Building the Foundations for Basic Security Hygiene

Published 19 June 2020 - ID G00720111 - 84 min read

By Analysts Mike Wonham

Initiatives:Security and Risk Management Programs for Technical Professionals

Mature security programs must ultimately coalesce around risk management. However, all effective security programs rely on the basic controls. This research provides security and risk management technical professionals with a guide to implementing the foundations for an effective security program.

Overview

Key Findings

- Security controls depend on a number of foundational practices, such as asset management. Weaknesses here can severely limit the effectiveness of security efforts. The responsibility for these practices may be outside the security team.
- All organizations face a set of similar (“commodity”) threats. Ineffective basic security hygiene can often be a significant factor in security incidents. Thus, certain practices, such as anti-malware, must always be a part of any organization’s basic security program.
- An organization’s specific control requirements will vary with IT architecture, regulation and risk assessment. Choosing technology and process controls based on risk enhances security, but it is not necessarily the most effective first step.
- Making security decisions based on risk is important for longer-term security relevance and business outcomes. Deferring decisions until a risk framework is in place can put organizations at higher risk, but implementing best-practice and regulatory-driven controls can fill the gap.

Recommendations

As a security and risk management (SRM) technical professional tasked with introducing, implementing or updating the organization’s security systems, you should:

- Identify existing controls and foundational practices, and implement an improvement plan focused on coverage, quality of delivery and consistency. Build cross-team support, especially

with HR and IT, because security effectiveness depends on their activities.

- Deploy additional basic controls, as described in this research, for better underlying hygiene. Some controls, such as anti-malware and user authentication, are universal. Prioritize others based on your organization's IT and regulatory environment.

- Implement monitoring, response and measurement capabilities to build visibility, highlight issues, improve security resilience and enhance identification of additional threats that might need to be addressed.

- Develop a risk-based approach, focused on business activities and relevant specific threats, to identify further control requirements and enhancements, and build a strategic roadmap unique to your organization. Doing so will legitimize and optimize further security investment.

Analysis

Gartner recommends taking a risk-based approach to IT security planning, as it provides a targeted and business-relevant method of selecting controls. However, clients often ask more fundamental questions about security architecture design and implementation. For clients without the security basics in place, suggesting a risk-based approach is inappropriate. It will delay and confuse both planning and implementation of core controls addressing common threats.

In practice, many threats, such as nontargeted malware or internet-based attacks, are common across organizations. Gartner refers to these as "commodity threats." For such threats, we suggest that most organizations can start with an initial set of security controls to deliver a baseline of security hygiene. Some organizations adequately control their environment in the longer term through this common baseline of security practices alone, with little to no further enhancement. Where the organization faces additional threats or a unique impact from a commodity threat, a risk assessment can then identify the additional control requirements.

> **The baseline creates the foundation upon which a risk management approach builds by then addressing the organization's specific threats and vulnerabilities to identify and fill gaps. Use this baseline to both "get something done" and to lay the groundwork for a future, risk-based security program. You may not be addressing threats specific to the organization, but unless you are definitely aware of immediate risk, the basics are crucially important in the short and long term.**

Security architecture must include security controls and processes to manage them. That much is a given. However, organizations should also build nonsecurity foundational capabilities (both tools and processes) that enable security effectiveness. Practices such as personnel management, asset management and service management form the bedrock on which effective security depends.

> **Without foundational practices such as asset management, personnel management, procurement control and change management in place, security controls cannot work at best effect. The lack of such practices limits the returns available from investment in high-quality security processes.**

This research supports both technical professionals who are new to security and those who are more experienced and looking for a reference to aid initial control selection. It focuses on three areas:

1. The drivers for using this basic security hygiene approach
2. The basic security controls organizations should initially consider using for a fundamental level of security hygiene
3. The key foundational practices that allow the security controls to be increasingly effective

In addition, Note 1 at the end of this document provides a comprehensive list of supplemental Gartner research by topic.

Basic Security Is Critical for Longer-Term Assurance

A number of frameworks and standards provide guidance on what security controls — basic or otherwise — should be in place to protect an organization. Examples of these frameworks include National Institute of Standards and Technology (NIST) Cybersecurity Framework and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000. (See "Security Frameworks: The What and Why, and How to Select Yours" for further information.)

Such frameworks are catalogs that include lists of controls extending into the hundreds. Knowing where to start selecting controls can be challenging for both experienced technical professionals and those newly tasked with delivering a basic level of security. These programs are often either ineffectively or incompletely implemented, resulting in issues that can easily lead to a security failure. A pragmatic approach is required — one that allows the organization to build its security program in stages. Additionally, the approach needs to reflect the availability or lack of processes such as risk management. Focusing on a "best-practice" approach can make more sense at the

early stages of a security program. Note that, even for more mature environments, basic hygiene remains a core requirement in partnership with risk-based approaches.

This research outlines a set of essential security controls that Gartner considers necessary to provide basic security hygiene. This set can be used as a starting point for an effective security program. We have endeavored to be as comprehensive as possible in creating this list of basic controls. We've also included a few additional control practices that may not be truly "basic" today. These elective controls should be considered best practice depending on the maturity and relative importance of a business process, such as software development.

Obligations

The bottom line is that an adequate level of baseline security is necessary to demonstrate due care. There must be a basic set of documented controls and practices that are applied uniformly to protect the business. Taking a position of naivety or ignorance in the fallout of a breach and hoping that regulators, customers and stakeholders will be accommodating is not "due care." Regulations (such as privacy and financial controls) demand a level of governance that builds on basic security hygiene.

> **An organization choosing to omit basic security controls in the long term should consider itself lucky if the regulator or auditor discovers the gaps before a breach occurs.**

Note that security does not equal "compliance." For example, most organizations are being asked to deliver "privacy." However, privacy regulations are *not* security regulations. Good security hygiene provides a platform for privacy compliance, but not compliance itself. A compliance program should be led by someone well-versed in that regulation, along with its various legal issues.

Organizations should focus on the following objectives in parallel:

- Getting a number of basic security practices implemented
- Embarking on the path to fully using a risk-based approach

In fact, security controls and processes provide important information about threats and vulnerabilities. Therefore, without having basic security hygiene in place, you can't be sure that you will have all the contextual information necessary to effectively perform risk assessments.

Good security hygiene provides critical support for other types of governance, especially risk, privacy and data governance. Boards and executives are increasingly discerning when

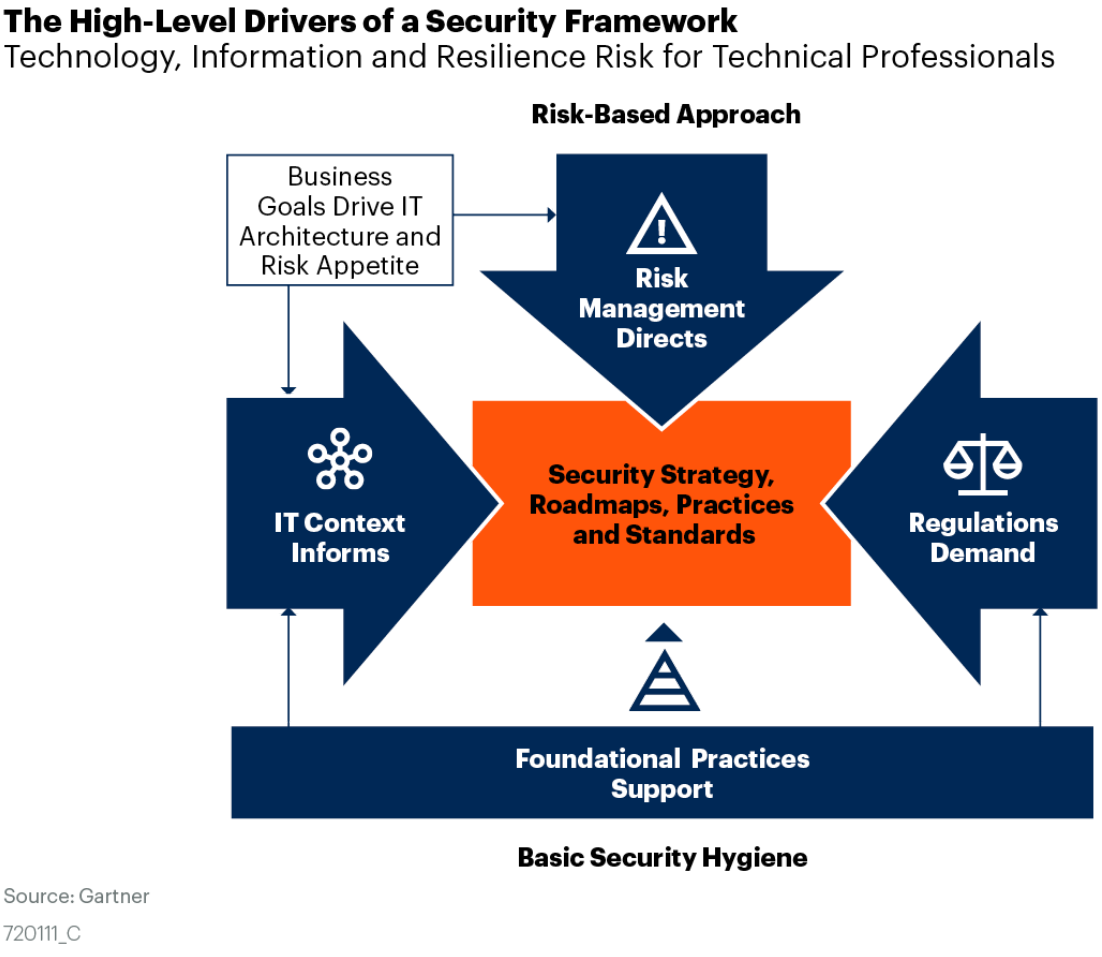
considering the impact of IT risk on the business. Technical practitioners must be able to demonstrate that they have constructed a reasonable foundation on which to base risk management processes and assessments, as well as requests for budget and resources.

Understand the Drivers for Security

Understanding the drivers for selecting controls is important in building a security plan that is attuned to the business. Buying based on marketing hype, instead of a detailed security plan, leads to poor control, wasted resources and a negative perception of the security team. Security should be no different from any other part of the business. That is, security organizations should invest in resources only when there's a demonstrable reason for doing so. Understanding the specific business benefits of security is one of the outcomes of risk management.

Figure 1 shows the three drivers for security controls.

Figure 1: The High-Level Drivers of a Security Framework



Source: Gartner
720111_C

- **The IT context** *informs* the need for a number of security requirements, driven through best practice and common sense. For any given IT asset (whether application, API, system, network or data), some threats are common to all organizations. A risk management framework is not necessary to determine the need for these basic controls. It is this "commodity" set of controls that is the main focus of the document.

- **Regulations** *demand* compliance. It is not acceptable for an organization to be noncompliant with a relevant regulation or industry standard; such failure could be very punitive. Treat compliance as a necessary, but insufficient, outcome. Remember that regulations and industry standards focus only on the issues perceived by that authority as risks or threats to be addressed. For example, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is necessary for payment card handling. However, PCI DSS compliance does not address the security of your personnel database, the security of your R&D or engineering teams, your privacy requirements, or your contractual obligations.

- **Risk management** *directs* choices the organization can make about the required security practices. It identifies and assesses specific assets, threats and outcomes; defines the risk; and determines what should be done. This evaluation results in removing, reducing or accepting the risk. Risk transference is more difficult for security risks. Although the growth of the cyberinsurance industry is making this option more viable, cyberinsurance does not allow the organization to abdicate responsibility for security. We discuss basic risk management frameworks in the Risk Management portion of The Details section.

Figure 1 also demonstrates how Gartner views the relationship between basic security hygiene and a risk-based approach. A risk-based approach must be built on a sound set of basic security practices. These practices include controls from IT-context-driven best practices and from regulatory requirements.

