**Final Generated Answers Statistics**

* The following table contains the FAQ question, retrieved question-answer pair, final generated answer by the application, and the accuracy.
* The accuracy column shows if the final generated answer by the application is the same answer, for the question, as in the PDF documents.
* After retrieving the FAQ pair from the vector database, the answer is passed to the GPT-4o model for refinement in order to remove grammatical mistakes(occured through parsing). After refinement the final answer is displayed on the application.
* The following table starts with questions from the Nist document in numerical order and then is followed by questions from the Windows document in numerical order
* Out of 73 questions, 71 questions are shown to be accurate and the same as present in the PDF document. As a result the final accuracy of the application for the 73 questions is 97 percent.

| **Question** | **Retrieved FAQ Pair** | **Final Generated Answer after refinement by GPT 4o** | **Accuracy** |
| --- | --- | --- | --- |
| What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Categorize step? | 1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Categorize step?  Answer: The following modifications have been made from NIST SP 800-37, Revision 1 [SP 800-37r1], to NIST SP 800-37, Revision 2 [SP 800-37r2], in the Categorize step:  · The System Registration task was moved to the Prepare step (Task P-18) to allow organizations to announce the existence of the system to the organization, add the system to the organizational system inventory, and explicitly announce implications to the organization's security and privacy programs from the creation of the system.  · The Security Categorization Review and Approval (Task C-2) task was added to ensure that the authorizing official reviews and approves the security categorization results to confirm that the security category selected for the system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions.  · Elements of privacy and roles for systems that process personally identifiable information were added to this publication as a direct response to OMB Circular A-130 [OMB A130], which requires agencies to implement the Risk Management Framework (RMF) and integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. 「Back to Table of Contents] | The following modifications have been made from NIST SP 800-37, Revision 1 [SP 800-37r1], to NIST SP 800-37, Revision 2 [SP 800-37r2], in the Categorize step:  - The System Registration task was moved to the Prepare step (Task P-18) to allow organizations to announce the existence of the system to the organization, add the system to the organizational system inventory, and explicitly announce implications to the organization's security and privacy programs from the creation of the system.  - The Security Categorization Review and Approval (Task C-2) task was added to ensure that the authorizing official reviews and approves the security categorization results to confirm that the security category selected for the system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions.  - Elements of privacy and roles for systems that process personally identifiable information were added to this publication as a direct response to OMB Circular A-130 [OMB A130], which requires agencies to implement the Risk Management Framework (RMF) and integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. | Accurate |
| What is security categorization and why is it important? | 2. What is security categorization and why is it important?  Answer: Security categorization provides a structured way to determine the criticality of the information being processed, stored, and transmitted by a system. The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization. The categorization determination results in the security category for the system, which is based on the potential adverse impact (worst case) to an organization should events occur that jeopardize the information and systems needed by the organization to accomplish its assigned mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day- to-day functions. Before a security categorization decision can be made, the identification of the types of information that are or will be processed, stored, and transmitted by the system needs to be performed in the Prepare step (Task P-12, Information Types). Similarly, in addition to identifying the information types, each stage in the information life cycle for each type identified also needs to be identified and understood. This is also addressed in the Prepare step (Task P-13, Information Life Cycle).  The information owner or system owner identifies the types of information processed, stored, and transmitted by the system as part of Prepare step Task P-12 and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type as part of Categorize step Task C-2. The high watermark concept is used to determine the security impact level of the system for the express purpose of prioritizing information security efforts among systems and selecting an initial set of controls from one of the three control baselines in NIST SP 800-53B [SP 800-53B]. According to the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization for Federal Information and Information Systems [FIPS 199], security categorization promotes effective management and oversight of information security programs, including the coordination of information security efforts across the Federal Government, and reporting on the adequacy and effectiveness of information security policies, procedures, and practices. [Back to Table of Contents] | Security categorization provides a structured way to determine the criticality of the information being processed, stored, and transmitted by a system. The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization. The categorization determination results in the security category for the system, which is based on the potential adverse impact (worst case) to an organization should events occur that jeopardize the information and systems needed by the organization to accomplish its assigned mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions. Before a security categorization decision can be made, the identification of the types of information that are or will be processed, stored, and transmitted by the system needs to be performed in the Prepare step (Task P-12, Information Types). Similarly, in addition to identifying the information types, each stage in the information life cycle for each type identified also needs to be identified and understood. This is also addressed in the Prepare step (Task P-13, Information Life Cycle).  The information owner or system owner identifies the types of information processed, stored, and transmitted by the system as part of Prepare step Task P-12 and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type as part of Categorize step Task C-2. The high watermark concept is used to determine the security impact level of the system for the express purpose of prioritizing information security efforts among systems and selecting an initial set of controls from one of the three control baselines in NIST SP 800-53B [SP 800-53B]. According to the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization for Federal Information and Information Systems [FIPS 199], security categorization promotes effective management and oversight of information security programs, including the coordination of information security efforts across the Federal Government, and reporting on the adequacy and effectiveness of information security policies, procedures, and practices. | Accurate |
| How is the categorization decision used? | 3. How is the categorization decision used?  Answer: The categorization decision is used to support the next step in the Risk Management Framework: the Select step. It informs all subsequent risk management decisions regarding the security of the system. This includes baseline and control selection and documentation level of effort, implementation details, assessment level of effort, authorization decisions, continuous monitoring frequencies and level of effort, checks and balances for the initial risk assessment, and ongoing risk assessment. Once the overall security impact level of the system is determined (i.e., after the system is categorized), an initial set of controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53B [SP 800-53B]. Organizations have the flexibility to adjust the control baselines following the tailoring guidance defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). The security category and system security impact level are also used to determine the level of detail to include in security documentation, such as plans, procedures, and the level of effort needed to assess the system. [Back to Table of Contents] | The categorization decision is used to support the next step in the Risk Management Framework: the Select step. It informs all subsequent risk management decisions regarding the security of the system. This includes baseline and control selection and documentation level of effort, implementation details, assessment level of effort, authorization decisions, continuous monitoring frequencies and level of effort, checks and balances for the initial risk assessment, and ongoing risk assessment. Once the overall security impact level of the system is determined (i.e., after the system is categorized), an initial set of controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53B [SP 800-53B]. Organizations have the flexibility to adjust the control baselines following the tailoring guidance defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). The security category and system security impact level are also used to determine the level of detail to include in security documentation, such as plans, procedures, and the level of effort needed to assess the system. | Accurate |
| Who is responsible for categorizing each system? | 4. Who is responsible for categorizing each system?  Answer: Ultimately, the information owner/system owner or an individual designated by the owner is responsible for categorizing a system. The information owner/system owner identifies all the information types stored in, processed by, or transmitted by the system as part of Prepare step Task P-12 and then determines the security category for the system by identifying the highest value (i.e., high water mark) for each security objective (confidentiality, integrity, and availability) and for each type ofinformation resident on the system as part of Categorize step Task C-2. Subject matter experts may also be tapped by the information owner/system owner to assist with the system security categorization efforts. For systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.  While the primary responsibility for categorization belongs to information owner/system owner, security categorizations are conducted as an organization-wide activity with the involvement of senior leadership (e.g., risk executive [function]) and system staff  (e.g., system security officer and system privacy officer when PII is being processed). The authorizing official or designated representative reviews the categorization results and decisions from other organizational systems and then collaborates with senior leaders to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets. Senior leadership participation in the security categorization process is essential so that the Risk Management Framework can be carried out in an effective and consistent manner throughout the organization. The authorizing official or designated representative reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. Back to Table of Contents] | Ultimately, the information owner/system owner or an individual designated by the owner is responsible for categorizing a system. The information owner/system owner identifies all the information types stored in, processed by, or transmitted by the system as part of Prepare step Task P-12 and then determines the security category for the system by identifying the highest value (i.e., high water mark) for each security objective (confidentiality, integrity, and availability) and for each type of information resident on the system as part of Categorize step Task C-2. Subject matter experts may also be tapped by the information owner/system owner to assist with the system security categorization efforts. For systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.  While the primary responsibility for categorization belongs to information owner/system owner, security categorizations are conducted as an organization-wide activity with the involvement of senior leadership (e.g., risk executive [function]) and system staff (e.g., system security officer and system privacy officer when PII is being processed). The authorizing official or designated representative reviews the categorization results and decisions from other organizational systems and then collaborates with senior leaders to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets. Senior leadership participation in the security categorization process is essential so that the Risk Management Framework can be carried out in an effective and consistent manner throughout the organization. The authorizing official or designated representative reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. | Accurate |
