# IT Key Metrics Data 2024: IT Security Measures — Framework Definitions

This document defines the Gartner IT Security consensus model and framework definitions for cost management.

## Overview

**Key Findings**

The model outlined in this document allows us to evaluate IT Security Spending and Staffing among different organizations on a consistent basis. It comprises definitions needed to correctly enter data into Gartner benchmarking tools. It can also be used to understand the metrics produced in Gartner IT Key Metrics Data Industry and IT Security documents. The model is a subset of the Gartner Key Metrics Data Industry Measures Framework.

**Recommendations**

- ■ In order to properly interpret definitions and data collection requirements, review this document prior to initiating an IT Security analysis using the  Budget and Efficiency Benchmark Tool for Enterprise IT.

- ■ Use this document to understand metrics produced in IT Key Metrics Data 2024: IT Security Measures — Analysis, other IT Key Metrics Data documents, and Gartner Benchmarking Tools.

- ■ Refer to the Security Practitioners Guide and IT Budget & Efficiency Benchmark for additional guidance in completing a benchmark analysis.

- ■ Schedule an  inquiry to review your results or address alignment questions or to review your results and gain valuable insight based on your submission.

## Analysis

**Scope**

This document defines the Gartner Benchmark Analytics IT Security consensus model and framework definitions for cost management.

IT Security management is the discipline of designing, implementing and maturing security practices to protect critical business processes and IT assets across the enterprise. It covers:

- Developing and maintaining effective program governance.

- Communicating and engaging successfully with all stakeholders.

- Defining a vision promoting desired security, risk management and business outcomes.

- Defining, communicating and enforcing security policies across the organization.

- Planning budgets and resourcing, including talent management and professional services.

- Assessing and improving program maturity and performance.

The scope of the IT security environment analysis is a high-level view of the non-personnel and personnel costs/FTEs associated with provisioning and management of all information technology security within an enterprise.

This includes identity and access management, network security, endpoint security, data security, application security, vulnerability management and security analytics, governance, risk, and compliance management, as defined below.

## Figure 1: IT Security Analysis Framework

**IT Security Analysis Framework**

| Domain | | Description |
|---|---|---|
| Network Security | | Protection of telecommunications infrastructure from threats resulting in compromised data in flight or loss of network availability |
| Endpoint Security | | Protection of endpoint systems, including servers, end-user laptops and desktops. |
| Data Security | | Protection from compromised data, exposed data, loss of data fidelity or lost data resulting from compromised systems, systems failure, or inappropriate user behavior |
| Identity & Access Management | | Protection from unauthorized access to data, applications, and devices, resulting from compromised identities and credentials |
| Vulnerability Management | | Proactive mitigation of risk due to weaknesses, and protection from data exposure and production loss resulting from compromised systems and IT infrastructure |
| Security Analytics | | Use of data analytics captured from security information and events management (SIEM) systems to proactively mitigate risk due to weaknesses in the IT infrastructure |
| Application Security | | Software applications to provide protection from data exposure resulting from transaction compromise or failure |
| Governance, Risk & Compliance | | Protection from security risks through the management and achievement of security objectives commensurate with and necessary for the achievement of business objectives |

Source: Gartner (2023)
ID: 801290

**Gartner**

## Figure 2: Consensus Model

**IT Security**

**Personnel**
- Infrastructure Security
- Applications Security
- Vulnerability Management and Security Analytics
- Security Governance, Risk Management and Compliance
- Management and Administration

**Hardware**
- Firewall/Unified Threat Management
- IDS/IPS Devices
- Radius/Proxy Servers
- Encryption Concentrators
- Email/Web Security Gateways

**Software***
- Identity and Access Management
- Security Information and Event Management
- Anti-Virus/Anti-Spam/Anti-malware
- URL Content Filtering
- End-User Encryption
- Host IDS/IPS
- Firewall Software
- Vulnerability and Threat Detection
- Application Testing/Scanning/ Shielding

**External Services**
- Traditional and cloud (Private and Public)

Include SaaS*
Source: Gartner (2023)
ID: 801290

**Gartner**

## General Information

IT Security Spending is a subset of Enterprise IT Spending defined here: IT Key Metrics Data 2024: Industry Measures — Framework Definitions. As with the enterprise model, IT Security spending/budget can come from anywhere in the enterprise that incurs the costs defined here. It is not limited to the IT organization and can include a non-IT CISO, enterprise risk management, shared services, or any other organization. It is calculated on an annualized 'cash flow view' basis, and, therefore, contains capital spending and operational expenses, but not depreciation or amortization.