The optimal approach is to start by doing what you *must do* and what is *commonly done,* providing the basis for moving forward into more discretionary practices.

It is important to understand that the process of choosing and implementing basic security practices is not a one-time event. The process must continue and evolve over time, led by changes in technology and IT best practices, or by the introduction and progression of regulations. Frequently, this evolution will be a response to additional needs identified through a change in context and a risk-based analysis.

Enabling Security Effectiveness Through Foundational Practices

All security controls, basic or otherwise, are supported and enabled by the environment in which they exist. For example, vulnerability management processes need to be able to link IP addresses to systems in order to enable remediation. This requires an asset database and, ideally, IT service management processes. These foundational practices are often not managed by the security function, but a good security plan will address the dependency.

The foundations discussed here are:

- **Policies, standards and culture:** Provide a broad direction for the organization and set expectations for user behavior, process definition and technology use.

- **Architectural rigor:** Provides a formal approach to designing both enterprise and security architecture.

- **Identity and HR management:** Controls user access to your assets based on role.
- **Asset management:** Provides visibility into what you're trying to protect and why.
- **Procurement:** Helps both workforce management and asset management by controlling acquisition of resources.
- **IT service management (ITSM):** Provides governance over IT activities. It includes
  - *Change management:* Governing and recording the status of the environment and its components
  - *Incident management:* Governing and defining how incidents are prepared for, responded to and managed

Figure 2 illustrates the typical impact that these foundational practices can have on security, by mapping them to security control groups (described in the Guidance section).

Figure 2: The Impact of the Foundational Practices on Security Effectiveness

The Impact of the Foundational Practices on Security Effectiveness

Occasional Impact | Context-Driven Impact | Strong Impact | Critical Impact

Foundational Practices	Security Groupings								
	Data	Governance and Risk Management	Application	Endpoint and Mobile	Infrastructure and Network	Security Monitoring and Operations	Threat and Vulnerability Management	Cloud	Identity and Access Management
Policies, Standards and Culture	●	●	◕	◕	◕	◕	◕	◕	●
Architectural Rigor	◕	◕	◕	◑	●	◕	●	●	◑
Identity and HR Management	◕	◔	◑	◑	◔	◕	◑	◕	●
Asset Management	◔	◔	◔	●	◑	●	●	◑	◕
Procurement	◑	◔	◑	◕	●	◑	◑	●	◕
Change Management	◑	●	◑	◑	●	◕	◕	◕	◔
Incident Management	◕	●	◑	◕	●	●	◑	◕	◕

Source: Gartner

720111_C

Organizations will experience differences in the strength of the dependencies. However, note how each foundation strongly impacts many security areas. This highlights the general importance of the foundations as universal activities. In other words, unlike the security controls themselves, the foundational practices are not based on any context, risk or regulation.

Note that the weighting given to any particular relationship will also vary across the specific controls within each grouping. Avoid arguments about the details. The objective is to highlight how and why the foundational activities are important in general.

The consistent themes of the foundations are *control, stability* and *insight:*

- **Control** means that activities happen according to a predefined process, and that mechanisms are in place to limit the possibility of actions occurring outside that process.
- **Stability** means that changes to the environment are thoughtful, rational and subject to some form of controlling governance.
- **Insight** allows the organization to know, understand and react to the components and activities within the environment, such as people, applications and APIs, systems, and cloud services.

Strengths

The strength of this approach is that it allows technical professionals to start effectively addressing standard threats and vulnerabilities, while simultaneously building the foundations necessary for a risk-based security model. The majority of significant breaches over the past decade have been attributed to failing to follow the most basic of practices, such as patch management. Most organizations face a common set of threats, such as ransomware or nontargeted phishing attacks, irrespective of their specific regulatory requirements or business activity. Leveraging the experience of thousands of organizations to select standard controls that address those commodity threats and risks tempers the need to start with a risk management process. Additionally, it can reduce the “noise” in your environment, so that you will be better-positioned to detect and defend against more advanced and more damaging attacks.

By using the drivers of regulation and context to identify initial requirements, organizations can take early advantage of checklists, standards and guidelines such as NIST or the Center for Internet Security (CIS).

Weaknesses

This approach is *only the beginning* of a security journey and is not a complete framework for long-term security effectiveness. One of our top concerns in developing this document is that it will be perceived as a final destination rather than a starting point.

> **Basic security hygiene is necessary, but not sufficient. At some point, the organization must build on this position through a risk management**

approach.

Basic network security, for example, is only sufficient while the application team is using “classical” infrastructures. A move toward platform as a service (PaaS) environments or distributed application architectures makes traditional network security approaches less relevant and will require a different mode of thinking. Similar developments apply to data security, where regulations increasingly imply that security should be an active part of a broader data governance approach.

Even basic security requires a significant number of controls. The individual organization must determine which of those to prioritize. This approach does not provide a low-cost security plan, so organizations with budgetary issues will need to make decisions about what to leave out or defer. Those decisions will require some level of risk assessment — which is why we suggest taking this approach in parallel with building a risk management program.

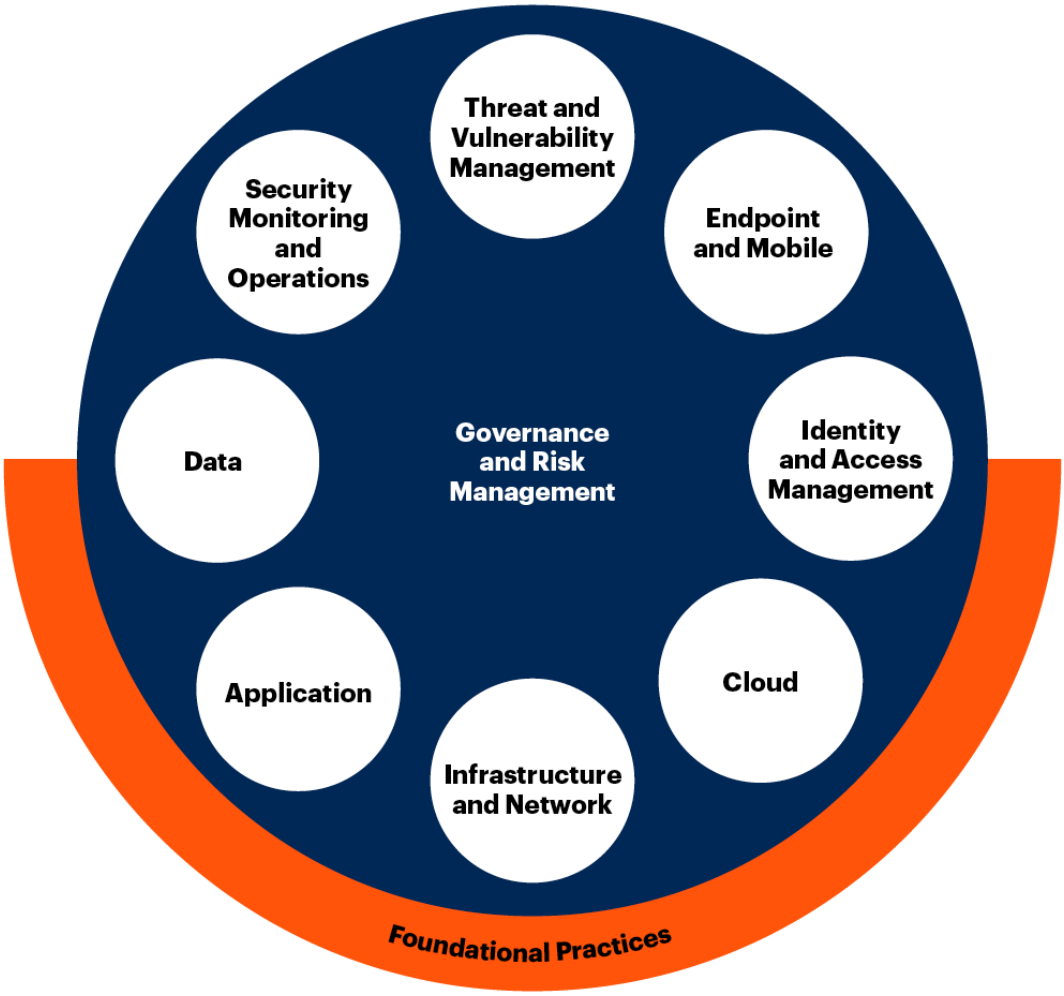
Guidance

A Framework for Basic Security Hygiene

Figure 3 illustrates the security control groups used in this document. This structure will be used to organize the rest of this Guidance section, as well as The Details section that follows.

Figure 3: Basic Security Groupings and Foundational Practices

Basic Security Groupings and Foundational Practices



Source: Gartner
720111_C

Vendor opinions might differ in terms of which group or groups their tools reside in. The security industry is continually shifting, and vendors are always looking to differentiate their products. Do not be concerned by these semantics. You should base your control selection initially on context and regulation, and then, eventually, on risk. After deciding what *control* you want, you will then select tools and vendors.

As part of this research, we also provide links to Gartner documents that are relevant to each practice and control. These documents offer more in-depth insight into selecting and operating a specific control, including vendor options.

A Quick Overview of the Security Groups

Here, we introduce the different security control groups shown in Figures 2 and 3. We address the foundational practices in detail later in the document (see The Foundational Practices section):

- **Governance and risk management:** Security requires constant oversight to ensure it's delivering the right controls at an acceptable level. Similarly, getting a basic risk management process implemented is necessary in order to appropriately move beyond the fundamentals presented here. The risk-based approach must itself be based on sound practices, which is why

we include essential risk management capabilities within basic security hygiene. Successful governance also links security with other activities in the organization, such as HR, procurement and the business. *Build relationships with those departments to support future development of integrated risk management and to drive early improvement in the foundational practices that support the security effort.*

- **Threat and vulnerability management:** Security aims to identify threats, patch or otherwise remove vulnerabilities, and then apply controls to mitigate remaining threats. Vulnerability management through scanning or limited penetration testing is a basic security practice, and it allows prioritization of remediation or mitigation activity.

- **Infrastructure and network:** The data center and the network typically host the most critical assets of the organization's IT environment. The use of virtual infrastructure as a service (IaaS) and infrastructure as code (IaC) environments has changed what infrastructure means. Network security includes activities protecting IaaS environments, local-area and wide-area networking, B2B networks, and other forms of remote access.

- **Endpoint and mobile:** The server or the user device (laptop, mobile phone or tablet) is a major component of all IT architectures, and introduces similar issues to all organizations. A major problem for organizations is the introduction of bring your own device (BYOD) and the loss of control that results. Organizations face a tension between the following two factors: (1) convenience and cost; and (2) the dangers of placing business data and processes outside of their direct control. A variety of BYOD management approaches exist, with some basic options suggested here.

- **Application:** Application security is about ensuring that the applications you develop or procure adequately protect the data and systems they utilize, both in development and at runtime. Applications are often highly specific to the organization, especially when developed in-house. However, common practices in the areas of procurement, development and testing can help mitigate commodity security issues.

- **Data:** Data security focuses on protecting data as it is processed, stored or transferred, rather than on protecting the systems that are hosting the data. Most security activity is, in the end, about protecting the data, because that's typically the regulated or valued asset. However, there are specific approaches to protecting data that are discussed in this section.

- **Cloud:** Most security concepts apply equally to both the cloud and the traditional data center, but how the concepts are implemented and operated may differ. For example, using cloud IaaS does not remove the need for endpoint, infrastructure and network security, and SaaS applications still require identity and access management (IAM) controls. Approaches to regulatory compliance also change in the cloud, because you lose direct control of some requirements.