| What is the role of privacy in the categorization process? | 5. What is the role of privacy in the categorization process?  Answer: Privacy programs are responsible for managing the risks to individuals associated with the processing of personally identifiable information (PII) and for ensuring compliance with applicable privacy requirements. When a system processes PII, the information security program and the privacy program have a shared responsibility for managing the security risks for the PII in the system. Informed by the privacy risk assessment conducted under the Prepare step (Task P-14, Risk Assessment - System), the privacy program and the security program collaborate on determining the security category and overall security impact level for the system. The senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review. | Privacy programs are responsible for managing the risks to individuals associated with the processing of personally identifiable information (PII) and for ensuring compliance with applicable privacy requirements. When a system processes PII, the information security program and the privacy program have a shared responsibility for managing the security risks for the PII in the system. Informed by the privacy risk assessment conducted under the Prepare step (Task P-14, Risk Assessment - System), the privacy program and the security program collaborate on determining the security category and overall security impact level for the system. The senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review. | Accurate |
| What is the relationship between categorization and the organization's enterprise architecture? | 6. What is the relationship between categorization and the organization's enterprise architecture?  Answer: The information types enumerated in NIST SP 800-60, Volume II [SP 800-60v2], are based on OMB's Business Reference Model (BRM) [OMB BRM], as described in the Federal Enterprise Architecture Consolidated Reference Model Document. The BRM provides a framework that facilitates a functional (rather than organizational) view of the Federal Government's lines of business, including its internal operations and its services for citizens, independent of the organizations performing them. [Back to Table of Contents] | The information types enumerated in NIST SP 800-60, Volume II [SP 800-60v2], are based on OMB's Business Reference Model (BRM) [OMB BRM], as described in the Federal Enterprise Architecture Consolidated Reference Model Document. The BRM provides a framework that facilitates a functional (rather than organizational) view of the Federal Government's lines of business, including its internal operations and its services for citizens, independent of the organizations performing them. | Accurate |
| What is the role of the risk executive (function) in the categorization process? | 7. What is the role of the risk executive (function) in the categorization process?  Answer: The risk executive (function) may not necessarily be the responsibility of a single person. It could be the responsibility of a group, committee, or any entity as defined by the organization. This function helps ensure that information security considerations for individual systems are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business processes.  During the categorization process, the risk executive (function) provides the senior leadership with input and oversight to help ensure that consistent categorization decisions are made for individual systems across the organization. The risk executive (function) facilitates the sharing of security-related and risk-related information among senior leaders to help ensure that all types of risk that may affect mission and business success and the overall interests of the organization at large are considered. Back to Table of Contents] | The risk executive (function) may not necessarily be the responsibility of a single person. It could be the responsibility of a group, committee, or any entity as defined by the organization. This function helps ensure that information security considerations for individual systems are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business processes.  During the categorization process, the risk executive (function) provides the senior leadership with input and oversight to help ensure that consistent categorization decisions are made for individual systems across the organization. The risk executive (function) facilitates the sharing of security-related and risk-related information among senior leaders to help ensure that all types of risk that may affect mission and business success and the overall interests of the organization at large are considered. | Accurate |
| During which phase of the system development life cycle is a new system categorized? | 8. During which phase of the system development life cycle is a new system categorized?  Answer: The initial security categorization for the information and the system is performed during the initiation phase of the system development life cycle along with an initial security risk assessment. The initial risk assessment defines the threat environment in which the system operates and includes an initial description of the basic security needs of the system. These needs are contingent upon an understanding of how a possible loss of confidentiality, integrity, or availability ofinformation of a system component can impact the organization and the resulting security categorization. For more details on security categorization, see Federal Information  Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. FIPS 199]  Once the system is operational, the organization revisits the risk management activities described in the Risk Management Framework, including the system categorization, on a regular basis. Additionally, events can trigger an immediate need to assess the security state of the system. If a security event occurs, the organization may reexamine the security category and impact level of the system to confirm the criticality of the system in supporting its mission operations or business case. The resulting impact on organizational operations and assets, individuals, other organizations, or the Nation may provide new insights regarding the overall importance of the system in assisting the organization to fulfill its mission responsibilities. Back to Table of Contents | The initial security categorization for the information and the system is performed during the initiation phase of the system development life cycle along with an initial security risk assessment. The initial risk assessment defines the threat environment in which the system operates and includes an initial description of the basic security needs of the system. These needs are contingent upon an understanding of how a possible loss of confidentiality, integrity, or availability of information of a system component can impact the organization and the resulting security categorization. For more details on security categorization, see Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.  Once the system is operational, the organization revisits the risk management activities described in the Risk Management Framework, including the system categorization, on a regular basis. Additionally, events can trigger an immediate need to assess the security state of the system. If a security event occurs, the organization may reexamine the security category and impact level of the system to confirm the criticality of the system in supporting its mission operations or business case. The resulting impact on organizational operations and assets, individuals, other organizations, or the Nation may provide new insights regarding the overall importance of the system in assisting the organization to fulfill its mission responsibilities. | Accurate |
| How does the use of external system services impact system categorization? | 9. How does the use of external system services impact system categorization?  Answer: The security categorization process assists a system or organization in assessing the impact of the loss of information confidentiality, integrity, or availability and helps define the necessary protection (controls) to reduce the likelihood of such losses. The organization then proceeds to the subsequent steps in the RMF until the system is authorized and continuously monitored. However, when using external system services (i.e., services that are implemented outside of the system's authorization boundary and are not part of the organization's systems), the organization typically has no direct control over the application of required controls or the assessment of control effectiveness. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of system security. These challenges include (i) defining the types of external services provided to the organization, (ii) describing how the external services are protected in accordance with the security and privacy requirements of the organization, and (iii) obtaining the necessary assurances that the risk to the organization's operations and assets and to individuals arising from the use of the external services is at an acceptable level. For example, the security categorization of cloud-based services that are identified and provided as part of their Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP] authorization is reviewed along with the potential impacts, if any, to the organization utilizing these external system services. [Back to Table of Contents | The security categorization process assists a system or organization in assessing the impact of the loss of information confidentiality, integrity, or availability and helps define the necessary protection (controls) to reduce the likelihood of such losses. The organization then proceeds to the subsequent steps in the RMF until the system is authorized and continuously monitored. However, when using external system services (i.e., services that are implemented outside of the system's authorization boundary and are not part of the organization's systems), the organization typically has no direct control over the application of required controls or the assessment of control effectiveness. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of system security. These challenges include  - (i) defining the types of external services provided to the organization,  - (ii) describing how the external services are protected in accordance with the security and privacy requirements of the organization, and  - (iii) obtaining the necessary assurances that the risk to the organization's operations and assets and to individuals arising from the use of the external services is at an acceptable level.  For example, the security categorization of cloud-based services that are identified and provided as part of their Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP] authorization is reviewed along with the potential impacts, if any, to the organization utilizing these external system services. | Accurate |
| How does the categorization decision affect external system services? | 10. How does the categorization decision affect external system services?  Answer: Categorizing external systems and the organizational information processed, stored, and transmitted by external system services provides the necessary information to determine the security and privacy requirements that the service provider is required to meet and the evidence that they are required to provide to achieve assurance that the external services are operating at an acceptable security level. For example, if a system is categorized as a high impact system, and if the external system is categorized as a moderate impact system, then the organization needs to understand what the security implications are regarding the utilization of the external system services/resources. Thus, the security categorization of the organization acquiring external system services may influence or determine requirements for utilizing such services.  The level of control over an external system is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services). In other cases, a level of trust in the external system service is derived from other factors that convince the authorizing official that the requisite controls have been employed and that a credible determination of control effectiveness exists in the external system.  Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider - not due to any inherent untrustworthiness on the provider's part,  but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services or service providers, the organization employs compensating controls or usage restrictions or accepts the greater degree of risk to its operations, assets, and individuals. 「Back to Table of Contents] | Categorizing external systems and the organizational information processed, stored, and transmitted by external system services provides the necessary information to determine the security and privacy requirements that the service provider is required to meet and the evidence that they are required to provide to achieve assurance that the external services are operating at an acceptable security level. For example, if a system is categorized as a high impact system, and if the external system is categorized as a moderate impact system, then the organization needs to understand what the security implications are regarding the utilization of the external system services/resources. Thus, the security categorization of the organization acquiring external system services may influence or determine requirements for utilizing such services.  The level of control over an external system is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services). In other cases, a level of trust in the external system service is derived from other factors that convince the authorizing official that the requisite controls have been employed and that a credible determination of control effectiveness exists in the external system.  Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider - not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services or service providers, the organization employs compensating controls or usage restrictions or accepts the greater degree of risk to its operations, assets, and individuals. | Accurate |