### Staffing

Staffing should be reported as full-time equivalents (FTEs). FTEs should be measured in calendar time. For example, an individual who works full time on an assignment for one full year would be reported as 1.0 FTE while an individual who was employed for six months of the study period would be reported as 0.5 FTE. Do not subtract such activities as vacation time, sick days and administration time. Do not count any one physical person as more than one FTE (for example, due to overtime). FTEs are assigned to services based on the functional definitions provided. If an individual or group performs more than one function, FTEs may be prorated between services and/or functions based on client estimates of time spent in each area.

Furthermore, only include personnel whose job comprises at least 10% of annual effort in a defined Security role. For example, an HR resource who enrolls new users via an IAM system, and assigns job role profiles and permissions automatically through this means, would not typically be counted since this is only a very small part of their on-boarding activities and effort. However, you would count and include the IT staff who support this IAM system, or a dedicated IAM role within the IT Service Desk or an IAM team member who performs this role on demand from HR.

### Company Employees

The count of employees (i.e., headcount excluding contractors or consultants) on a full-time equivalent basis, regardless of whether these employees are frequent users of the technology supported by the IT organization. This includes full-time and part-time employees, or as reported in the public record.

### IT Operational Infrastructure Security

- **Identity and Access Management** is the discipline that enables the right individuals to access the right resources at the right times and for the right reasons. It comprises a set of practices, processes and technology responsible for the management of digital identities and their associated access to resources. Specific IAM related activities are: user account provisioning, password management, user access administration (e.g., changes in roles, position or status (JML)), directory integration, single sign-on (SSO), Active Directory, remote access services, strong or multi factor authentication/two-factor (2FA)/three-factor (3FA), hard and soft token based authentication services, Public Key Infrastructure (PKI) and Federation type services, privileged user management (PUM), Identity and access governance (IAG) (inclusive of the processes for user access certification/recertification, attestation, application access audits etc.), and cloud based identity services (e.g., IDaaS). Identity and access management is not limited to internal employees. It includes access to systems by contractors, business partners, customers etc.

- **Network Security** comprises measures taken to protect a communication pathway from unauthorized access to, and accidental or willful interference with, regular operations, and hence involves protecting computers and computer networks from attack and infiltration. Network security provides network protection through the restricting of network traffic, based on a set of policy defined rules. Network security provides protection at key ingress and egress points in the form of perimeters, segments and zones, typically defined and enforced by firewalls/NGFWs/firewall administration, Wireless Access Firewalls (WAF)s/RASP, Network Intrusion Detection & Prevention (NIDS and NIPS), Virtual Private Networking (VPN) concentrators, Hardware Security Modules (HSMs), Proxy Servers, Secure Email and/or Web Gateways, Unified Threat Management (UTM) appliances, Network Access Control (NAC) services, and Distributed Denial of Service (DDoS) protection and prevention services.

- **Endpoint Security** is a set of capabilities and services provisioned across devices and platforms to provide the required and expected level of protection against potential compromise resulting from inappropriate configuration, use or attack(s). It covers the security services, capabilities and associated management and support thereof used in the protection of all endpoint devices such as desktops, servers, laptops and mobile devices which users leverage to access corporate data and information. Specific examples would typically include antivirus/anti-spyware/anti-malware software on PCs and servers, mobile device management (MDM), device encryption and management, Host Intrusion Detection & Prevention (HIPS), hardware-based protection (e.g., personal firewalls), advanced anti-malware and threat detection software and also any physical security control in place for these assets (e.g., locks.)

- **Data Security** ensures confidence in the ability of users, systems and business processes to provide the required and expected level of protection from data compromise or loss of data fidelity resulting from system compromise or failure, or inappropriate user behavior with regard to data in whatever stage of its life cycle. It focuses on confidentiality (to protect against unauthorized or inappropriate access), integrity (to ensure data is not improperly changed or deleted), availability (to ensure appropriate access to data for the right parties) and privacy (to assure personal information is only used for the specific business purpose for which it was collected). Typical data security protection capabilities include: data discovery & classification, encryption/decryption of data "at rest," "in motion" or "in use" (incl. endpoint & bulk storage data encryption/decryption), digital certificate life cycle management for digital signature based services, privacy enforcement techniques (data masking), database audit and protection (DAP) techniques, data loss prevention (DLP) services and data destruction, removal and erasure type services.

**Vulnerability Management and Security Analytics**

- **Vulnerability Management** is the process cycle for finding, assessing, remediating and mitigating security weaknesses. It comprises the policy and scope definition, proactive identification, remediation, mitigation and ongoing monitoring of security vulnerabilities via dedicated vulnerability assessment and management products and services. These services typically scan enterprise networks (IP ranges) and establish a baseline and trending of vulnerability status of devices, applications and databases; identify and report on the security configuration of IT assets; discover unmanaged assets; support specific compliance reporting and control frameworks; support risk assessment and remediation prioritization; and support remediation by IT operations groups which involves scanning (through resident agents on network-attached devices) of all internal and external facing target applications or devices for vulnerabilities, to determine if they are at latest available historic patch level. Service typically also includes periodic penetration testing, vulnerability assessments, asset auto discovery, generation of patch and vulnerability status compliance reports, vulnerability monitoring, and ticket raising.