- **Security monitoring and operations:** As security controls become more involved, and threats more advanced, no single tool can mitigate all issues, let alone resolve them. It is important to

at least measure the quality of operations to support service improvement and greater security effectiveness. This implies that organizations should move from "occasional review" of controls to continuous monitoring and incident response. This group includes the use of security controls and processes — such as ongoing penetration testing and KPI tracking — to support measurement, testing, reporting and audit.

- **Identity and access management:** Access control is often the main goal of security. IAM governs which entity (user, thing or process) has access to an asset, and provides assurance (through authentication) that the entity is who/what it claims to be. IAM applies at all parts of the IT context, within applications and as part of many data security controls. IAM is a separate security group, because there are distinct controls. However, other controls usually have elements of IAM either built in or as a dependency for their correct function.

Table 1 provides a summary of the control groupings. More specifics are provided in The Details section later in this research.

Table 1: Summary of Basic Security Hygiene Practices, by Security Group

Practices	Basic Controls*
Governance and Risk Management	
Security Policies	■ Build a security policy framework ■ Develop information classification rules, schema and guidance
Security Program	■ Identify and assign authority and ownership ■ Establish a security awareness program
Risk Management	■ Establish a basic risk management process ■ Develop basic context information ■ Assess and treat risk
Quality and Performance Management	■ Develop basic metrics and measurements ■ Perform an annual independent audit of key systems/environments
Threat and Vulnerability Management	

Vulnerability Assessment	■ Perform regular vulnerability scanning for internal- and external-facing systems
Patching	■ Implement a prioritized patch management program
Change Detection	■ Implement change detection in configuration of systems
Penetration Testing of High-Value Systems	■ Perform, or contract for, regular penetration testing of high-value systems
Infrastructure and Network	
Infrastructure Security	■ Establish physical protection ■ Implement privileged access management ■ Develop and test basic disaster recovery plans ■ *Consider approaches to "secrets" protection* ■ *Consider approaches to rogue device detection*
Network Security	■ Implement a firewall and VPN at the perimeter ■ Implement wireless network security ■ Use network intrusion detection system/intrusion prevention system (IDS/IPS) capabilities ■ Design network segmentation/zones to separate systems ■ *Consider distributed denial of service (DDoS) protection* ■ *Consider network access control (NAC)* ■ *Consider other methods of egress filtering, such as secure email and secure web gateways*
Endpoint and Mobile	

Endpoint Security	■ Implement a patch management process ■ Implement endpoint protection software ■ Develop configuration and hardening standards ■ Implement full-disk encryption (FDE) ■ *Consider basic backup and data recovery* ■ *Consider application control, device control and whitelisting*
Mobile Security	■ Design a mobile device strategy and governance process ■ Implement mobile device policy management (such as Microsoft Exchange ActiveSync) ■ Implement an enterprise mobility management solution ■ *Consider a light-touch unified endpoint management (UEM) approach* ■ *Develop a mobile threat defense (MTD) system* ■ *Use mobile device management (MDM) where available* ■ *Consider a cloud access security broker (CASB) if you are using cloud as part of your infrastructure*
Application	
Application Security Development	■ Provide basic education, training and awareness for code developers ■ Push for a basic QA process for code development ■ Introduce structured security testing of code, such as static application security testing (SAST) ■ Require version control and release management of custom code; provide a secure repository for custom code and libraries ■ Implement an approach to trusted components/framework security ■ *Consider a limited dynamic application security testing (DAST) program* ■ *Evolve your development team training, testing and incident review* ■ *Build maturity into a secure software development life cycle* ■ *Evolve to require trusted components and repositories*

Application Security Operations	■ Perform infrastructure dependency analysis ■ Introduce web application firewalls (WAFs) for high-value, internet-facing applications ■ Use authentication and access control within applications ■ Implement a log management system ■ *Consider advanced web application protection*
Data	
Data Security Planning and Strategy	■ Introduce a corporate data security policy ■ Start a program for data inventory and classification ■ Implement database access control ■ Implement a data backup solution ■ Require transport layer encryption for sensitive data ■ Implement data loss prevention (DLP) for email and web access (i.e., SEG and SWG) ■ Use controls available within SaaS environments ■ *Increase use of encryption* ■ *Expand your DLP capability* ■ *Consider classification and tagging tools* ■ *Consider database audit and protection*
Cloud	
Cloud Security Design, Governance and Use	■ Implement a CASB ■ SaaS: Evolve your IAM practice ■ PaaS: Evolve IAM and application security practices ■ IaaS: Evolve IAM, application security and endpoint security practices; apply controls to cloud workloads in IaaS, perhaps using cloud workload protection platforms ■ Develop awareness and insight into procurement processes ■ *Use cloud security posture management (CSPM)* ■ *Consider automating system configuration management*

Security Monitoring and Operations	
Monitoring and Security Operations	■ Introduce incident detection, response management and after-action reporting ■ Deploy basic log management ■ Identify opportunities for managed detection and response (MDR) or managed security service provider (MSSP) options ■ Implement operational security metrics and a delivery improvement plan ■ *Expand log management into a full SIEM* ■ *Consider security orchestration, automation and response (SOAR)*
Identity and Access Management	
IAM	■ Implement a structured, central identity management directory/database ■ Standardize account life cycle management ■ Implement authorization processes and reviews ■ Introduce role-based access control (RBAC) ■ Identify appropriate end-user authentication solutions ■ Employ privileged access management approaches ■ *Consider automating account provisioning* ■ *Enhance both RBAC and IAM governance* ■ *Evolve privileged access management approaches* ■ *Introduce single sign-on (SSO)* ■ *Consider using adaptive access approaches*
* Italicized text in this column indicates elective practices, as covered in The Details section.	

Source: Gartner (June 2020)

Effective and Ongoing Control Management

The basic security practices suggested in this research are only a starting point — necessary, but rarely sufficient.

> **Security is as much about detection as prevention.**

When you implement controls, consider how you will be able to use the information they provide to detect an incident in a timely manner. Doing so will lead to better overall resilience, which will provide demonstrably better control of risks.

Developing the security architecture is not a one-off event, but an ongoing process of continual improvement. See "A Guidance Framework for Establishing Your Approach to Security Architecture" for more insight.

It is imperative that opportunities for business risk reduction, or for more effective and efficient delivery, are identified and implemented if required. Some common areas where roadmaps can quickly move beyond the basics include monitoring and response, endpoint threat management, and assessment and remediation of vulnerabilities and risks.

The foundation of a risk-based approach is basic security hygiene, and the foundation of security is good organizational practices. Build one on top of the other, and improve delivery and capability over time. This approach will support future risk assessments by including vital context information, which will have first been identified and developed as part of the basic security practices.

The Details

The Foundational Practices

Building an effective security operation requires reliable foundational practices that are usually outside the security team's direct control. You will need to collaborate with other parts of the organization in order to develop and improve these foundations. The list is not exhaustive across all scenarios or combinations of security controls. Additional requirements will surface as part of the risk-based approach. For example, if your organization decides other controls are required to address vendor risks, then these should be addressed through the procurement and contracting processes.

> **Do not consider these foundations as prerequisites for security — you can continue to implement the security controls even without them. Indeed, it might be easier to convince people of the need for improvement in these areas by demonstrating how current deficiencies impact your controls.**

Policies, Standards and Culture

Security is not just the responsibility of the security team. All parts of the organization must contribute to implementing good practice, mindset and diligence. These practices should become standard operating procedures for IT operations and development. Achieving this normalization

requires building the right culture and developing policies and standards to inform and direct behavior.

Policies and standards are not just about security. They address all domains. For example, policies around finance, procurement, personnel and ethics are common. Security policies that stand alone with no corporate governance context will suffer because of a lack of documented discipline in other domains.

Publishing policies and standards is of no use unless you have the ability to enforce these practices and standards. Proper enforcement requires consistent leadership from the highest levels of the organization, committing everyone to making those changes and holding them accountable when the boundaries are crossed.

Where other governance exists, make sure your security policies (described in the Basic Security Practices section below) align and, if possible, match in terms of language and format. Use any preexisting corporate processes for governance to support the development, ratification and publication of policies. As organizations mature, the need for governance increases, and is demanded by some regulations.

See "Creating Security Standards: Context, Structure and Must-Have Content" for more insight on this topic.

Architectural Rigor

Enterprise architecture (EA) will provide a strategic framework for developing the IT, application and business process environment. But even without formal EA, implementing some form of architectural rigor will bring some predictability and stability to the environment. This helps to drive standards, consistent and repeatable development, and roadmaps. It also helps constrain and guide the implementation of new technologies and new approaches to addressing business needs. With an increasingly mature development practice in the organization, the security practitioner can develop more appropriate security solutions for the organization's development, and be less reactive.

This concept also applies to agile environments. Good security does not preclude the use of high-cadence and innovative development practices. Integrating security decisions into the development cycle, clearly outlining risk boundaries, and enhancing the use of patterns and standard approaches all help to reduce uncertainty and surprise. This allows security to be more predictive, and to provide integrated and supportive solutions to the development team.

Work with the CIO and other stakeholders to introduce and develop an architectural practice — perhaps even an EA team. Advocate for a security seat on the EA team, in order to:

- Proactively identify and resolve security issues before they become problems
- Incorporate security as part of the decision-making process

Identity and HR Management

Security can often be seen as an access control problem — i.e., allowing entities appropriate access to systems and data such that they can perform their roles. IAM forms the most visible part of this activity, and affects people, devices and applications alike. Success depends on the organization continuously knowing who is eligible to access an asset and with what capabilities. The lead responsibility is typically with the personnel team, but procurement and legal also have a role, because IAM applies to all workers, not just employees. Outsourcing activities at any scale usually require workers other than employees to have access to one or more data or other assets. Customers may also have access, and such access needs to be equally understood and managed. If the list of people and their roles is not correct or complete, then the security controls won't be either, significantly limiting their effectiveness.

Work with personnel and line managers to drive continuous improvement in the personnel process, so that a formal process for the user life cycle is in place. Use role-based access control (RBAC) to enable standards for access, rather than a per-user approach. Procurement and legal must work with the team requesting the resource to define roles for other workers, as well as contract requirements for other personnel. Require line managers and system owners to review access lists regularly, with a cadence aligned to the sensitivity or criticality of the data or system.

The objective is to develop the following:

- A continuously accurate list of all users and their roles
- An effective process for maintaining that list for all users, not just employees
- An effective link between that list and the team or teams implementing authentication and access control

Asset Management

Asset management strengthens security controls by providing insight into the coverage of the controls. *If you don't know what you have, you can't know what to protect.* Endpoint security controls need to be distributed throughout the environment tactically, rather than randomly. Without an accurate record of the endpoints the organization has, the security professional cannot attest to the level of coverage, leaving a gap of unknown size and, therefore, unknown risk.

Asset management provides the insight required to determine what needs protecting and which parts of the IT system can act as vectors for attack. Assets include, among other things:

- IT systems (including various cloud types and Internet of Things [IoT] environments)
- Data (including code)

An ideal asset management approach merges the two to provide a map of the overall environment, enabling sensitive hot spots to be identified. However, asset management will often be handled by multiple groups (e.g., IT, applications, finance and procurement). Because each

group will have a particular focus, a comprehensive asset management system may be impractical at the outset. Therefore, expect this to be a program of continuous improvement.

Focus initially on the following:

- Work with the appropriate other teams to enhance existing lists and governance practices to support the controls you are building. Ideally, a centralized and dynamic asset database will be created, along with appropriate processes to ensure it is properly maintained.
- Avoid snapshot lists that are improperly maintained. However, do not expect 100% accuracy. There will always be churn in an environment, and this churn drives some inaccuracy. Orchestration tools can automate record keeping and reduce this inaccuracy, but will not eliminate it.
- Track user endpoint devices through client management tools and scripts. It's not safe to assume that each user will have only one device.
- Work with the procurement team to record how and what systems, applications and services are bought. Knowing what is introduced to the environment simplifies the security problem.
- Push for development of an IT service inventory that identifies the services IT manages, the business customers that are dependent on each service, and the IT individuals who are responsible for supporting each service. This list of services will help identify required controls and support risk assessment.