| What is the difference between a security category and a security impact level? | 11. What is the difference between a security category and a security impact level?  Answer: Security category is the characterization of information or a system based on an assessment of the potential impact to organizational operations and assets, individuals, other organizations, or the Nation should there be a loss in confidentiality, integrity, or availability (security objectives) of such information or system. Note that an information type has a security category with three components - one for each security objective (i.e., confidentiality, integrity, or availability).  Security impact level consists of a single component with the value of low, moderate, or high. The security impact level for a system is determined by taking the maximum impact value of the system's security category - that is, the highest level ("high watermark") of the three security objectives for each information type and security category.  Table 1 Key terms  Key terms related to security are outlined with specific focus on objectives, categories, and impact levels. Security objectives include confidentiality, integrity, and availability, which are essential for protecting information and systems. Confidentiality ensures that information is accessible only to those authorized to view it. Integrity involves maintaining the accuracy and completeness of data, while availability ensures that information and resources are accessible when needed.  Security categories are defined as low, moderate, or high, and these apply to each of the security objectives. This categorization helps in assessing the level of protection required for different types of information and systems based on their sensitivity and importance.  Security impact levels are also classified as low, moderate, or high. These levels indicate the potential impact on an organization if a security breach occurs, guiding the implementation of appropriate security measures to mitigate risks.  For example, in Table 2 below (extracted from Table C-2, Type-based Impacts for Federal Information and Information Systems, in NIST SP 800-60, Volume 2, Guide for Mapping Types of Information and Information Systems to Security Categories [SP 800- 60v2]), there is an information type ("C.3.5.8 System and Network Monitoring") with a Moderate confidentiality impact level, a Moderate integrity impact level, and a Low availability impact level:  Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)} 1  Table 2 Sample security category  In the context of security categorization for management and support information, the focus is on three key aspects: confidentiality, integrity, and availability. For the category C.3.5 Information and Technology Management, specifically C.3.5.8 System and Network Monitoring, confidentiality and integrity are both rated as moderate. This indicates that the protection of sensitive information and the accuracy and trustworthiness of the data are of moderate importance. On the other hand, availability is rated as low, suggesting that while it is important for the system and network monitoring information to be accessible, it is not as critical as the other two aspects. This prioritization helps in allocating resources and implementing security measures effectively.  For illustration purposes, the security category for the information or system is Moderate (the high watermark between Moderate- Moderate-Low).  While the system's security impact level is used to look up the corresponding control baseline (low, moderate, or high) in NIST SP 800-53B [SP 800-53B], the system's security category (e.g., the specific impact value for each of the three security objectives:  1 See How is the security category expressed? question and answer for expanded description.  confidentiality, integrity, and availability) is considered when adjusting the system's controls, as defined in NIST SP 800-53 [SP 800- 53r5]. [Back to Table of Contents] | Security category is the characterization of information or a system based on an assessment of the potential impact to organizational operations and assets, individuals, other organizations, or the Nation should there be a loss in confidentiality, integrity, or availability (security objectives) of such information or system. Note that an information type has a security category with three components - one for each security objective (i.e., confidentiality, integrity, or availability).  Security impact level consists of a single component with the value of low, moderate, or high. The security impact level for a system is determined by taking the maximum impact value of the system's security category - that is, the highest level ("high watermark") of the three security objectives for each information type and security category.  Table 1 Key terms  Key terms related to security are outlined with specific focus on objectives, categories, and impact levels. Security objectives include confidentiality, integrity, and availability, which are essential for protecting information and systems. Confidentiality ensures that information is accessible only to those authorized to view it. Integrity involves maintaining the accuracy and completeness of data, while availability ensures that information and resources are accessible when needed.  Security categories are defined as low, moderate, or high, and these apply to each of the security objectives. This categorization helps in assessing the level of protection required for different types of information and systems based on their sensitivity and importance.  Security impact levels are also classified as low, moderate, or high. These levels indicate the potential impact on an organization if a security breach occurs, guiding the implementation of appropriate security measures to mitigate risks.  For example, in Table 2 below (extracted from Table C-2, Type-based Impacts for Federal Information and Information Systems, in NIST SP 800-60, Volume 2, Guide for Mapping Types of Information and Information Systems to Security Categories [SP 800-60v2]), there is an information type ("C.3.5.8 System and Network Monitoring") with a Moderate confidentiality impact level, a Moderate integrity impact level, and a Low availability impact level:  - Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}  Table 2 Sample security category  In the context of security categorization for management and support information, the focus is on three key aspects: confidentiality, integrity, and availability. For the category C.3.5 Information and Technology Management, specifically C.3.5.8 System and Network Monitoring, confidentiality and integrity are both rated as moderate. This indicates that the protection of sensitive information and the accuracy and trustworthiness of the data are of moderate importance. On the other hand, availability is rated as low, suggesting that while it is important for the system and network monitoring information to be accessible, it is not as critical as the other two aspects. This prioritization helps in allocating resources and implementing security measures effectively.  For illustration purposes, the security category for the information or system is Moderate (the high watermark between Moderate-Moderate-Low).  While the system's security impact level is used to look up the corresponding control baseline (low, moderate, or high) in NIST SP 800-53B [SP 800-53B], the system's security category (e.g., the specific impact value for each of the three security objectives:  - confidentiality  - integrity  - availability  is considered when adjusting the system's controls, as defined in NIST SP 800-53 [SP 800-53r5]. | Accurate |
| How is the security category expressed? | 12. How is the security category expressed?  Answer: The generalized format for expressing the security category, SC, of an information type is:  SC information type {(confidentiality, impact), (integrity, impact), (availability, impact)}, =  where the acceptable values for potential impact are low, moderate, high, or not applicable. The potential impact value of not applicable only applies to the security objective of confidentiality. For example, a security category for an information type that processes routine administrative information (non-PII) can be denoted as:  SC administrative information = {(confidentiality, low), (integrity, low), (availability, low)}.  The generalized format for expressing the security category, SC, of a system is similar:  SC = {(confidentiality, impact), (integrity, impact), (availability, impact)}, system  where the acceptable values for potential impact are low, moderate, or high. The potential impact values assigned to the respective security objective (confidentiality, integrity, and availability) are the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the system. The value of not applicable cannot be assigned to any security objective in the context of establishing a security category for a system. For example, a system that processes some information with a potential impact from a loss of confidentiality at moderate, some information with a potential impact from a loss of integrity at moderate, and all the information with a potential impact from a loss of availability at low, may have a security category expressed as:  SC = {(confidentiality, moderate), (integrity, moderate), (availability, low)} [Back to Table of Contents] system | The generalized format for expressing the security category, SC, of an information type is:  SC information type {(confidentiality, impact), (integrity, impact), (availability, impact)}, =  where the acceptable values for potential impact are low, moderate, high, or not applicable. The potential impact value of not applicable only applies to the security objective of confidentiality. For example, a security category for an information type that processes routine administrative information (non-PII) can be denoted as:  SC administrative information = {(confidentiality, low), (integrity, low), (availability, low)}.  The generalized format for expressing the security category, SC, of a system is similar:  SC = {(confidentiality, impact), (integrity, impact), (availability, impact)}, system  where the acceptable values for potential impact are low, moderate, or high. The potential impact values assigned to the respective security objective (confidentiality, integrity, and availability) are the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the system. The value of not applicable cannot be assigned to any security objective in the context of establishing a security category for a system. For example, a system that processes some information with a potential impact from a loss of confidentiality at moderate, some information with a potential impact from a loss of integrity at moderate, and all the information with a potential impact from a loss of availability at low, may have a security category expressed as:  SC = {(confidentiality, moderate), (integrity, moderate), (availability, low)} system | Inaccurate  - Formula Notation Incorrect |
| What information is needed to categorize a system? | 13. What information is needed to categorize a system?  Answer: Information needed to categorize a system is now being collected in the Prepare step of the Risk Management Framework. Prior to categorizing a system, the authorization boundary needs to be defined. This is now done by task P-11, Authorization Boundary, per SP 800-37, Revision 2 [SP 800-37r2]. Based on the authorization boundary, all information types associated with the system can be identified. The identification of information types and information life cycle is now done by tasks P-12, Information Types, and P-13, Information Life Cycle, in NIST SP 800-37, Revision 2. Information about the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems, may affect the final security impact level determined for the system. Back to Table of Contents] | Information needed to categorize a system is now being collected in the Prepare step of the Risk Management Framework. Prior to categorizing a system, the authorization boundary needs to be defined. This is now done by task P-11, Authorization Boundary, per SP 800-37, Revision 2 [SP 800-37r2]. Based on the authorization boundary, all information types associated with the system can be identified. The identification of information types and information life cycle is now done by tasks P-12, Information Types, and P-13, Information Life Cycle, in NIST SP 800-37, Revision 2. Information about the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems, may affect the final security impact level determined for the system. | Accurate |