- **Security Analytics** comprises the ability of the security program via technologies, processes and people to identify, define, react and remediate against potential or current or active attacks and the associated threat actors, that may result in system or service compromise, breaches or data loss events. It is essentially a set of services delivered by a Security Operations Center (SOC) or equivalent capability consisting of a centralized focal point of security specialists where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended, and action plans devised to counter any undesirable events detected. Typical security analytics services include security incident and event log collection, monitoring and management (SIEM), managed log retention & analysis, user behavior analytics (UBA), threat intelligence services, fraud detection and response services, digital forensics and cyber incident response services. The total cost of security analytics tools are included here even though these tools may be used for many purposes. This function does not cover activities such as providing assistance to law enforcement in prosecuting malevolent actors, or aiding internal risk management/human resources investigations around violations of company policies.

**Application Security**

- **Application Security** describes the use of software, hardware, staff and process methods to provide protection from threats throughout the application development life cycle. It therefore comprises a set of measures built into the application development process to prevent the unauthorized access, theft, modification of or erasure of sensitive data through the exploitation of applications. Specific examples include: the identification of security flaws in application design, development, deployment, upgrade, or maintenance through code assurance techniques such as black box analysis and testing, health checks, the use of static & dynamic application testing techniques (SAST/DAST/IAST) and application security frameworks, and/or via data obfuscation, filtering & masking, secure coding practices and software composition analysis (SCA) etc.

- Application Security is about building a secure environment in which to build applications. It does not include functions that are a part of the application development and support processes that use these tools. For example the implementation and maintenance of tools and processes to perform code reviews are included. The performance of these code reviews are not. Building security features into applications are also not included.

- Application Security costs as defined here are also included if they cover environments that build applications for external customers on a custom or packaged basis.

### Governance, Risk, and Compliance Management

Governance, Risk, and Compliance Management (GRC) comprises of a set of practices and processes, supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.

- **Security Governance** is defined as a number of "cross-functional" security activities which include the development and maintenance of security policies, standards & procedures, the communication of business values, culture & principles, security strategy & organization, training & awareness, documentation & guidance, communication plans, security service metrics, audit and compliance oversight, financial management of security services, security vendor management, security PMO etc. obligations. Governance costs and staffing include the strategic leadership of security standards, policies and practices, as typically represented by the Chief Information Security Officer (CISO) or equivalent, and his immediate office.

- **Risk Management** is defined as the function dedicated to ensuring that adequate controls are designed and implemented to mitigate the various risks associated with IT assets (including data), infrastructure, and processes. It includes activities such as periodic and annual IT audits (non-regulatory), risk assessment/monitoring, issue management & action tracking, and the development and execution of remediation plans.

- **Compliance Management** is the process of identifying, managing and reporting compliance activities related to organizational, commercial and regulatory compliance obligations. Compliance requirements can be derived from internal directives, procedures and requirements, or from external laws, regulations, standards and contractual agreements. The compliance activities here only cover what is necessary to ensure the IT Infrastructure and Application environment is compliant and not the compliance of every aspect of the business. As an example a regulation might require specific reporting around issues that affect public welfare. The regulation may mandate that the presence, communication, and enforcement of formal data security policies are in effect to ensure the integrity of reporting. For this category, only the latter compliance activities would be included and not the entire reporting activity itself.

NOTE: The governance, risk, and compliance management category excludes all items in the operational infrastructure security, vulnerability management and security analytics, and applications security categories.

For the purpose of this framework IT security spending does not include any IT disaster recovery costs and staffing associated solely with service continuity plans, nor does it include any costs or staffing associated with physical security measures — such as security guards or patrols, scanning equipment, coding panels or badges for control of physical/logical access — taken as protection against burglary, theft, vandalism, terrorism, fire or natural disasters.

This model excludes spending related to the restoration of compromised systems. Restoration is viewed as the cost of not having appropriate security in place.

## IT Security Spending Distribution by Asset Class

The distribution of operational infrastructure security spending by asset class provides an understanding of how investments are dispersed within the environment. This distribution helps to outline non-personnel versus personnel related cost allocations as defined below:

![Gartner logo]

**Personnel Costs**

Personnel is defined as:

- **Salary and Benefits Expenses:** Salary (including overtime pay), benefits and "other" employee costs, such as travel and training for all IT FTEs. The "benefit load" should include costs for bonuses, paid holidays, vacations, medical/dental coverage, life and accident insurance, retirement plans, stock plans, disability, Social Security, unemployment compensation, dependent care, tuition reimbursements and employee assistance programs (for example, physical exams, exercise programs and similar costs).