Procurement

Procurement has a significant effect on the IT environment and the risks it faces. A poorly controlled procurement system can introduce a range of risks, including shadow IT or poorly written contracts. Individual purchasing capability can allow unconstrained cloud purchasing, internet connections or even third-party application development. Procurement drives quality in third-party relationships and can effectively eliminate shadow IT if addressed properly.

Work with procurement teams to limit, where possible, individual purchasing power, corporate credit card use and authorization to enter into contracts. These steps can help improve the predictability and stability of the environment from a security perspective. Such improvements, in turn, can reduce the unknowns for the security organization, allowing more effective control. Additional benefits can include:

- Reduced complexity and heterogeneity in devices and endpoints
- Improved stability of IT components
- Lower support costs
- Faster response and resolution times

Controlling application development, as described in "Best Practices for Securing Continuous Delivery Systems and Artifacts," can reduce costs, improve consistency and increase reuse of trusted components.

IT Service Management

ITSM covers a range of practices that formalize IT services and activities. The implementation of ITSM brings benefits such as measurable delivery, service catalogs and continual improvement. All ITSM practices are important to security, but two processes in particular provide significant benefit: change management and incident management.

Change Management

Although stability is important, no IT system ever remains frozen for long — especially in a DevOps environment. More generally, as organizations, technology and the environment change, so will the business processes and the technical architecture. Change management provides governance before, during and after the event, allowing security to plan and react. It allows for proper evaluation of changes, planning of change processes, identification of any "knock on" effects and maintenance of the asset database.

> **Formal change management processes range from the highly detailed to the very light touch. At least include simple security vetting in change management.**

If there is no change management process, work with IT and application leaders to introduce a light-touch approach that addresses significant changes in systems, applications and networks. Developing automation in any change management process will speed the flow and encourage its acceptance.

See "How to Implement a Modern IT Change Management Practice" for more insight on this topic.

Incident Management

By introducing security controls, the organization creates a need to manage the security incidents that will become visible. Controls will make unwanted activity visible or possibly cause service impacts to the organization. Management for security incidents is not the same as management for IT incidents, but the existence of an IT incident management plan will aid security.

A useful security incident management plan will include:

- A plan for determining which sensors from the controls are being used to prompt incidents, how and when.

- A response and management process to stop, recover and mitigate an incident. There may be more than one of these, known as “playbooks,” for more complicated environments.
- A review process, known as an “after-action review,” “root cause analysis” or “problem analysis.” This analysis allows planning to prevent a recurrence or, at least, development of an improved response and mitigation process for any recurrence.

See “How to Implement a Computer Security Incident Response Program” for more insight on this topic.

Basic Security Practices

The following sections describe the basic security practices applicable to most organizations. They are divided into “basic” and “elective” sets.

“Elective” practices are those that are on the brink of being basic security practices and that should be considered for inclusion in your baseline approach. They are usually more complex in both their implementation and their dependencies. Exercise caution when considering early adoption of such practices. Elective practices should be factored into security planning discussions and considered as early next steps for most security program roadmaps.

This guidance is provided with the following caveats:

- A practice may be omitted, but only after a risk-based analysis that considers costs, benefits, and any alternative or compensating controls. Of course, if there is no technology or process in use that warrants the control, then don’t implement it. However, remember that these controls are considered “basic” because they address universal risks and threats. These controls should be treated as standard mitigation measures for those common risks.
- This guidance does *not* account for practices required by external authorities. Regulatory requirements usually make a control mandatory. Make sure that your list of controls reflects those external requirements in addition to these basic practices.

Governance and Risk Management

It is critical to have some basic structures in place for security governance and risk management, in order to establish the role and precedent for a security program. Individuals should be identified and assigned with key responsibilities and authority for security decisions. Identify individuals who can provide leadership and guidance, and who can help others embed good risk decision making into their daily activities. Work in a collaborative manner across the organization to mentor, educate and influence people about security and about making better risk decisions. These steps will help build a security-aware culture. For more insight, see “Security and Risk Management Programs for Technical Professionals Primer for 2020.”

The following practices are necessary to support a security program that can be seen as providing reasonable care. It will be very difficult for security and risk management practitioners

to be successful without these basics in place.

Security Policies

Policies reflect the organization's security objectives. They inform the workforce about how they should behave and think about security. The policy framework should be supported by standards — i.e., documents targeted toward technical architects, engineers and administrators defining controls, processes and practices that must be followed.

- **Security policy framework (priority):** A minimal set of policies should be published and endorsed at the highest levels of the organization to authorize the program and provide authority to act. A base set should include:
  - *Corporate security charter:* This is a high-level policy that indicates what the organizational position is for security and board accountability. It also provides a basic description of the security organization.
  - *Information-handling policy:* Based on the information classification policy (see below), this policy describes the limits for the use of sensitive information. For example: "Secret information must never be sent by email, and only people with a need to know should be granted access."
  - *Acceptable use policy:* This is a broad set of statements about how users should act when using corporate systems, or when representing the organization on the internet. For example:
    - "Do not leave corporate laptops in vehicles or unattended in public spaces."
    - "Do not use corporate systems to access gambling sites on the internet."
    - "Do not use corporate systems to run a private business."
    - "Report all security concerns to the security team." *(Give an email address.)*

Avoiding Policy Pitfalls

Policies may have unintended side effects. Therefore, although it sounds counterintuitive, you need to avoid going into too much detail. Policy documents should be accessible to the target audience (your whole user community), as well as freely available. Draft policies and standards in partnership with operations teams and business owners. Be careful when documenting a requirement that cannot be easily enforced, else you run the risk of undermining the credibility and standing of the policy framework (including its legal authority).

- **Information classification policy:** Much (but not all) security is focused on protecting information assets, some or all of which might be subject to particular regulations. An information classification policy provides the framework for determining which information falls into what category, and helps users make more consistent decisions. Typically, information classification focuses on confidentiality, but other dimensions can be important. Categorizing information by its type (e.g., personally identifiable information), by its business owner or by its regulatory oversight is common. Information classification should form the basis of security architecture standards. Classification can be used as decision-making support for the risk-based development of future architectural standards, such as encryption, network compartmentalization, data sharing and access control. This approach avoids inconsistent decisions, excess cost and resource demands, and helps to align security, IT and business architecture.

Security Program

A typical regulatory requirement is that organizations must have a formally defined security program, even if most security-related practices are embedded within operations and development teams. Most security frameworks and standards (e.g., ISO/IEC 27001 and NIST Cybersecurity Framework) have a similar stipulation. There are good reasons for this, such as:

- Security accountability resides at the C-level, and security lapses can potentially bring legal action against both the company and its officers.
- Security, via risk management, can form part of the organization's financial statements. An assertion by auditors or C-level officers needs to be based on some level of rigor in the security practice.
- Failure of critical infrastructure and control systems can have a huge impact, even introducing physical risk to people.

Therefore, the following attributes must be accounted for in the foundation of the security program:

- **Authority and ownership (priority):** *Assigning responsibility without authority is ineffective.* The security team must be clearly delegated the authority to act, and it must be supported at the top of the organization. A failure to correctly assign responsibility and authority can lead to the impression that an organization is not committed to addressing security. That said, you need to address the following questions:
  - Who is ultimately in charge?
  - Who has final say on security recommendations and practices?
  - Who is responsible for briefing executives and the board?

- What authority do security and risk management professionals have to instigate change within the organization?

- **Security awareness program:** Security awareness is a key component of a security program. People need to be adequately informed of security goals, acceptable use of technology and data, and specific information relevant to their day-to-day roles. Don't try to make the general user a security expert, but avoid relying solely on annual computer-based training (CBT) modules. Create ongoing programs that provide timely and meaningful guidance to people. All awareness program initiatives must have a means for measuring effectiveness, such as a quiz (possibly with a prize). Initiatives should be tailored to specific audiences and designed to meet a specific need, to reinforce the policies or to address particularly concerning risk factors. For example, the general workforce should be informed about the acceptability (or otherwise) of sharing passwords and accounts. However, details about password encryption, storage, and the strict process for password creation or reset are useful only to IT professionals.

Risk Management

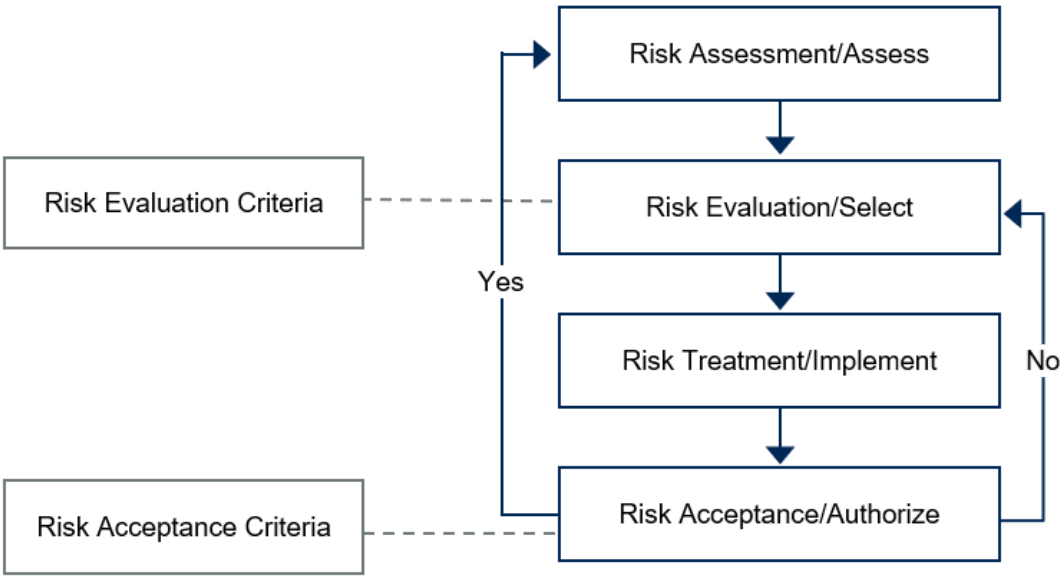
While much of this document discusses implementing basic controls without the need for a risk management process, this approach will not be sufficient in the long term. It is incredibly important to establish at least a basic risk management process as early as possible. A simple approach that focuses on consistent risk assessment in a basic workflow is all that is needed to start with.

Getting the basic risk management process in place provides the foundation upon which prioritized improvements to basic security can be made. It also provides a structure to support change management and to track, document and respond to issues, such as the output of an after-action review.

A number of frameworks provide accessible risk management processes that can be easily implemented within an organization. These frameworks include NIST Special Publication (SP) 800-30, ISO 31000, ISACA COBIT and OCTAVE Allegro. The use of a framework is not necessary, although it can help with implementing a defensible solution. Figure 4 shows a simple, generic approach to risk management.

Figure 4: A Simplified Risk Management Process

Simplified Risk Management Process Circle With Criteria



Source: Gartner
ID: 461795_C

There are three key activities within the risk management process that must be included as a basic starting point:

- **Context:** Establishing context involves understanding the business and identifying key processes, key systems and data sources, key personnel, and sensitivity to loss and exposure. Without context setting, all additional steps lack the necessary foundation to be meaningful.
- **Assessment:** Assessment aims to understand the risk, its causes, its potential impacts, its level of acceptability and the possible options for managing it. Documenting these issues allows organizations to make decisions in the short term while establishing a long-term "memory" for ongoing risk management.
- **Treatment:** Finally, a treatment (or remediation) decision must be made, even if that decision is to "do nothing." A key consideration for risk treatment is ensuring that the risk assessment findings have been properly communicated to decision makers. All outcomes must be recorded and tracked through a risk register. Initially, a spreadsheet is usually sufficient, with IT risk management tools being an option for later use when the base process is mature.