| How is the Categorize step related to FIPS publication 199? | 14. How is the Categorize step related to FIPS publication 199?  Answer: FIPS Publication 199 defines the security categorization standard and provides guidance along with NIST SP 800-60, Guide for Mapping Types of Information and Systems to Security Categories [SP 800-60v1]. In accordance with FIPS Publication 199, agencies shall identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The initial activity in mapping types of federal information and systems to security objectives and impact levels is the development of an information taxonomy or the creation of a catalog of information types. The basis for the identification of information types is the OMB's Business Reference Model (BRM) [OMB BRM] Federal Enterprise Architecture (FEA) [OMB FEA] Consolidated Reference Model Document. Each category supports two business areas based on OMB's Business Reference Model (BRM). [Back to Table of Contents] | FIPS Publication 199 defines the security categorization standard and provides guidance along with NIST SP 800-60, Guide for Mapping Types of Information and Systems to Security Categories [SP 800-60v1]. In accordance with FIPS Publication 199, agencies shall identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The initial activity in mapping types of federal information and systems to security objectives and impact levels is the development of an information taxonomy or the creation of a catalog of information types. The basis for the identification of information types is the OMB's Business Reference Model (BRM) [OMB BRM] Federal Enterprise Architecture (FEA) [OMB FEA] Consolidated Reference Model Document. Each category supports two business areas based on OMB's Business Reference Model (BRM). | Accurate |
| What is the organization 's role in categorizing systems? | 15. What is the organization 's role in categorizing systems?  Answer: In order to effectively support information owners and system owners with the categorization process, the organization needs to establish relationships with other organizational entities; develop organization-wide categorization guidance; prepare a supplement to NIST SP 800-60, Volume I [SP 800-60v1]; lead organization-wide categorization sessions; and designate a point of contact to provide advice throughout the categorization process.  The success of the Risk Management Framework is dependent upon collaboration among the organization's many entities. Typically, this is led by the organization 's information security program office. The information security program office reaches out to the information owner/system owner to provide them with the guidance and support they need to effectively and consistently categorize their systems. The information security program office also collaborates with the organization's enterprise architecture group, the personnel conducting the capital planning and investment control process, the information technology operations organization, and others to categorize the organization's systems.  The information security program office prepares categorization guidance that supplements the guidance in NIST SP 800-60 and provides organization-specific procedures, documentation, approval, and reporting requirements. The guidance is distributed to all individuals involved in the categorization process. The information security program office also considers offering training to individuals involved in the categorization process. Training ensures that the organization-specific guidance, tools, templates, and techniques are applied consistently throughout the organization.  While NIST SP 800-60, Volume II SP 800-60v2], provides a comprehensive list of information types that are consistent with the Federal Enterprise Architecture [OMB FEA], organizations may also identify additional information types that are unique to their mission (e.g., National Archives and Records Administration Controlled Unclassified Information Registry [NARA CUI]). The additional, organization-specific information types need to be identified, validated as consistent with the organization 's enterprise architecture, documented, and distributed to the organization's information owner/system owner for use in their system categorization efforts.  Organizations conduct security categorizations of their systems as an organization-wide activity with the involvement of senior leaders and other key officials within the organization (e.g., mission and business owners, information owner/system owner, enterprise architects, information technology planners, system security officers, chief information officer, senior agency information security officer, authorizing officials, and officials executing or participating in the risk executive function) to ensure that each system receives the appropriate management oversight and reflects the needs of the organization as a whole.  The authorizing official or designated representatives reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. The authorizing official collaborates with the senior agency official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets.  W orking together, senior leaders can make informed decisions, provide adequate security, mitigate risks, and help ensure the organization's mission and business activities remain functional. The risk management process begins with the categorization process, which influences all the remaining steps in the Risk Management Framework. A mistake in the initial security categorization process can result in either an over specification or an under specification of the controls for the organization's systems. [Back to Table of Contents] | In order to effectively support information owners and system owners with the categorization process, the organization needs to:  - establish relationships with other organizational entities  - develop organization-wide categorization guidance  - prepare a supplement to NIST SP 800-60, Volume I [SP 800-60v1]  - lead organization-wide categorization sessions  - designate a point of contact to provide advice throughout the categorization process  The success of the Risk Management Framework is dependent upon collaboration among the organization's many entities. Typically, this is led by the organization's information security program office. The information security program office reaches out to the information owner/system owner to provide them with the guidance and support they need to effectively and consistently categorize their systems. The information security program office also collaborates with the organization's enterprise architecture group, the personnel conducting the capital planning and investment control process, the information technology operations organization, and others to categorize the organization's systems.  The information security program office prepares categorization guidance that supplements the guidance in NIST SP 800-60 and provides organization-specific procedures, documentation, approval, and reporting requirements. The guidance is distributed to all individuals involved in the categorization process. The information security program office also considers offering training to individuals involved in the categorization process. Training ensures that the organization-specific guidance, tools, templates, and techniques are applied consistently throughout the organization.  While NIST SP 800-60, Volume II [SP 800-60v2], provides a comprehensive list of information types that are consistent with the Federal Enterprise Architecture [OMB FEA], organizations may also identify additional information types that are unique to their mission (e.g., National Archives and Records Administration Controlled Unclassified Information Registry [NARA CUI]). The additional, organization-specific information types need to be identified, validated as consistent with the organization's enterprise architecture, documented, and distributed to the organization's information owner/system owner for use in their system categorization efforts.  Organizations conduct security categorizations of their systems as an organization-wide activity with the involvement of senior leaders and other key officials within the organization (e.g., mission and business owners, information owner/system owner, enterprise architects, information technology planners, system security officers, chief information officer, senior agency information security officer, authorizing officials, and officials executing or participating in the risk executive function) to ensure that each system receives the appropriate management oversight and reflects the needs of the organization as a whole.  The authorizing official or designated representatives reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. The authorizing official collaborates with the senior agency official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets.  Working together, senior leaders can make informed decisions, provide adequate security, mitigate risks, and help ensure the organization's mission and business activities remain functional. The risk management process begins with the categorization process, which influences all the remaining steps in the Risk Management Framework. A mistake in the initial security categorization process can result in either an over specification or an under specification of the controls for the organization's systems. | Accurate |
| How does the system categorization affect the use of common controls? | 16. How does the system categorization affect the use of common controls?  Answer: In most cases, common controls are managed by an organizational entity other than the information owner/system owner. The common controls are usually implemented by an organization or at a specific site and used to support multiple systems (with various security categories) and organizational needs. The impact level associated with the organization's common controls supports the highest impact level of any individual system within the organization relying on those common controls.  The identification of common controls, which is part of Task P-5 in the Risk Management Framework, is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, senior agency official for privacy, authorizing officials, information owner/system owner, program managers, and system security and system privacy officers. The organization-wide exercise considers the categories of the systems within the organization and the minimum controls necessary to protect the operations and assets supported by those systems. The senior agency information security officer, acting on behalf of the chief information officer, coordinates with the common control provider that is responsible for the development and implementation of the designated common controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information owner/system owner to better support the security authorization process.  If the organization chooses to implement common controls at an impact level that falls below the highest level required for individual systems, the information owner/system owner and authorizing officials for higher impact systems take appropriate actions to supplement the lower impact common controls, as required for any protection deficits that result at the system level. Back to Table of Contents] | In most cases, common controls are managed by an organizational entity other than the information owner/system owner. The common controls are usually implemented by an organization or at a specific site and used to support multiple systems (with various security categories) and organizational needs. The impact level associated with the organization's common controls supports the highest impact level of any individual system within the organization relying on those common controls.  The identification of common controls, which is part of Task P-5 in the Risk Management Framework, is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, senior agency official for privacy, authorizing officials, information owner/system owner, program managers, and system security and system privacy officers. The organization-wide exercise considers the categories of the systems within the organization and the minimum controls necessary to protect the operations and assets supported by those systems. The senior agency information security officer, acting on behalf of the chief information officer, coordinates with the common control provider that is responsible for the development and implementation of the designated common controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information owner/system owner to better support the security authorization process.  If the organization chooses to implement common controls at an impact level that falls below the highest level required for individual systems, the information owner/system owner and authorizing officials for higher impact systems take appropriate actions to supplement the lower impact common controls, as required for any protection deficits that result at the system level. | Accurate |
