how policies and procedures are actively implemented within daily service delivery, using Autotask's robust capabilities.

1. Integrated service ticketing

Centralized alert management: All alerts are managed through a centralized system, ensuring that nothing is missed and all issues are addressed promptly.

Data-driven prioritization: Alerts contain all the pertinent data to allow users to consider the severity and impact of each issue, ensuring that resources are allocated efficiently.

Efficient setup: All system alerts are visible from a single pane of glass. The ticketing system is designed for simplicity, with clearly mapped priorities and categories that streamline the ticketing process and reduce the need for manual checks across multiple portals.

Automated resolution: Rules and conditions are applied in Datto RMM to automatically resolve common issues without technician intervention.

2. Urgency/Impact matrix

Standardization of prioritization: Prioritization of tickets is standardized across the team by following the Information Technology Infrastructure Library (ITIL) framework for prioritizing incidents based on the impact to users and the urgency to resume normal operations, ensuring consistent handling of incidents.

Policy alignment: The prioritization process is aligned with organizational policies, with the "Impact" and "Urgency" fields automatically setting the "Priority" field, thus ensuring that each ticket is treated according to its importance to business operations.

3. Workflow automation

Streamlined ticket management: The service desk automates the movement of tickets through the service process, such as different queues, ensuring that each issue is quickly escalated to the appropriate team or individual without delay.

Dynamic status updates: Automatic status updates and queue adjustments prevent tickets from falling through the cracks, promoting swift and effective resolution in line with governance standards.

4. Speed codes

Enhanced interaction accuracy: Speed codes automate much of the technician's interaction with the ticketing system, reducing the time spent on manual entries and increasing the accuracy of ticket data.

Professional communication: Standardized language templates ensure that all communications are professional, consistent and clear, reflecting the organization's commitment to quality in customer service.

5. Checklists:

Error reduction: Using checklists for troubleshooting steps ensures that issues are resolved correctly the first time, significantly reducing the rate of ticket re-openings and enhancing customer satisfaction.

Accountability ensured: Checklists provide a documented trail of completed tasks, ensuring accountability and adherence to procedures which supports auditing and compliance requirements.

By automating and standardizing processes, Autotask reduces the time technicians spend on routine tasks, allowing them to focus on more complex issues and strategic initiatives. The integration of these features into everyday service delivery exemplifies how tools like Autotask are essential in modern cybersecurity frameworks, supporting both operational efficiency and comprehensive governance.

CHAPTER 10

Summary and future outlook

As we conclude this guide, it's crucial to recap the integration of the three pillars of cybersecurity — people, technology and process — with an emphasis on governance as directed by NIST CSF 2.0. This emphasis on governance underscores the need for MSPs and internal IT teams to focus on the process pillar to improve policy and procedure compliance.

Furthermore, the role of tools like Autotask cannot be overstated. These tools are essential not just for automating processes but for embedding and enforcing governance across all levels of IT operations. By utilizing such tools, organizations can ensure that policies and procedures are consistently applied, making it an integral part of everyday activities and decision-making processes.

Looking ahead, we anticipate advancements in cybersecurity technologies and methodologies. As these technologies evolve, so will the ways in which governance is integrated and implemented. By understanding these dynamics and preparing for these changes, organizations can ensure that they are not only protected against current threats but are also ready to adapt to the cybersecurity challenges of the future.

Want to see how Autotask can improve your cyber security processes first hand?

BOOK A DEMO