See "7 Critical Elements of a Security Risk Management Framework" for further insight on this topic.

Exception Management

Fostering a corporate culture of security is very important, and this is best achieved through both top-down example setting and workforce awareness and education. Individuals need the latitude to do their jobs, but must also have the necessary knowledge to make appropriate decisions for which they can be accountable.

For example, applications may be developed in an agile environment. To enable success, organizations must give people the freedom to experiment. However, at the same time, organizations must also expect those people to recognize, own and respond to failures quickly. A culture of security responsibility helps individuals contribute to the security program, enables earlier detection of issues and provides opportunities to keep small problems from escalating.

Security policies embody the organization's default position for risk management. Policies and standards address commonly understood threats and implicitly manage a set of risks as a result. Activities that don't comply with policy are not necessarily unacceptable, but they introduce risks that may not have been previously identified.

Develop policies that prescribe acceptable use and basic security requirements. Initially, these policies will be user-facing documents rather than detailed security standards for architects and engineers. They should therefore focus on behavior and attitude, rather than detailed technical statements. You will develop technical standards and specifications as part of the outcome of a risk management process and in consultation with stakeholders, such as IT, application developers and business leaders.

Occasionally, however, you will come across a situation where it is not possible to comply with a policy or standard. To address these circumstances, use an exception process. This provides a "get out" clause that recognizes that policies cannot predict every situation. An exception process allows a noncompliant project to request approval to continue, but only after a risk assessment. That assessment might allow the project to continue (perhaps with specific mitigations). Or, it might require the project to change or cease altogether if the risk remains too high even after mitigation.

> **Record any activity that continues to be noncompliant in a risk register, even if it has been approved based on use of mitigating controls. Review all risks regularly to assess if the risk remains acceptable. The review frequency will depend on the severity of the risk.**

The risk register will provide important information toward policy review. Once assessments have shown that a risk is either acceptable or specifically prohibited, policies will change to subsume those findings accordingly. Continuously aligning policy with such findings provides clarity and avoids repeating assessments. Adjust standards to reflect alternate approaches to maintaining acceptable security levels.

Review all policies and standards periodically, at least annually. Perform exception-based reviews when new information or circumstances imply that a significant change might be required.

Introduce formal governance processes to support the authority of the risk management processes and policies.

See "Creating Security Standards: Context, Structure and Must-Have Content" for further insight to this topic.

Quality and Performance Management

In building a security practice, you will be developing operating processes that are important to protecting the business. Tools and processes will need to be maintained at a level of quality and performance to secure the organization. Thus, you will need to:

- **Develop basic metrics and measurements:** Measurement provides various insights into how well you are doing and how much progress is being made. You do not need a lot of metrics, but it is a good idea to develop a set of measures that focus on your priorities. Start your program with operational metrics that reflect the performance of the controls and of the teams delivering them. See "Developing Metrics for Security Operational Performance" for further insight.

- **Conduct an annual audit of key systems/environments:** An audit compares the delivery of controls against policies and regulatory requirements. If this review is performed by auditors, they may also comment on the policies and controls themselves — offering insight into any gaps they identify. Feed these comments into the ongoing control selection and risk management processes. Audits need not be extensive (unless mandated by regulation), but they should, at least, report on adherence to policies and processes. Auditors will require documentation and records to demonstrate that processes are being followed. Make sure all relevant processes record actions, document decisions and review outcomes continuously. An external audit helps keep your organization honest, but unless regulation demands otherwise, an internal audit team is a good place to start.

Threat and Vulnerability Management

Threat and vulnerability management cuts across many other areas, and is one of the most important topics for basic security hygiene. Visibility into vulnerabilities is a core security requirement that enables patching. It also informs risk management, identifies control requirements and focuses security activity. Key practices include:

- **Basic vulnerability assessment on external-facing and high-value systems:** Run vulnerability assessment tools against external-facing and high-value systems to identify any exposed major vulnerabilities. Cloud-based tools can simplify the deployment of vulnerability scanning infrastructure. Most tools will include some element of threat information to help assessment and prioritization. Use this information to help teams prioritize and fix the high-risk issues first. Scanning should be performed frequently, at least monthly. See "A Guidance Framework for Developing and Implementing Vulnerability Management" for more information.

- **Patching:** Patching is rarely the responsibility of the security team. However, security should act as a guide and orchestrator for patching activities. IT teams can suffer under the weight of patching requirements if a "patch everything now" approach is taken. Work with delivery teams to prioritize patches, understand conflicts and issues, and support them in establishing "patching windows."

- **Change detection:** Change detection insight is often provided via file integrity monitoring (FIM) solutions or system compliance tools. It will also come from endpoint security or log review. Change detection helps monitor the operating state of environments and can provide a rudimentary form of anomaly detection. Basic reporting on change detection is critical, especially for high-value systems, including point-of-sale systems, internet-facing systems or systems subject to standards such as PCI DSS.

- **Routine penetration testing of high-value systems:** Testing, including penetration testing, is more than just an audit or vulnerability assessment. It identifies potential weaknesses and also validates those findings, converting "could be a problem" to "definitely is a problem." Unfortunately, a good penetration testing service can be expensive, which is why limiting it initially to just high-value systems and applications makes sense. Expand penetration testing to other systems when the organization is ready to act on the information. This approach is helpful, because many compromises start with lower-value systems and then use them as a stepping-stone to attack high-value systems. See "Using Penetration Testing and Red Teams to Assess and Improve Security" for more information.

Infrastructure and Network

The network and data center provide the main IT facilities for the organization, and a number of controls should be implemented as a default. Endpoint security, including anti-malware, patching and configuration standards, is critical for servers (see the Endpoint Security section below). IAM, discussed in detail later, provides a significant amount of threat management. Here, we discuss basic security practices specific to the management of the core infrastructure.

Many organizations are moving some or all of their infrastructure to a cloud environment. We address cloud-specific security practices later in the Cloud section. The approaches discussed in this section should also be applied to cloud or virtual data centers — the tools differ, but the control remains the same.

Infrastructure Security

The data center and its systems contain the most sensitive and valuable of corporate assets. Comprehensive security hygiene for the data center is a combination of all the elements of this document. Additional practices that should be addressed are:

- **Physical protection (priority):** Your central infrastructure needs physical protection from attack, the elements of nature and random events (such as power failure). Whatever the physical nature of the environment, the "data center" should have appropriate physical access controls,

limiting who can gain entry and when. Power supply continuity, flood protection and fire suppression all form part of physical protection.

- **Privileged access management (priority):** This is discussed in more depth in the Identity and Access Management section. At a basic level, users should not be using their day-to-day account to perform privileged commands, such as system builds, patching or maintenance. Require the use of a secondary user-specific account or a dedicated administrator account for privileged activities. Limit the use of generic accounts, such as "root" or "local administrator," to enforce attribution and reduce password sharing. Consider revoking some privileges and allowing them only on a per-event basis. See "Best Practices for Managing and Governing Third-Party Identities, Including Contractors and Business Partners" and "Guidance for Privileged Access Management" for more information on this topic.

- **Basic disaster recovery plans (priority):** Even with a business continuity plan, which enables business operations to continue, things will break and need to be repaired. Document basic processes for the most complicated and highest-negative-impact scenarios. For example, what happens if a data center goes offline? What happens if there is a fire in a facility? Disaster recovery plans need not be overly complicated. Management and administrators must walk through several scenarios, adding response procedures where possible, to reduce the impact of a disaster event. See "Data Center Infrastructure for Technical Professionals Primer for 2020" for further insight.

- **Elective practices:**

  - *"Secrets" protection:* When systems and applications communicate, they must authenticate, and that process involves the exchange of a "secret" (e.g., a password or token). Placing secrets in code or configuration scripts is a common vulnerability that should be avoided. See "Guidance for Privileged Access Management" for an approach to achieving this.

  - *Rogue device detection:* Unapproved devices on the network can be perfectly legitimate or, alternatively, malicious. A network-connected water-monitoring device in the data center is useful, but an ADSL internet connection is a significant hole in security. Detecting and investigating unknown devices should be considered good practice for the data center. Approaches include implementing network access control (NAC), scanning for IP addresses that haven't been issued, or monitoring Dynamic Host Configuration Protocol (DHCP) and DNS logs for events initiated by unknown devices.

Network Security

Network security remains an issue for both LAN and WAN, and it is now an issue for cloud computing as well. Controlling how things communicate and what they communicate with remains a fundamental security measure. Network concepts have evolved with software-defined networking, microsegmentation, and the increased mobility and distribution of systems, but the underlying principle of "traffic control" remains the same. Regulations often remain focused on traditional network control approaches. Under the surface, applications, servers and mobile

devices still use TCP/IP to communicate, and routing that communication efficiently and securely remains important. A general view can be found in "Security Technology and Infrastructure for Technical Professionals Primer for 2020," but some basic controls are listed here:

- **Firewall and VPN (priority):** Network firewalls remain a mainstay in securing the enterprise network, even with the explosion of cloud services and mobile devices. Vendors now often provide specific implementations of their products for cloud and mobile environments. Similarly, VPNs are a necessity for most organizations, securing remote access and B2B connections (including connections to IaaS environments). Note that specific remote access objectives are often derived from a risk assessment balancing the business needs against the potential solutions.
- **Wireless network security (priority):** Wireless networking is almost ubiquitous. Wireless network security using Wi-Fi Protected Access 3 (WPA3) provides strong defense for the home environment. Although preshared keys may work at home, such shared passwords are poor security for organizations. Utilize certificate-based authentication in the enterprise. For a more robust solution with increased flexibility for role-based and guest access, employ a user- or device-based authentication system (such as NAC).
- **Network intrusion detection system/intrusion prevention system:** Network IDS/IPS functionality can defend against a variety of threats. This control is now an integrated feature of network firewalls. As such, it is often unnecessary to purchase a separate device to get the benefit. Certain use cases, such as separation of duties or virtual patching, may still dictate stand-alone appliances.
- **Network segmentation/zones:** This topic is covered extensively in "Decision Point for Postmodern Security Zones." Separating assets logically and physically limits the potential for attacks to access sensitive systems. Dividing networks into subsections based on some criteria (e.g., functionality, regulation or sensitivity) allows controls to be installed at the boundaries. Even without security controls, use of basic routing protocols or VLANs can limit, or slow, attack and accidental impact. A very basic approach to segmentation may include:
  - A demilitarized zone (DMZ) for internet-facing devices
  - An office network for user systems separate than that for servers and storage
  - A ringfenced system housing PCI DSS data
  - A specific "landing zone" for remote-user VPN access
- **Elective practices:**
  - *Distributed denial of service (DDoS) protection:* For some organizations, DDoS protection is a must, while for others, it is unnecessary. Choosing DDoS protection will be a business decision that is dependent on a few factors. Thus, we have classified DDoS as an elective

practice here. See "DDoS: A Comparison of Defense Approaches" for further recommendations about DDoS protection.

- *Network access control:* NAC is often overlooked. It can be costly and difficult to implement and maintain, but vendors continue to simplify solutions. NAC's success remains highly dependent on the network architecture. If employed to meet specific use cases (such as in wireless networking) or for highly sensitive network segments, NAC can be very valuable at lower cost. See "Guidance Framework for Implementing Network Access Control" for further insight.