| What are the steps to categorize a system? | 17. What are the steps to categorize a system?  Answer: To categorize a system, the information owner/system owner identifies the information types (Task P-12 in the Prepare step of the Risk Management Framework), selects the provisional impact value (low, moderate, or high) for each security objective (confidentiality, integrity, and availability) and for each information type, adjusts the provisional impact values for each information type, and assigns the final security impact level for each system.  Prepare for Categorization  In order to determine the system security category, the information owner/system owner collects relevant artifacts specific to the system, such as the system description and architecture. In addition, the information owner/system owner also collects any available guidance artifacts issued by the organization. The information owner/system owner develops relationships with others within their organization who support the categorization process, such as the information security program office, the enterprise architecture group, information sharing partners, and technical operations personnel. Note that many of these activities are addressed by system- level tasks of the Prepare step.  Identify Information Types  The information owner/system owner determines the types of information that is processed by, stored in, or transmitted by the system and documents the information types in the security and privacy plans. This is Task P-12, Information Types, of the Prepare step. While most information types are included in NIST SP 800-60, Volume II [SP 800-60v2], or the organization 's supplement to NIST SP 800-60, an information owner/system owner may identify an information type unique to their system. If so, the unique information type is documented and submitted to the organization's information security program office for validation and inclusion in the organization's supplement to NIST SP 800-60. Note that once information types are identified, all stages of the information life cycle for each information type also needs to be identified and understood. This is addressed by Task P-13, Information Life Cycle.  Select the Provisional Impact Values for Each Information Type  The information owner/system owner reviews NIST SP 800-60, Volume II, and the organization's supplement to NIST SP 800-60 and selects the provisional or initial security category established for each information type. The provisional security category of each information type is documented in the security and privacy plans.  Adjust the Information Type's Provisional Impact Values  The information owner/system owner reviews the appropriateness of the provisional impact values (low, moderate, high) for each security objective (confidentiality, integrity, and availability) for each information type in the system based on the system's operational environment, mission, use, and information sharing with other systems. The provisional impact values are adjusted as necessary based on the special factor guidance provided for each information type in NIST SP 800-60, Volume II, or the organization's supplement to NIST SP 800-60. The rationale for adjusting the provisional impact value of each information type is documented in the security and privacy plans.  After the information types have been adjusted and documented in the security and privacy plans, the information owner/system owner derives the provisional security category for the system by determining the highest value among each security objective (confidentiality, integrity, and availability) for the system's information types (i.e., the highest impact value for confidentiality, the highest impact value for integrity, and the highest impact value for availability).  Adjust the Information Type's Security Category  After each information type has been adjusted and the provisional system security category has been determined, the information owner - with input from senior management - reviews the impact values for confidentiality, integrity, and availability to determine if they are applicable to the system or if a more realistic view of the potential impact on the system requires an increase in one or more security objectives of the system security category. If the impact value for a security objective is changed, the final, adjusted system security category is documented in the security and privacy plans along with the rationale for the change.  Determine the System Security Impact Level  The information owner/system owner assigns the one-value security impact level of low, moderate, or high to the system. For example, if the system's security category is:  SC = {(confidentiality, HIGH), (integrity, MODERATE), (availability, LOW)}, system  the system security impact level is high since the impact value for the confidentiality security objective is high. The one-value impact level is used to determine the initial security baseline during the select process, while the system security category (three values, one for each security objective) is used to tailor the initial control baseline.  The system impact level is documented in the security and privacy plans.  Obtain Approval for the System Security Category and Impact Level  The security category and impact level for the system is approved as defined in an organization's categorization guidance before continuing to the next step (Select) in the Risk Management Framework. It is important to validate the categorization decision since the categorization decision determines the selection of controls that are implemented in the system. For information systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.  Maintain the System Security Category and Impact Level  Periodically the information owner/system owner reconfirms the criticality of the system and the information processed, stored, or transmitted by the system to ensure that the system continues to support the organization's mission or business case. Changes to the system or its operational environment may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities. 「Back to Table of Contents] | To categorize a system, the information owner/system owner identifies the information types (Task P-12 in the Prepare step of the Risk Management Framework), selects the provisional impact value (low, moderate, or high) for each security objective (confidentiality, integrity, and availability) and for each information type, adjusts the provisional impact values for each information type, and assigns the final security impact level for each system.  Prepare for Categorization  In order to determine the system security category, the information owner/system owner collects relevant artifacts specific to the system, such as the system description and architecture. In addition, the information owner/system owner also collects any available guidance artifacts issued by the organization. The information owner/system owner develops relationships with others within their organization who support the categorization process, such as the information security program office, the enterprise architecture group, information sharing partners, and technical operations personnel. Note that many of these activities are addressed by system-level tasks of the Prepare step.  Identify Information Types  The information owner/system owner determines the types of information that is processed by, stored in, or transmitted by the system and documents the information types in the security and privacy plans. This is Task P-12, Information Types, of the Prepare step. While most information types are included in NIST SP 800-60, Volume II [SP 800-60v2], or the organization's supplement to NIST SP 800-60, an information owner/system owner may identify an information type unique to their system. If so, the unique information type is documented and submitted to the organization's information security program office for validation and inclusion in the organization's supplement to NIST SP 800-60. Note that once information types are identified, all stages of the information life cycle for each information type also needs to be identified and understood. This is addressed by Task P-13, Information Life Cycle.  Select the Provisional Impact Values for Each Information Type  The information owner/system owner reviews NIST SP 800-60, Volume II, and the organization's supplement to NIST SP 800-60 and selects the provisional or initial security category established for each information type. The provisional security category of each information type is documented in the security and privacy plans.  Adjust the Information Type's Provisional Impact Values  The information owner/system owner reviews the appropriateness of the provisional impact values (low, moderate, high) for each security objective (confidentiality, integrity, and availability) for each information type in the system based on the system's operational environment, mission, use, and information sharing with other systems. The provisional impact values are adjusted as necessary based on the special factor guidance provided for each information type in NIST SP 800-60, Volume II, or the organization's supplement to NIST SP 800-60. The rationale for adjusting the provisional impact value of each information type is documented in the security and privacy plans.  After the information types have been adjusted and documented in the security and privacy plans, the information owner/system owner derives the provisional security category for the system by determining the highest value among each security objective (confidentiality, integrity, and availability) for the system's information types (i.e., the highest impact value for confidentiality, the highest impact value for integrity, and the highest impact value for availability).  Adjust the Information Type's Security Category  After each information type has been adjusted and the provisional system security category has been determined, the information owner - with input from senior management - reviews the impact values for confidentiality, integrity, and availability to determine if they are applicable to the system or if a more realistic view of the potential impact on the system requires an increase in one or more security objectives of the system security category. If the impact value for a security objective is changed, the final, adjusted system security category is documented in the security and privacy plans along with the rationale for the change.  Determine the System Security Impact Level  The information owner/system owner assigns the one-value security impact level of low, moderate, or high to the system. For example, if the system's security category is:  - SC = {(confidentiality, HIGH), (integrity, MODERATE), (availability, LOW)}, system  the system security impact level is high since the impact value for the confidentiality security objective is high. The one-value impact level is used to determine the initial security baseline during the select process, while the system security category (three values, one for each security objective) is used to tailor the initial control baseline. The system impact level is documented in the security and privacy plans.  Obtain Approval for the System Security Category and Impact Level  The security category and impact level for the system is approved as defined in an organization's categorization guidance before continuing to the next step (Select) in the Risk Management Framework. It is important to validate the categorization decision since the categorization decision determines the selection of controls that are implemented in the system. For information systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.  Maintain the System Security Category and Impact Level  Periodically the information owner/system owner reconfirms the criticality of the system and the information processed, stored, or transmitted by the system to ensure that the system continues to support the organization's mission or business case. Changes to the system or its operational environment may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities. | Inaccurate  - Formula notation wrong |
| What are the potential security impact values? | 18. What are the potential security impact values?  Answer: FIPS Publication 199 defines three levels of potential adverse impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) that represents a worst-case scenario. The application of the impact level definitions takes place within the context of each organization and the overall national interest. The potential impacts are:  · Low, if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  · Moderate, if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  ● High, if the loss confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  Establishing an appropriate security category of an information type essentially requires determining the potential impact for each security objective associated with the particular information type. An additional impact value of not applicable only applies to the security objective of confidentiality if the information type is public information. [Back to Table of Contents] | FIPS Publication 199 defines three levels of potential adverse impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) that represents a worst-case scenario. The application of the impact level definitions takes place within the context of each organization and the overall national interest. The potential impacts are:  · Low, if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  · Moderate, if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  · High, if the loss confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.  Establishing an appropriate security category of an information type essentially requires determining the potential impact for each security objective associated with the particular information type. An additional impact value of not applicable only applies to the security objective of confidentiality if the information type is public information. | Accurate |