For contractors, include all compensation that was paid directly to the individual or agency.

Do not include the spending related to human resource department staffing allocations, early retirement incentive bonuses and internal "cross-charges" for corporate overhead such as for the chairperson's salary.

- **Insourced IT FTEs** are defined as FTEs who are employed by the IT organization (excluding contractors). Contract IT FTEs are defined as: FTEs who are supplemental to your staff and are "operationally" managed by the in-house staff.

Costs/FTEs include in-house and contract personnel supporting IT Operational Infrastructure Security, Vulnerability Management and Security Analytics, Application Security and Governance and Risk and Compliance Management.

**Non-Personnel Costs**

*Non-personnel costs include in-house related costs as well as fees for third party and outsource contracts.*

**Hardware** is defined as:

- All dedicated hardware assets utilized in support of the Security operations, for each category indicated (i.e., Network Security, Endpoint Security etc.).

- Examples include firewalls, security gateways, security appliances, security toolset platforms and ID tokens, etc.

- Include only annual asset costs that are directly or recognizably related to the defined in-scope security functions. Do not include costs of hardware assets whose prime purpose is not security. For example, there may be routers deployed that have firewall, encryption or NIPS capabilities, but you must not include any apportionment of their annual costs unless you can identify a cost to specifically enable a security function — such as a firewall "add-on" enabler cost of extra router hardware or software.

- Hosting/facilities/occupancy costs for space dedicated to in-scope security hardware such as the apportioned annual costs of hosting security-related devices, storage arrays and appliances in the data center, including power/heat management and raised floor. It also includes the annual cost of any consumables related to the security activities

**Software** is defined as:

- Annual license and maintenance as well as costs associated with new purchases and upgrades for all software dedicated to operating or managing the security systems applications for each category of security expenditure.

- Examples include endpoint security suites, identity and access management, security information and event management, URL/content filtering, antivirus, end-user encryption, host IDS/IPS, firewall, vulnerability and threat management, application testing/scanning/shielding, etc.

- Includes only software license costs that are directly or recognizably related to the defined in-scope security functions are included. Costs of software whose prime purpose is NOT security are excluded.

- For example, there may be enterprise licenses for OS, productivity suite software or enterprise packages that have security capabilities (e.g., BitLocker encryption in WinOS). No apportionment of their annual costs are included unless a cost to specifically enable a security function can be identified. An example would be an "add-on" software charge for a security capability, or a specific module license charge for security functionality (e.g., Oracle Identity Manager).

- This category only includes on-premises software expenses.

**Software as a Service (SaaS)** includes:

- All the assets providing the functionality in the software section, but only when it is delivered as SaaS. SaaS is defined as software owned, produced, and managed remotely by one or more providers. The provider provides software based on one set of standard code and data definitions consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics.

**External Services** includes:

- **Traditional Outsourcing** is defined as any situation in which the full operational responsibility for IT services is completely handed over to an external service provider. An example here would be a SOC managed by a third party for a fee. Services can be provided on-premisess or from a remote location. Note that if an outsourced SOC uses public cloud services to perform its duties, and the cost of the public cloud services aren't billed separately, those would still be considered Traditional Outsourcing. It can also include Consulting. Consulting is defined as security advisory services that help companies analyze and improve the efficacy of business operations and technologies strategies. This is considered an external service only if the personnel performing it are performing a statement of work and not managed by internal IT Staff.

- **Public Cloud Services** are managed by a provider, offered by subscription and in a multitenant manner, with some sharing of resources between tenants to increase overall efficiency and scalability of the operation.

## Recommended by the Authors

*Some documents may not be available as part of your current Gartner subscription.*

"IT Score for Security & Risk Management"

"Top Strategic Technology Trends for 2024: AI Trust, Risk and Security Management"

"Cybersecurity Leadership Primer for 2023"

"IT Cost Optimization, Finance, Risk and Value Primer for 2023"

"Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer"

"Ignition Guide to Designing and Launching a Security Champion Program"

"Security Program Management 101 — How to Select your Security Framework"

## Evidence

This research contains the relevant industry standard consensus model and IT performance measurement framework as defined by Gartner Benchmark Analytics. To learn more about Gartner Benchmark Analytics contact your account executive or email us at inquiry@gartner.com

## Document Revision History

IT Key Metrics Data 2023: IT Security Measures — Framework Definitions - 8 December 2022

IT Key Metrics Data 2022: IT Security Measures — Framework Definitions - 16 December 2021

IT Key Metrics Data 2021: IT Security Measures — Framework Definitions - 18 December 2020