- *Egress filtering:* Filtering of outbound traffic is often poorly controlled compared with filtering of inbound traffic. If resources and network architecture allow, all outbound traffic should be controlled, including end-user nonweb traffic and application traffic. Firewall rules should be set to deny by default, and other rules should be implemented to allow traffic from only known systems and applications across specific protocols. Deploying egress filtering is often straightforward, although it can require detailed insight about the communication requirements of both systems and applications. Outbound end-user web traffic controls are discussed in the Data section.

Endpoint and Mobile

Endpoint Security

For the purpose of this research, endpoints include all of the following:

- Workstations (including laptops)
- Virtual desktop environments
- Servers (including virtual servers both on-premises and in IaaS environments)

The basic security hygiene practices generally apply uniformly across all endpoint platforms, although the mechanisms for implementing them may differ. These practices include:

- **Patch management (priority):** If you do nothing else under this category, do this. Exploitation of known, but unmitigated, vulnerabilities is the primary method of compromise for most threats. Security events impacting both servers and workstations occur because of preventable exploits succeeding. The bottom line is that a patched vulnerability is no longer a vulnerability, and eliminating the problem is a better control than mitigation. However, there can be good reasons for not removing a specific vulnerability. Functional impact, decreased reliability and potential disruption to legacy systems are often cited as major risks of patching. The risk register is an important tool when these issues are raised. Patching is not usually the responsibility of the security team, and is better placed with system administrators and application owners. The security team's responsibility is normally to monitor, prioritize and even cajole the implementation of patches.

- **Endpoint protection (priority):** Endpoint protection software is not a panacea for modern-day advanced attacks, but using it remains a best practice. Because nothing truly goes away on the internet, there are sufficient threats to justify having endpoint protection software as a basic control. Without it, you will almost certainly have more security incidents, and worse, you may not know about them. You are also more likely to be seen as incompetent (or negligent) if a major breach is tied to lack of anti-malware protection. In addition, regulatory compliance requirements may dictate using this class of software. See "Comparing Techniques for Endpoint Protection" and "Solution Criteria for Endpoint Protection Platforms" for more information on how anti-malware solutions work.

- **Simple configuration management and hardening:** This best practice makes sense for stability and predictability within the IT environment, as well as for security. Beware of mandating excessive configurations that require more exceptions than implementations. In general, this best practice can be boiled down to a few simple things:

  - *Leverage approved and tested build images secured using hardening standards:* Off-the-shelf hardening standards (such as Center for Internet Security [CIS] Benchmarks) are available and make excellent starting points.

  - *Minimize the software preinstalled on build images, and keep images up to date:* Build images are rarely maintained with patched or updated software, and the build process must therefore include the necessary steps for fully updating the new system. Remove unnecessary software when possible. Although having to install software can slow the build time, it reduces the chance of unintended vulnerabilities existing on the final system.

  - *Limit local administrator/root privileges for workstations and servers:* Administrative privileges on any device should be available as needed, not by default. Excessive privileges provide opportunity for errors to have a significantly higher impact, and for malware and other attacks to act with the same privileges.

  - *Ensure host-based firewalls, including IPS, are enabled on workstations and laptops*: Laptops in unmanaged networks are at great risk, and a default firewall can eliminate many threats. You should assume that even the corporate network is compromised. End-user firewalls can reduce the ability of attacks to propagate around your environment.

- **Full-disk encryption:** Another common regulatory requirement is to deploy FDE on laptops. FDE protects data from theft caused by lost devices or media duplication. In its most basic form, FDE is available for free from all major OS vendors. See "Comparing Options for User Endpoint and Mobile Device Encryption" for more information on selecting an appropriate level of protection.

- **Elective practices:**

  - *Basic backup and data recovery:* Loss of devices and accidental deletion of data are common occurrences. Laptops can be replaced, but the data stored on them can be difficult to

recover. The impact of even limited data loss can be high if events conspire against you. Ransomware attacks present a similar problem. To address these threats, provide a mechanism to back up the data on endpoint devices.

- *Application control, device control and whitelisting:* Preventing unknown applications and devices from use addresses a variety of threats and is common among endpoint protection solutions. However, for many organizations, the complexity of the environment and the processes necessary to make whitelisting useful (rather than just obstructive to the business) can deter the implementation of such solutions. Host-based DLP agents can perform this role with a content-aware focus, at additional cost and complexity. If the endpoint protection solution is in place, this approach is worth considering, because the same agent typically provides the additional functionality. See "How to Plan, Implement and Operate a Successful Application Whitelisting Deployment" for further insight into this topic.

Mobile Security

Mobile device usage continues to grow, and as organizations move to web-based services, more and more of the business process is accessible to the mobile phone or tablet. Users often expect permission to employ these devices for at least a significant part of their roles. Some organizations make mobile devices available for just that purpose. However, the risk of both corporate-owned and BYOD mobility is high, especially in the areas of data loss, malware and access control.

A key question is whether to allow users to employ their own devices for work (BYOD). Employ a split strategy if necessary, allowing personally owned devices to access only lower-sensitivity resources (like email and calendar). Access to other higher-sensitivity resources would then require the device to be fully managed by an enterprise mobility management (EMM) solution.

A variety of tools exist to address these issues, including mobile device management (MDM), mobile access management (MAM), moblie threat detection (MTD), cloud access security brokers (CASB) and enterprise digital rights management (EDRM). These practices are recognized as essential to the security of most organizations, but they remain complicated enough that they may not be fundamental practices for many. See "Advance and Improve Your Mobile Security Strategy" for further insight.

Following is a short list of basic security hygiene practices that help enterprises limit risk exposure related to giving mobile devices access to enterprise resources:

- **Mobile device strategy and governance (priority):** Define the limits of acceptable use for mobile devices, especially for user-owned devices. Specify what kinds of devices and which OS versions are acceptable, and require some form of access control to the device, such as a PIN. The following steps are key:

  - *Establish an acceptable use policy:* As part of your governance, implement an acceptable use policy (AUP) that informs users about what the organization will allow when they're using

corporate devices or services. This policy should include how personal devices may be used for business purposes, and the limitations of such use.

- *Implement basic policy management (priority):* Even a basic MDM control, such as Exchange ActiveSync, is better than nothing. Use a solution that is commonly supported on most mobile platforms, and that requires little management on the device itself. Enforcing device authentication, screen lockout and some form of encryption adds to protection. For BYOD devices, you will need to communicate to users what you are implementing, so that they can make an informed decision about the use of the device.

- **Enterprise mobility management (priority):** EMM is a necessary control and should be used as soon as possible, especially for organizations that proactively encourage the use of mobile devices. These solutions include a range of options, but the immediate goal is to gain some level of control of the data and use of mobile systems. At least, look to implement a "containerized" approach that enables remote data wiping, imposes encryption and enforces authentication of the user. Other capabilities are described in the elective practices. If your organization is supporting, or planning to support, a large field of mobile devices, then EMM will quickly become a critical capability.
- Elective practices:
  - *Unified endpoint management (UEM):* A light-touch UEM approach can support a BYOD environment. Consider offering anti-malware or other security software to users under a corporate license, giving them the opportunity to improve the overall security of their personally owned device. Corporate-owned devices should, of course, be included by default.
  - *Mobile threat defense:* MTD solutions address a wide variety of threats affecting the mobile device, and are useful in both user-owned and corporate-provided devices. Some organizations with specific security concerns, such as government agencies or financial-sector businesses, may want to prioritize this control.
  - *Mobile device management:* MDM solutions allow varied levels of control over the device, ranging from "light touch" to full control. You should apply controls commensurate with the device's level of access to sensitive data.
  - *CASB:* You are unlikely to be able to implement all the controls you want on the device. This is especially true for BYOD systems, because users may not welcome the corporate oversight. A CASB can protect your cloud and some of your physical infrastructure by implementing a variety of equivalent controls at the time of access by the user. These include strong authentication, threat protection, data loss prevention and conditional access policies. CASBs should be considered whenever cloud environments are being used. See the Cloud section for more details.

Application

Application Security Development

Organizations that procure or build applications must consider the security issues that need to be addressed, and this is typically a risk-based process. It requires identifying the processes that are being embodied in the application and the data involved. However, the development process is also a security challenge — the objective being to implement a secure software development life cycle (SSDLC). The goal is development of a trusted process and a trusted toolset. See "A Guidance Framework for Establishing and Maturing an Application Security Program" for further details.

The following practices apply to application security development:

- **Basic education, training and awareness for code developers:** Developers are actually implementing and securing your code. Make sure they are aware of the processes they should follow and the specific requirements for code use, structure and policy compliance.
- **Basic quality assurance (priority):** All software should go through basic functional and security testing as part of routine QA processes. Define functional and security requirements upfront, and restrict "drift" by establishing a change control process in the project.
- **Static application security testing:** Some degree of static AST (SAST) should be included at least for web applications. See "How to Deploy and Perform Application Security Testing" for full guidance on how to approach AST. Consider using Open Web Application Security Project (OWASP) as a framework for defining such tests. Introduce AST in any continuous integration/continuous development (CI/CD) pipeline using DevSecOps approaches.
- **Version control and repository governance:** As iterative versions of code are developed, control over the versioning can both prevent faults from slipping through quality gateways and improve quality in release management. Such control will also require a level of governance, including access control, logs and possibly workflow management, within source code repositories. See "Best Practices for Securing Continuous Delivery Systems and Artifacts."
- **Trusted components/framework security:** Evaluate and test the underlying frameworks and components used to build software. By using automated software composition analysis (SCA) tools to detect known vulnerabilities in open-source and third-party libraries, you can avoid common issues and alleviate some of the manual work. To help reduce code-based vulnerabilities, introduce governance for using third-party code, development frameworks, and even languages and integrated development environments (IDEs). Identify standard trusted components and approaches to address common services like IAM, encryption and key management. Application security teams should collaborate with development teams to identify and endorse trusted components that can be easily leveraged for actively developed applications, thus reducing unnecessary risk to the business.
- **Elective practices:**
  - *Dynamic application security testing (DAST):* Deploy limited DAST for specific use cases. Beyond basic QA and AST, a combination of both SAST and DAST is becoming a standard

practice. This combination both improves code coverage and increases the efficacy of application security testing. Results should be delivered through the standard issue management process.

- *Advanced structured development program:* Provide specific security training to application teams, backed up with extensive AST and incident data to demonstrate where bad things have happened. Highlight what the impact was to the organization and how to avoid such incidents in the future. Develop career paths for developers, and include security roles in development programs (including agile).

- *Secure SDLC:* For organizations repeatedly developing and evolving applications, a formal process for software development benefits functionality, reliability and security. It provides a higher level of QA in all areas, because development processes follow a mandated pathway.

- *Advanced trusted components and repositories:* Certain trusted components, such as those for encryption and key management, can be complex to introduce and maintain. Your roadmap should identify the basic trusted components that must be in place right away. Additional components will add value, but they will come at a cost of procurement, development, deployment or support, thus requiring further planning and budgeting. Introduce secure code repositories to further protect core code, builds and release cycles.

Application Security Operations

Regardless of how well they've been developed, applications need further protections upon deployment. These protections will normally be external to the application itself, whether its commercial off-the-shelf (COTS) or open-source software. These protections include:

- **Quality in infrastructure dependencies (priority):** Applications almost always depend on other parts of the infrastructure, including IAM, databases and encryption processes, for some security functions. Application owners should document what is required from the infrastructure to secure the application, giving particular attention to the delivery of such requirements.

- **Web application firewalls:** WAFs should be considered a basic practice, especially for protecting legacy environments or COTS applications, where source code may be unavailable. Even in cases where source code is available, it might be desirable to quickly create a virtual patch for a known web application vulnerability until a code-level fix can be created.

- **Access control:** If the application allows users differentiated levels of privilege based on their roles, take advantage of that capability. For applications known or planned to have sensitive data within them, make this differentiation capability a prerequisite as part of the design or procurement process. In general, the "principle of least privilege" should be applied to all components of an IT infrastructure to mitigate a variety of both accidental and malicious threats.