| How are the security categories of information types adjusted? | 19. How are the security categories of information types adjusted?  Answer: After each information type has been identified, the provisional security impact values (low, moderate, high, or, for confidentiality only, not applicable) are selected from the recommended provisional levels in NIST SP 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Systems to Security Categories [SP 800-60v2], or the organization's supplement to NIST SP 800- 60. The organization reviews the appropriateness of the provisional security impact values in the context of the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems.  NIST SP 800-60, Volume I [SP 800-60v1], provides the criteria for adjusting the provisional security impact values. The confidentiality, integrity, and availability impact values may be adjusted as necessary during the review. The special factor guidance in NIST SP 800-60, Volume II, provides guidance to adjust each information type. If the special factor guidance applies to the individual system, the impact value for the security objective can be modified. For example, the Budget and Performance Integration Information Type includes the following special factor guidance for the confidentiality security objective that has a recommended impact value of low:  In aggregate, budget and performance integration information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from moderate to high to national security-related.  In another example, the Contingency Planning Information Type has a recommended confidentiality impact value of moderate but provides the following special factors guidance that allows a decrease of the recommended value:  The consequences of unauthorized disclosure of extracts from contingency plans are likely to have negligible to limited adverse effects on agency operations. In such cases, the confidentiality impact would be, at most, low.  In addition, each information type is evaluated with respect to the answers to questions such as the following:  · How can a malicious adversary use the information to do [limited, serious, severe] harm to organizational operations, organizational assets, or individuals?  · w ould authorized disclosure or the dissemination of elements of the information type violate laws, Executive Orders, or organizational regulations?  · What is the impact associated with unauthorized modification or destruction of the information or each unauthorized use of the information by the system?  · What is the impact associated with the loss of availability of the information in the system? [Back to Table of Contents]  After each information type has been identified, the provisional security impact values (low, moderate, high, or, for confidentiality only, not applicable) are selected from the recommended provisional levels in NIST SP 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Systems to Security Categories [SP 800-60v2], or the organization's supplement to NIST SP 800-60. The organization reviews the appropriateness of the provisional security impact values in the context of the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems.  NIST SP 800-60, Volume I [SP 800-60v1], provides the criteria for adjusting the provisional security impact values. The confidentiality, integrity, and availability impact values may be adjusted as necessary during the review. The special factor guidance in NIST SP 800-60, Volume II, provides guidance to adjust each information type. If the special factor guidance applies to the individual system, the impact value for the security objective can be modified. For example, the Budget and Performance Integration Information Type includes the following special factor guidance for the confidentiality security objective that has a recommended impact value of low:  In aggregate, budget and performance integration information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from moderate to high to national security-related.  In another example, the Contingency Planning Information Type has a recommended confidentiality impact value of moderate but provides the following special factors guidance that allows a decrease of the recommended value:  The consequences of unauthorized disclosure of extracts from contingency plans are likely to have negligible to limited adverse effects on agency operations. In such cases, the confidentiality impact would be, at most, low.  In addition, each information type is evaluated with respect to the answers to questions such as the following:  · How can a malicious adversary use the information to do [limited, serious, severe] harm to organizational operations, organizational assets, or individuals?  · Would authorized disclosure or the dissemination of elements of the information type violate laws, Executive Orders, or organizational regulations?  · What is the impact associated with unauthorized modification or destruction of the information or each unauthorized use of the information by the system?  · What is the impact associated with the loss of availability of the information in the system? | After each information type has been identified, the provisional security impact values (low, moderate, high, or, for confidentiality only, not applicable) are selected from the recommended provisional levels in NIST SP 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Systems to Security Categories [SP 800-60v2], or the organization's supplement to NIST SP 800-60. The organization reviews the appropriateness of the provisional security impact values in the context of the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems.  NIST SP 800-60, Volume I [SP 800-60v1], provides the criteria for adjusting the provisional security impact values. The confidentiality, integrity, and availability impact values may be adjusted as necessary during the review. The special factor guidance in NIST SP 800-60, Volume II, provides guidance to adjust each information type. If the special factor guidance applies to the individual system, the impact value for the security objective can be modified. For example, the Budget and Performance Integration Information Type includes the following special factor guidance for the confidentiality security objective that has a recommended impact value of low:  In aggregate, budget and performance integration information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from moderate to high to national security-related.  In another example, the Contingency Planning Information Type has a recommended confidentiality impact value of moderate but provides the following special factors guidance that allows a decrease of the recommended value:  The consequences of unauthorized disclosure of extracts from contingency plans are likely to have negligible to limited adverse effects on agency operations. In such cases, the confidentiality impact would be, at most, low.  In addition, each information type is evaluated with respect to the answers to questions such as the following:  · How can a malicious adversary use the information to do [limited, serious, severe] harm to organizational operations, organizational assets, or individuals?  · Would authorized disclosure or the dissemination of elements of the information type violate laws, Executive Orders, or organizational regulations?  · What is the impact associated with unauthorized modification or destruction of the information or each unauthorized use of the information by the system?  · What is the impact associated with the loss of availability of the information in the system? | Accurate |
| Can the system's security category be adjusted? | 20. Can the system 's security category be adjusted?  Answer: Yes, in some cases, the security category for a system may be higher than any impact value for any information type processed by the system. The following factors can be used to adjust the system security category above that of its constituent information types to reflect a more realistic view of the potential impact that a security breach could have on the system.  Aggregation  Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregate. In some cases, the aggregation of large quantities of a single information type can reveal sensitive patterns or plans or facilitate access to sensitive or critical systems. In other cases, the aggregation of information of several different and seemingly innocuous types can have similar effects. If a review reveals increased criticality associated with information aggregates, an impact value for a security objective in the security category may need to be adjusted to a higher value than would be indicated by the impact values associated with any individual information type.  Critical System Functionality  Compromise of some information types may have a low security impact value in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact on other systems to which the system is connected or on other systems that are dependent on that system's information.  Extenuating Circumstances  There are times when a system's security category is elevated based on reasons other than its information, such as the system's critical process flow or security capability, the visibility of the system to the public, the sheer number of other systems reliant on its operation, or the potential overall cost of replacement. These examples, given a specific situation, may provide reason for the information owner/system owner to increase the impact value for one or more of the security objectives in the security category. An elevation of the security category based on extenuating circumstances can be made more apparent by comparing the original security category to the business impact analysis.  Public Information  Most organizations maintain web pages that are accessible to the public. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the organization. In most cases, the damage can be corrected within a relatively short period of time, and the damage is limited (i.e., the impact value for integrity is low). In other cases (e.g., very large fraudulent transactions or modification of a highly visible web page), the damage to mission function or public confidence in the organization can be serious. In such cases, the integrity impact value associated with unauthorized modification or the destruction of a public web page would be at least moderate.  Catastrophic Loss of System Availability  Either physical or logical destruction of major assets can result in very large expenditures to restore the assets or result in long time periods for recovery. Permanent loss or unavailability of system capabilities can seriously hamper an organization's operations and - where direct services to the public are involved - have a severe adverse impact on public confidence in the organization. In the case of large systems, the loss of system availability may result in a high availability impact that is dependent on the cost and criticality attributes of the system rather than on the availability impact values of the types of information being processed by the system.  Critical Infrastructures and Key National Assets  The Critical Information Infrastructure Act of2002 [HSACT 2002] defines the term critical infrastructure information to mean "information not customarily in the public domain and related to the security of critical infrastructure or protected systems. 22 If information types are aligned with critical infrastructures, then the system must comply with Homeland Security Presidential Directive No. 7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]. Where the mission served by a system or the information that the system processes affects the security of critical national infrastructures or key national assets, the harm that results from a compromise requires particularly close attention. The security category is carefully determined when a loss of confidentiality, integrity, or availability results in a negative impact of the critical infrastructure components and high-value assets (HV As)2.  Trade Secrets  There are several laws that specifically prohibit the unauthorized disclosure of trade secrets. Therefore, if a system stores, communicates, or processes trade secrets, the system's confidentiality security objective is at least moderate. [Back to Table of Contents] | Yes, in some cases, the security category for a system may be higher than any impact value for any information type processed by the system. The following factors can be used to adjust the system security category above that of its constituent information types to reflect a more realistic view of the potential impact that a security breach could have on the system.  - Aggregation: Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregate. In some cases, the aggregation of large quantities of a single information type can reveal sensitive patterns or plans or facilitate access to sensitive or critical systems. In other cases, the aggregation of information of several different and seemingly innocuous types can have similar effects. If a review reveals increased criticality associated with information aggregates, an impact value for a security objective in the security category may need to be adjusted to a higher value than would be indicated by the impact values associated with any individual information type.  - Critical System Functionality: Compromise of some information types may have a low security impact value in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact on other systems to which the system is connected or on other systems that are dependent on that system's information.  - Extenuating Circumstances: There are times when a system's security category is elevated based on reasons other than its information, such as the system's critical process flow or security capability, the visibility of the system to the public, the sheer number of other systems reliant on its operation, or the potential overall cost of replacement. These examples, given a specific situation, may provide reason for the information owner/system owner to increase the impact value for one or more of the security objectives in the security category. An elevation of the security category based on extenuating circumstances can be made more apparent by comparing the original security category to the business impact analysis.  - Public Information: Most organizations maintain web pages that are accessible to the public. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the organization. In most cases, the damage can be corrected within a relatively short period of time, and the damage is limited (i.e., the impact value for integrity is low). In other cases (e.g., very large fraudulent transactions or modification of a highly visible web page), the damage to mission function or public confidence in the organization can be serious. In such cases, the integrity impact value associated with unauthorized modification or the destruction of a public web page would be at least moderate.  - Catastrophic Loss of System Availability: Either physical or logical destruction of major assets can result in very large expenditures to restore the assets or result in long time periods for recovery. Permanent loss or unavailability of system capabilities can seriously hamper an organization's operations and - where direct services to the public are involved - have a severe adverse impact on public confidence in the organization. In the case of large systems, the loss of system availability may result in a high availability impact that is dependent on the cost and criticality attributes of the system rather than on the availability impact values of the types of information being processed by the system.  - Critical Infrastructures and Key National Assets: The Critical Information Infrastructure Act of 2002 [HSACT 2002] defines the term critical infrastructure information to mean "information not customarily in the public domain and related to the security of critical infrastructure or protected systems." If information types are aligned with critical infrastructures, then the system must comply with Homeland Security Presidential Directive No. 7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]. Where the mission served by a system or the information that the system processes affects the security of critical national infrastructures or key national assets, the harm that results from a compromise requires particularly close attention. The security category is carefully determined when a loss of confidentiality, integrity, or availability results in a negative impact of the critical infrastructure components and high-value assets (HVAs).  - Trade Secrets: There are several laws that specifically prohibit the unauthorized disclosure of trade secrets. Therefore, if a system stores, communicates, or processes trade secrets, the system's confidentiality security objective is at least moderate. | Accurate |
| How is the overall security impact level of the system determined? | 21. How is the overall security impact level of the system determined?  Answer: The security impact level of a system is the highest impact value for the security objectives (confidentiality, integrity, and availability) associated with the aggregate impact values of the system's information types (i.e., the system's security category). Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular system, the high watermark concept (highest value) representing the worst-case scenario is used to determine the security impact level of the system.  Therefore, a low-impact system is defined as a system in which all three of the security objectives are low. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is greater than moderate. A high- impact system is a system in which at least one security objective is high. The system's impact level is subsequently used to select the initial set of baseline security controls from NIST SP 800-53B [SP 800-53B]. The end result produces an organization-wide view of the criticality and sensitivity of the systems supporting mission and business processes and potential (worst case) impact to  2 High-value assets do not necessarily impact the categorization. However, having HVAs in and/or interconnected with the authorization boundary may impact the categorization.  organizational operations and assets, individuals, other organizations, and the Nation should the systems be compromised. [Back to Table of Contents] | The security impact level of a system is the highest impact value for the security objectives (confidentiality, integrity, and availability) associated with the aggregate impact values of the system's information types (i.e., the system's security category). Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular system, the high watermark concept (highest value) representing the worst-case scenario is used to determine the security impact level of the system.  Therefore, a low-impact system is defined as a system in which all three of the security objectives are low. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is greater than moderate. A high-impact system is a system in which at least one security objective is high. The system's impact level is subsequently used to select the initial set of baseline security controls from NIST SP 800-53B [SP 800-53B]. The end result produces an organization-wide view of the criticality and sensitivity of the systems supporting mission and business processes and potential (worst case) impact to organizational operations and assets, individuals, other organizations, and the Nation should the systems be compromised. | Accurate |
| Should a system always be high-impact if at least one of its information types is categorized as high? | 22. Should a system always be high-impact if at least one of its information types is categorized as high?  Answer: Y es, once the system security category has been determined (with impact values assigned to the respective security objectives), the system's impact level is the highest value (high water mark) from among the values assigned to the security objectives in the security category. However, while the impact level is based on the high watermark and determines the initial security control baseline associated with the system (low, moderate, or high security baseline), organizations have the flexibility to adjust the control baselines by following the tailoring guidance as defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). [Back to Table of Contents] | Yes, once the system security category has been determined (with impact values assigned to the respective security objectives), the system's impact level is the highest value (high water mark) from among the values assigned to the security objectives in the security category. However, while the impact level is based on the high watermark and determines the initial security control baseline associated with the system (low, moderate, or high security baseline), organizations have the flexibility to adjust the control baselines by following the tailoring guidance as defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). | Accurate |
| How should the system categorization be documented? | 23. How should the system categorization be documented?  Answer: The information owner/system owner documents the system categorization in the security and privacy plans. In addition to the final categorization decision (i.e., the system's security impact level), the research, key decisions, and supporting categorization rationale are also documented in the security and privacy plans.  For each information type, the following information is documented:  · Information type title  · Reference to the catalog in which the information type is described (e.g., NIST SP 800-60, Volume II [SP 800-60v2], or the organization's supplement to NIST SP 800-60)  · Provisional security category of the information type  · If the provisional security category of the information type was changed:  ○ The adjusted security impact values of the information type and ○ Rationale for increasing or decreasing the impact value of the information type  For the system, the following information is documented:  · Provisional (three-value) security category of the system  · The (one-value) security impact level of the system (derived from the security category) [Back to Table of Contents] | The information owner/system owner documents the system categorization in the security and privacy plans. In addition to the final categorization decision (i.e., the system's security impact level), the research, key decisions, and supporting categorization rationale are also documented in the security and privacy plans.  For each information type, the following information is documented:  - Information type title  - Reference to the catalog in which the information type is described (e.g., NIST SP 800-60, Volume II [SP 800-60v2], or the organization's supplement to NIST SP 800-60)  - Provisional security category of the information type  - If the provisional security category of the information type was changed:  - The adjusted security impact values of the information type and  - Rationale for increasing or decreasing the impact value of the information type  For the system, the following information is documented:  - Provisional (three-value) security category of the system  - The (one-value) security impact level of the system (derived from the security category) | Accurate |
| Is it ever necessary to modify the security category of an information type? | 24. Is it ever necessary to modify the security category of an information type?  Answer: Yes, there are times when it is necessary to modify the security category of an information type after the initial categorization is completed. The security impact values for an information type may vary throughout the system's life cycle. For example, contract information that has a moderate confidentiality impact value during the life of the contract may have a low impact value when the contract is completed. Legislation may also levy additional requirements on some types ofinformation. Some of the statutory and regulatory specifications are listed in NIST SP 800-60, Volume II [SP 800-60v2]. The security category is reviewed on an ongoing basis to help ensure that it reflects the current organizational environment and priorities. Back to Table of Contents] | Yes, there are times when it is necessary to modify the security category of an information type after the initial categorization is completed. The security impact values for an information type may vary throughout the system's life cycle. For example, contract information that has a moderate confidentiality impact value during the life of the contract may have a low impact value when the contract is completed. Legislation may also levy additional requirements on some types of information. Some of the statutory and regulatory specifications are listed in NIST SP 800-60, Volume II [SP 800-60v2]. The security category is reviewed on an ongoing basis to help ensure that it reflects the current organizational environment and priorities. | Accurate |
| What system characteristics does an organization document? | 25. What system characteristics does an organization document?  Answer: A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the system development life cycle. Duplication of information is avoided whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the security and privacy risk assessments of the system. Information may be added to the system description as it becomes available during the system life cycle and execution of the RMF steps.  System characteristics include:  · Descriptive name of the system,  · System version or release number,  · Purpose of the system,  · Incident response points of contact,  · Authorization date and authorization termination date, and  · Network topology and architecture description.  [Back to Table of Contents | A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the system development life cycle. Duplication of information is avoided whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the security and privacy risk assessments of the system. Information may be added to the system description as it becomes available during the system life cycle and execution of the RMF steps.  System characteristics include:  - Descriptive name of the system,  - System version or release number,  - Purpose of the system,  - Incident response points of contact,  - Authorization date and authorization termination date, and  - Network topology and architecture description. | Accurate |