- **Logging:** Application and user behavior should be logged for debugging and investigative purposes. If a security information and event management (SIEM) tool is in place, then investigate the possibility of using that tool to detect the more obvious malicious events (see the Security Monitoring and Operations section).

- **Elective Practices:**

  - *Advanced web application protections:* Beyond the WAF, other protections may be needed. APIs can enable DDoS and other attacks from either human or automated "bot" attackers. Specific measures to mitigate these issues can be complicated and application-specific. However, for regulated data or applications that effectively *are* the business, these controls can be very important, even to business survival.

Data

The topic of data security — specifically, data-centric security planning and strategy — is gaining traction and importance. Overall, if you don't know what data you have, where it is or how it moves, then you will have a difficult time trying to secure the enterprise. Privacy regulations are increasingly stringent and are in place in many jurisdictions. Although good data security won't solve all privacy concerns, it remains a critical component of ensuring privacy.

Work with legal and other departments to build a basic privacy strategy, and identify a privacy officer who will take full ownership of the program's development.

The following are key data security practices:

- **Data security policy (priority):** A corporate policy for data classification and handling is fundamental. Implement at least one document that describes how sensitive data should be handled and what your organization expects from users to keep data safe. See the Governance and Risk Management section above for further information.

- **Data inventory and classification (priority):** Knowing what data you have and where it resides is crucial. Implement a manual process to identify where regulated data is stored and what kind of data it is. Often, getting to the point of having a reasonable data inventory will entail conducting some form of data discovery.

- **Database access control (priority):** Data in an organization has a life cycle, and the database often is involved very early in that life cycle. Security benefits disproportionately from being implemented early in any process, and improving the quality of database security can mitigate a variety of threats. Database access control should be implemented to limit each individual's capabilities to the extent reasonable within the bounds of business requirements.

- **Data backups (priority):** Systems and hardware can fail, and accidental deletions are not infrequent. Implement a backup solution that, at least, covers critical data, and test recovery on a regular basis. Data backups often form part of a disaster recovery plan.

- **Transport and full-disk encryption (FDE):** Encryption is not a panacea for data security, but it is important. By default, all sensitive data should be transferred over a connection secured with transport layer encryption (such as TLS 1.3). FDE protects data should the user device get lost or stolen, and it is available as part of most operating systems.

- **User gateway controls:** SEGs and SWGs mitigate threats against data, malware and phishing. Web gateway (proxy) solutions have been standard networking practice for many years, and recent developments for cloud-based solutions have reduced both implementation complexity and operational cost. A quick deployment can provide useful protection for common data elements, including personal data. SWG use is described in "Using Secure Web Gateway Technologies to Protect Users and Endpoints." SEGs can perform similar functions, but for the email route (see "How to Build an Effective Email Security Architecture" for further insight).

- **SaaS controls:** If you're using a cloud environment, then it will probably come with native security controls. Use them unless you have effective alternatives already available. They are often bundled with a subscription for the service, but even if there is an additional fee, they can be simpler to implement and maintain for a stretched organization. In the long term, you may continue to use them, or you may decide to implement a strategy that uses third parties to reduce security console overload.

- **Elective practices:**

  - *Other encryption:* Other forms of data encryption may also be appropriate for protecting your information assets. Some regulations, such as PCI DSS, even require certain subsets of data to be encrypted. Encryption tools should be used with care because they can cause an availability risk, and poorly managed encryption can provide much lower levels of security than anticipated. See "Understanding and Evaluating Cryptographic Systems: An Information Security Foundation" for more in-depth coverage of options for protecting data with encryption.

  - *Broader data loss protection:* DLP solutions are now mainstream and have demonstrated value in the enterprise, despite numerous examples of failed deployments. "Integrated DLP," as termed by Gartner, can be found in many places, including SWGs, CASBs and SaaS environments. Integrated DLP approaches are increasingly merging with traditional enterprise DLP systems. See "Building an Effective DLP Program" for further discussion of the use and selection of DLP controls.

  - *Classification and tagging tools:* Automated classification approaches provide insight and useful metadata for the wider data security problem. They support DLP, data governance and a variety of regulations (such as the EU General Data Protection Regulation [GDPR]). If you have a heavy regulatory burden, you may consider these tools a basic security control. However, the process of actually labeling datasets in production can be challenging outside of a few core file types. Given that the ability to identify and track data through its life cycle is an increasing requirement from regulations, however, we expect to see continued development and improvement of these tools. User-driven classification is an increasingly

capable tool that provides significant value to a variety of DLP approaches. Early adoption of this technology can pave the way for later introduction of DLP, as well as increase general security awareness.

- *Database audit and protection (DAP):* DAP is also considered as an elective practice, though it is more likely a step beyond the elective practices listed here. For more information, see "When to Use Database Audit and Protection to Enhance Database Security and Compliance."

Cloud

Cloud security is not a distinct security practice. All of the basic security practices described to this point, as well as IAM, apply to a cloud environment. However, the use of IaaS, PaaS, SaaS or any other form of cloud service requires slightly different solutions to what are similar problems. The cloud introduces the concept of the "shared responsibility" model, which highlights that cloud services prevent direct control of some elements of the IT stack and relevant controls. The approach to cloud security should be one of "clouds can be secure *if* we use them securely." See "How to Evaluate Cloud Service Provider Security" for a more extensive discussion of managing cloud security concerns. "Guide to Cloud Security Concepts" provides important background information about key issues in cloud security.

Cloud-specific security practices include the following:

- **Cloud access security brokers (priority):** Gartner considers CASBs a minimum requirement for cloud usage. The CASB provides a number of controls, including IAM, DLP, conditional access, cloud discovery and mobile management. CASB services allow those controls to be applied across multiple cloud environments. See "How to Secure Cloud Applications Using Cloud Access Security Brokers."

- **SaaS:** Implement IAM processes that include provisioning a unique (not shared) account for each user. Extend your on-premises user life cycle process to include the cloud, and ensure that changes and deprovisioning occur in a timely, accurate fashion. Be aware that some SaaS solutions create their own copy of identity information, and that without adequate user data orchestration, this duplication can lead to inconsistencies. Look to use single sign-on (SSO) solutions, and integrate IAM solutions with your identity ecosystem (e.g., Active Directory).

- **PaaS, database as a service (DBaaS) and equivalents:** The application security practices described in the Application Security Development section should be followed. For examples of cloud-specific implementations, see "Consuming DBaaS Securely: Comparing Options for Securing On-Premises and Cloud Databases."

- **IaaS:** Building on the requirements for SaaS and PaaS, add the server security and network security practices described throughout this document (including in the Endpoint Security section). In addition:

- Treat cloud workload protection platforms (CWPP) as a minimum requirement, providing system hardening and protection as well as network management capabilities. See "Improve Your Cloud Security With Cloud Workload Protection Platforms" for more detailed information.
- Use the native security controls provided by the IaaS environment, where appropriate. Note, however, that the IaaS providers implement controls to different degrees and in different ways. For examples, see "Guide to Cloud Security Concepts."

- **Basic awareness and insight into procurement processes:** Much of cloud security relies on legal support and on performing risk assessments that address the loss of direct control over some parts of the environment. Including security as a stakeholder in procurement processes is an important practice to help manage these concerns.
- **Elective practices:**
  - *Cloud security posture management:* Cloud is secure *if* you use it securely. A continuous stream of reports about breaches resulting from basic failures in security configuration in the cloud suggests that organizations still aren't doing so. CSPM tools will identify misconfigurations and other vulnerabilities in the use of cloud environments.
  - *Automated system configuration management*: Automated tools for building and maintaining systems to a known state are becoming standard and affordable. This is especially true as cloud services, virtualization and continuous deployment (DevOps) models become more prevalent. Controls like patch management can often benefit greatly from improvement in this practice area.

Security Monitoring and Operations

Security controls need administering, and their output needs monitoring, else incidents will not be detected and remediated. A fully developed security operations center (SOC) is not necessary for all organizations, and is out of the reach of many. However, the basic functionality should be in place for the process to be effective. *This practice does require that a human resource be available to act on the information, which can be a problem for some organizations.*

See "Security Operations for Technical Professionals Primer for 2020" and "How to Start Your Threat Detection and Response Practice" for more detailed insight and links to relevant research.

The following are best practices for security monitoring and operations:

- **Basic incident response management and after-action reporting (priority):** Define a basic incident response management process, test it, and refine it as necessary. Specialized skills are needed to develop a more specific process, and it is possible to obtain these skills through outsourcing. Investigate all incidents as a concluding part of the incident response process, in order to contribute to learning lessons and making improvements. "How to Implement a

Computer Security Incident Response Program" provides topical coverage and recommendations for incident response.

- **Basic log management (priority):** Implement a central repository for log retention to meet investigative and legal requirements, and support some sort of reporting or analysis. Be sure to consider service providers as a viable option to implement this practice. Log management capabilities can come as part of security incident and event monitoring (SIEM) tools, which are almost a basic requirement. If possible, use a SIEM from the outset, even if you don't take full advantage of its capabilities immediately.

- **Outsourcing options (MSSP and MDR):** The human resource requirement for security operations is a real issue for many organizations. Outsourcing is an option, and for organizations starting the security journey, limited security services from a provider can offer a very useful way of uplifting some security capabilities quickly and simply. These vary from monitoring-only services to fully supported deployment, monitoring and response capabilities. See "How to Work With an MSSP to Improve Security."

- **Operating metrics:** You need to know how installed security controls are performing. Targets, key performance indicators (KPIs) and metrics can be contentious issues, and this situation is no different for security operations. However, security tools provide useful information to inform risk assessments, and can be a vital part of the wider IT operation. Thus, such measurements are necessary. A base level of measurement, as well as ideas for evolving security controls, can be found in "Developing Metrics for Security Operational Performance."

- **Elective practices:**

  - *Full SIEM:* At some point, the controls you have implemented will be providing levels of information beyond the capability of any manual approach. The SIEM tool has become mainstream for many organizations because it enables and automates detection of many security incidents. Cloud-based SIEMs are available (as a service), as are managed SIEM services. These simplify the implementation and reduce the resource burden. See "How to Architect and Deploy a SIEM Solution" for further insight.

  - *Security orchestration, automation and response (SOAR):* The more security controls you have, the more burden is placed on the operations part of the process — i.e., implementing, monitoring and responding. Automation becomes necessary for both efficiency and effectiveness, especially in large environments. Use SOAR tools to support teams with limited resources in relation to the workload they face. See "SOAR: Assessing Readiness Through Use-Case Analysis" for further insight.

Identity and Access Management

No enterprise functions without at least a small amount of IAM. Access management ensures that only authorized and authenticated entities can perform approved actions on systems or data. IAM defines the structure and tools to provide the authorization and authentication. An entity can be a human, an application or a device. Digital entities require IAM controls as much as humans,

although some of the governance practices will differ. See "Identity and Access Management for Technical Professionals Primer for 2020" for detailed insight.

Controls for IAM include:

- **Centralized user directory:** The foundational practice of identity and HR management provides the list of people, their roles and attributes. That information needs to be translated into an access and authorization directory. Having a single directory simplifies IAM functionality, reduces risk, and also standardizes IAM processes for application and system owners. Require all systems and applications to use the centralized system for authentication. The centralized directory can be used for the entire workforce, not just direct employees. However, separate groups and user constituencies within the directory (e.g., by using organizational units in an Active Directory). This segregation helps other access control systems be more effective. Segregation is especially important with regard to consumer customers; implement a separate directory environment for this community.
- **Standardize account life cycle management:** Each entity (human or digital) has a life cycle that can be characterized as "joiner, mover, leaver." Developing standards and processes for what should happen at each phase of the life cycle reduces errors, holdover privileges and insider threats, and it is indeed required by some regulations. Implement standard processes for:
  - Account provisioning at commencement of the life cycle (starter).
  - Periodic validation of the account against workforce management.
  - Periodic validation of access rights (also known as access certifications) by system and application owners. Keep records of such reviews for audit purposes.
  - Modification of access rights to reflect new requirements when a role changes (mover), and removal of rights that are no longer required.
  - Disabling of the account when the user leaves, or when the digital entity is no longer operational (leaver).
  - Removal of the account after cleanup and data recovery actions are complete.
- **Authorization and reviews:** Implement a formal authorization process for access requests that separates requester and authorizer roles. Keep records of authorization approvals for audit purposes. Require periodic review of all access rights. The cadence should be monthly or quarterly, depending on the level of account privilege.
- **Role-based access control (RBAC):** Provide access rights based on the user's role, rather than rebuilding each person's authorizations individually. RBAC introduces standardization and reduces the overhead of provisioning and maintaining accounts, including supporting default authorization. Reflecting standard authorizations through group membership also supports

periodic review and simplifies configuration and management of access (such as on a file share).

- **Authentication:** Various methods exist for proving that entities are who/what they claim to be, which is the process of authentication. Implement a standard for password length and complexity, along with policies to prevent reuse, sharing and disclosure. Longer, simpler passwords are better than shorter, complex passwords. Passwords remain a security risk for most use cases. Therefore, use multifactor authentication (MFA) for, at least, privileged accounts and remote access, with a plan to expand its scope. See "Guidance for Selecting User Authentication Solutions" for detailed insight.

- **Privileged access management:** Some users and entities have higher-level privileges. Examples include system and database administrators, domain administrators, network administrators, application support, and customer support. Those privileged accounts should be a particular focus for control, because the risk of abuse of those privileges (malicious or otherwise) is high. Basic privileged access management approaches include implementing stronger governance of RBAC, enforcing the use of secondary accounts, and limiting the use of generic accounts (accounts not attributable to a specific user). Use logging to record activities that privileged accounts are performing. More advanced approaches are mentioned in the elective practices (below).

- **Elective practices:**

  - *Automated account provisioning:* Automating the link between the workforce management system and the identity directory (such as Microsoft Active Directory) supports faster and more robust standard provisioning, deprovisioning and change processes. Disabling a terminated employee's account should happen in minutes rather than days, and automated approaches allow for that kind of activity.

  - *Enhanced RBAC:* Attribute-based access control (ABAC) uses a wider variety of attributes to control the access an entity might have, and is often implemented to support dynamic access control. For example, users located in the main office may be granted greater access rights than if they were located in a foreign country.

  - *Enhanced governance:* Use analytics and information from the IAM systems' log files and user directories to further automate governance processes, such as access certification and access request. Next-generation identity governance and administration systems leveraging advanced analytics can both reduce administrative effort and increase compliance. See "Modernizing IGA Architecture for the Digital Enterprise."

  - *Enhanced privileged access management:* Specific tools exist to provide much higher levels of privileged access management, including password vaulting, session recording and workflow management. These systems can be complex to implement, but provide more robust control than the basic level of privileged access management. Also, such tools can provide methods for managing application (digital entity) accounts, eliminating the need to

embed passwords in scripts and removing the risk of humans using digital entity accounts. See "Guidance for Privileged Access Management."

- *Federated IAM and single sign-on (SSO)*: Organizations may wish to enhance their IAM capabilities by deploying a solution that readily integrates with cloud service providers and existing IAM systems. Such a deployment usually includes federated identity to enable cross-domain SSO. Federated IAM is considered an elective practice today because deployment involves additional expense and effort. The widespread availability of IAM-as-a-service offerings that include out-of-the-box connectors to the most popular SaaS applications is leading to increased adoption.

- *Adaptive access:* A number of approaches can enhance the authentication and access control process. Adaptive access (aka context-based authentication) is one such approach that evaluates multiple attributes about the authentication request. These attributes can include IP address, geolocation, geovelocity, device fingerprint, and the previous behavior of the user or device. Once the context is known, adaptive access can then mitigate risk by blocking or reducing access, initiating extra monitoring, or increasing authentication requirements. As security threats increase and MFA becomes less expensive and easier to use, the trend is to deploy MFA for a wider scope of users. Over time, expect adaptive access to evolve from being an elective feature to being a basic control.

- *Passwordless authentication:* Passwords are a notorious weak point, whether they are simple or complex. Passwordless authentication is a growing trend that is easily implemented under some circumstances and that provides significant risk management. See "Guidance for Selecting User Authentication Solutions."

- *Enhanced API life cycle management:* When organizations develop APIs, they need specialized controls to protect these APIs. API gateways — the runtime protection part of a full API life cycle management solution — can be used in conjunction with other IAM and security tools to mediate access to APIs. See "A Guidance Framework for Evaluating API Management Solutions."

- *Specialized IAM for customers:* Organizations with consumer-facing systems need IAM tools designed to meet the needs of consumer relationships. Examples of these tools include self-service registration, identity proofing, and consent and preference management. See "Key Features for Customer Identity and Access Management."

Note 1: Supplemental Gartner Research

Table 2 provides a comprehensive, but not exhaustive, list of supplemental Gartner research on the topics covered in this document.

Table 2: Supplemental Gartner Research, by Topic

Topic ↓	*Supplemental Gartner Research* ↓

Topic	*Supplemental Gartner Research*
General	■ “2020 Planning Guide for Security and Risk Management” ■ “2020 Planning Guide for Identity and Access Management”
Foundational Practices	■ “How to Modernize the Configuration Management Database” ■ “How to Implement a Modern IT Change Management Practice” ■ “A Guidance Framework for Establishing Your Approach to Security Architecture” ■ “5 Ways EA Can Help the Organization Focus on Security” ■ “Direct Material Sourcing and Supply Chain Services Primer for 2020”

Topic	*Supplemental Gartner Research*
Governance and Risk Management	■ “Creating Security Standards: Context, Structure and Must-Have Content” ■ “Effective Risk Communication for the IT Professional” ■ “Research Roundup for Creating Information Security Policy” ■ “Toolkit: Security Policy Exception” ■ “How to Design a Security Champion Program” ■ “Use a Structured Approach to Communicate Your Security Strategy” ■ “Security Governance, Management and Operations Are Not the Same” ■ “Security Fundamentals — The Services and Processes You Must Get Right” ■ “A Guidance Framework for Developing and Implementing Vulnerability Management” ■ “Using Penetration Testing and Red Teams to Assess and Improve Security” ■ “Best Practices for Managing and Governing Third-Party Identities, Including Contractors and Business Partners” ■ “Guidance for Privileged Access Management” ■ “Data Center Infrastructure for Technical Professionals Primer for 2020” ■ “Best Practices in Disaster Recovery” ■ “Designing a Disaster Recovery Plan Document” ■ “The Future of Network Security Is in the Cloud” ■ “OT Security Best Practices” ■ “A Comparison of Remote Network Access Products for Enterprise Endpoints” ■ “Decision Point for Postmodern Security Zones” ■ “Guidance Framework for Implementing Network Access Control” ■ “DDoS: A Comparison of Defense Approaches”

Topic	*Supplemental Gartner Research*
Endpoint and Mobile Security	■ "Comparing Techniques for Endpoint Protection" ■ "Solution Criteria for Endpoint Protection Platforms" ■ "Comparing Options for User Endpoint and Mobile Device Encryption" ■ "How to Plan, Implement and Operate a Successful Application Whitelisting Deployment" ■ "Advance and Improve Your Mobile Security Strategy" ■ "Creating, Implementing and Measuring an Effective BYOD Program" ■ "Comparison of Mobile Threat Defense Solutions" ■ "Mobile OSs and Device Security: A Comparison of Platforms"
Application Security	■ "A Guidance Framework for Establishing and Maturing an Application Security Program" ■ "How to Deploy and Perform Application Security Testing" ■ "Structuring Application Security Practices and Tools to Support DevOps and DevSecOps" ■ "12 Things to Get Right for Successful DevSecOps" ■ "Best Practices for Securing Continuous Delivery Systems and Artifacts" ■ "Modern Identity and APIs: OpenID Connect, OAuth 2.0 and SCIM 2.0" ■ "DDoS: A Comparison of Defense Approaches" ■ "Solution Path for Forming an API Security Strategy" ■ "Protecting Web Applications and APIs From Exploits and Abuse"

Topic	*Supplemental Gartner Research*
Data Security	■ “Building an Effective DLP Program” ■ “How to Successfully Design and Implement a Data-Centric Security Architecture” ■ “Build Once, Use Many Times: Use Privacy Engineering to Support a Data-Centric Security Architecture” ■ “Use the Data Security Governance Framework to Balance Business Needs and Risks” ■ “Improving Data Security Governance Using Classification Tools” ■ “Consuming DBaaS Securely: Comparing Options for Securing On-Premises and Cloud Databases” ■ “How to Select the Right Email Encryption Solution” ■ “Understanding and Evaluating Cryptographic Systems: An Information Security Foundation” ■ “When to Use Database Audit and Protection to Enhance Database Security and Compliance”
Cloud Security	■ “Guide to Cloud Security Concepts” ■ “How to Secure Cloud Applications Using Cloud Access Security Brokers” ■ “Consuming DBaaS Securely: Comparing Options for Securing On-Premises and Cloud Databases” ■ “Containers: 11 Threats and How to Control Them” ■ “Improve Your Cloud Security With Cloud Workload Protection Platforms” ■ “Enabling High-Risk Services in the Public Cloud With IaaS Encryption”
Security Monitoring and Operations	■ “Security Operations for Technical Professionals Primer for 2020” ■ “The Managed Security Services Landscape Is Changing” ■ “How to Work With an MSSP to Improve Security” ■ “Solution Path for Implementing Threat Detection and Incident Response” ■ “Developing Metrics for Security Operational Performance” ■ “How to Implement a Computer Security Incident Response Program”

Topic	*Supplemental Gartner Research*
Identity and Access Management	■ "Identity and Access Management for Technical Professionals Primer for 2020" ■ "Architecting an Agile and Modern Identity Infrastructure" ■ "Is Passwordless Authentication Ready for the Enterprise?" ■ "A Guidance Framework for Deploying PKI" ■ "Eight Ways CASBs Improve Your IAM Security Posture" ■ "Guidance for Privileged Access Management" ■ "IGA, RPA, and Managing Software Robot Identities"

Source: Gartner (June 2020)

Document Revision History

Building the Foundations for Effective Security Hygiene - 8 August 2018

Strengthen Basic Security Hygiene With a Two-Pronged Security Architecture Approach - 5 March 2015

Recommended by the Author

2020 Planning Guide for Security and Risk Management

2020 Planning Guide for Identity and Access Management

A Guidance Framework for Establishing Your Approach to Security Architecture

Creating Security Standards: Context, Structure and Must-Have Content

Comparing Techniques for Endpoint Protection

Advance and Improve Your Mobile Security Strategy

A Guidance Framework for Establishing and Maturing an Application Security Program

Building an Effective DLP Program

How to Successfully Design and Implement a Data-Centric Security Architecture

Guide to Cloud Security Concepts

Security Operations for Technical Professionals Primer for 2020

Developing Metrics for Security Operational Performance

Identity and Access Management for Technical Professionals Primer for 2020

Architecting an Agile and Modern Identity Infrastructure

Recommended For You

Security Frameworks: The What and Why, and How to Select Yours

Security Operations for Technical Professionals Primer for 2020

Security and Risk Management Programs for Technical Professionals Primer for 2020

Creating Security Standards: Context, Structure and Must-Have Content

Improve Your Security With Security Architecture