| What is new in Windows Server 2012? | Q1. What is new in Windows Server 2012?  Answer: Windows Server 2012 brings our company's experience building and operating public clouds to the server platform for private clouds. The new licensing and packaging makes it easier to manage workloads in highly virtualized public and private cloud environments. Windows Server 2012 will move to a consistent licensing model and will have common features enabling the reduction of editions. These include  · Two editions, Standard and Datacenter. · Single licenses that cover up to two physical processors. · Editions differentiated by virtualization rights only (two for Standard; unlimited for Datacenter). | Windows Server 2012 brings our company's experience building and operating public clouds to the server platform for private clouds. The new licensing and packaging makes it easier to manage workloads in highly virtualized public and private cloud environments. Windows Server 2012 will move to a consistent licensing model and will have common features enabling the reduction of editions. These include  - Two editions, Standard and Datacenter.  - Single licenses that cover up to two physical processors.  - Editions differentiated by virtualization rights only (two for Standard; unlimited for Datacenter). | Accurate |
| What is the difference between Windows Server 2012 Standard edition and Windows Server 2012 Datacenter edition? | Q2. What is the difference between Windows Server 2012 Standard edition and Windows Server 2012 Datacenter edition?  Answer: Both Standard and Datacenter editions provide the same set of features; the only thing that differentiates the editions is the number of Virtual Machines (VMs). A Standard edition license will entitle you to run up to two VMs on up to two processors (subject to the VM use rights outlined in the Product Use Rights document). A Datacenter edition license will entitle you to run an unlimited number of VMs on up to two processors. | Both Standard and Datacenter editions provide the same set of features; the only thing that differentiates the editions is the number of Virtual Machines (VMs). A Standard edition license will entitle you to run up to two VMs on up to two processors (subject to the VM use rights outlined in the Product Use Rights document). A Datacenter edition license will entitle you to run an unlimited number of VMs on up to two processors. | Accurate |
| Will Windows Server 2012 Standard edition have all of the same features as Windows Server 2012 Datacenter edition? | Q3. Will Windows Server 2012 Standard edition have all of the same features as Windows Server 2012 Datacenter edition?  Answer: Yes. All features that are available in the Datacenter edition are also available in the Standard edition, including high availability features like failover clustering. The only difference between the two editions will be virtualization rights. | Yes. All features that are available in the Datacenter edition are also available in the Standard edition, including high availability features like failover clustering. The only difference between the two editions will be virtualization rights | Accurate |
| Is Windows Server 2012 aligning to the System Center 2012 and Enrollment for Core Infrastructure (ECI) model? | Q4. Is Windows Server 2012 aligning to the System Center 2012 and Enrollment for Core Infrastructure (ECI) model?  Answer: Yes. As part of the alignment with the Microsoft private cloud licensing model, Windows Server 2012 and System Center 2012, as well as Enrollment for Core Infrastructure (ECI), will have the same licensing and packaging structure. These include  · Two editions, Standard and Datacenter. · Single licenses that cover up to two physical processors. · Editions differentiated by virtualization rights only (two for Standard; unlimited for Datacenter).  Client Access Licenses (CALs) will continue to be required for access to Windows Server 2012 servers. | Yes. As part of the alignment with the Microsoft private cloud licensing model, Windows Server 2012 and System Center 2012, as well as Enrollment for Core Infrastructure (ECI), will have the same licensing and packaging structure. These include  · Two editions, Standard and Datacenter.  · Single licenses that cover up to two physical processors.  · Editions differentiated by virtualization rights only (two for Standard; unlimited for Datacenter).  Client Access Licenses (CALs) will continue to be required for access to Windows Server 2012 servers. | Accurate |
| What are some of the features now available in Windows Server 2012 Standard that were previously only available in Windows Server 2008 R2 Enterprise and Datacenter editions? | Q5. What are some of the features now available in Windows Server 2012 Standard that were previously only available in Windows Server 2008 R2 Enterprise and Datacenter editions?  Answer: There are a variety of new features in Windows Server 2012 Standard edition. Here are just a few examples of what was previously only available in the premium editions:  · Windows Server Failover Clustering · BranchCache Hosted Cache Server · Active Directory Federated Services · Additional Active Directory Certificate Services capabilities · Distributed File Services (support for more than 1 DFS root) · DFS-R Cross-File Replication | There are a variety of new features in Windows Server 2012 Standard edition. Here are just a few examples of what was previously only available in the premium editions:  · Windows Server Failover Clustering  · BranchCache Hosted Cache Server  · Active Directory Federated Services  · Additional Active Directory Certificate Services capabilities  · Distributed File Services (support for more than 1 DFS root)  · DFS-R Cross-File Replication | Accurate |
| How do I determine which Windows Server 2012 edition is right for me? | Q6. How do I determine which Windows Server 2012 edition is right for me?  Answer: Since there is feature parity between Windows Server 2012 Standard and Datacenter editions, your decision will be based solely on your virtualization strategy as virtualization rights become the only differentiator between editions. If your strategy calls for a highly virtualized environment, Datacenter edition will provide you with optimum flexibility since it allows for unlimited virtualization. If you do not plan on a highly virtualized environment at this time, Standard edition is the right product for your needs. If you purchase Standard edition today but find that you need more capacity in the future you will have two options to expand the virtualization capacity of your licensed server:  1. Purchase additional Standard edition licenses and assign them to the same physical server giving you the rights to run additional instances of Windows Server, or 2. If you have Software Assurance on your Standard license you can purchase a Software Assurance Step-Up and migrate to a Datacenter edition license on that server  If you are running a highly virtualized environment, management may also be a need for you. You should consider purchasing System Center 2012 with Windows Server 2012 together in the Core Infrastructure Suite, which is available inside or outside of an Enrollment for Core Infrastructure (ECI) agreement. | Since there is feature parity between Windows Server 2012 Standard and Datacenter editions, your decision will be based solely on your virtualization strategy as virtualization rights become the only differentiator between editions. If your strategy calls for a highly virtualized environment, Datacenter edition will provide you with optimum flexibility since it allows for unlimited virtualization. If you do not plan on a highly virtualized environment at this time, Standard edition is the right product for your needs. If you purchase Standard edition today but find that you need more capacity in the future you will have two options to expand the virtualization capacity of your licensed server:  - Purchase additional Standard edition licenses and assign them to the same physical server giving you the rights to run additional instances of Windows Server, or  - If you have Software Assurance on your Standard license you can purchase a Software Assurance Step-Up and migrate to a Datacenter edition license on that server  If you are running a highly virtualized environment, management may also be a need for you. You should consider purchasing System Center 2012 with Windows Server 2012 together in the Core Infrastructure Suite, which is available inside or outside of an Enrollment for Core Infrastructure (ECI) agreement. | Accurate |
| If I have a Windows Server 2012 Standard edition license, how can I increase my virtualization rights? | Q7. If I have a Windows Server 2012 Standard edition license, how can I increase my virtualization rights?  Answer: With the Windows Server 2012 Standard edition licensing model, you can grow your virtualization environment by either stepping up your license to Datacenter edition if you have Software Assurance, or by simply buying additional Standard edition licenses and assigning them to the same physical server. For example, if you have a 2-processor server and want to run a total of 4 VMs, you can purchase two Standard edition licenses and assign them to the same server. Additional examples are shown in the table below.  The information outlines the relationship between the number of Standard edition licenses on a single server and the total number of virtual machines (VMs) that can be supported. With one Standard edition license, a server can host two virtual machines. Increasing the licenses to two allows for four virtual machines. When three licenses are applied, the server can support six virtual machines. Finally, with four licenses, the server can accommodate eight virtual machines. This pattern indicates that each additional license enables the support of two more virtual machines on the server. | With the Windows Server 2012 Standard edition licensing model, you can grow your virtualization environment by either stepping up your license to Datacenter edition if you have Software Assurance, or by simply buying additional Standard edition licenses and assigning them to the same physical server. For example, if you have a 2-processor server and want to run a total of 4 VMs, you can purchase two Standard edition licenses and assign them to the same server. Additional examples are shown in the table below.  The information outlines the relationship between the number of Standard edition licenses on a single server and the total number of virtual machines (VMs) that can be supported.  - With one Standard edition license, a server can host two virtual machines.  - Increasing the licenses to two allows for four virtual machines.  - When three licenses are applied, the server can support six virtual machines.  - Finally, with four licenses, the server can accommodate eight virtual machines.  This pattern indicates that each additional license enables the support of two more virtual machines on the server. | Accurate |
| Why is Windows Server 2012 licensing moving to a processor model? | Q8. Why is Windows Server 2012 licensing moving to a processor model?  Answer: By making this change, Windows Server 2012, System Center 2012 and the Core Infrastructure Server (CIS) will all have consistent licensing model creating alignment across Microsoft infrastructure products. Having a single-licensing model will make it easier for you to buy the right product for your needs and to compare the cost of alternatives (such as individual products, the CIS SKU outside of ECI, ECI and SO on). Additionally, the new licensing model provides a single, familiar, and easy-to-track metric for all infrastructure products further reducing management overhead. | By making this change, Windows Server 2012, System Center 2012, and the Core Infrastructure Server (CIS) will all have a consistent licensing model creating alignment across Microsoft infrastructure products. Having a single-licensing model will make it easier for you to buy the right product for your needs and to compare the cost of alternatives (such as individual products, the CIS SKU outside of ECI, ECI, and so on). Additionally, the new licensing model provides a single, familiar, and easy-to-track metric for all infrastructure products, further reducing management overhead. | Accurate |
| How do I calculate the number of licenses I need for a server? | Q9. How do I calculate the number of licenses I need for a server?  Answer: The number of licenses you will need depends on the number of physical processors on the server and the number of server instances that you will be running. (This only applies for Standard edition because Datacenter edition allows for unlimited VMs.) The larger of these two numbers determines the number of total licenses required.  Determining the number of physical processor licenses  Each license covers up to two physical processors, SO to determine the number of licenses needed to fully license a physical server, simply count the number of physical processors in the server, divide that number by two and that tells you the number of licenses that will be needed.  Here are some examples:  · You have a 2-processor server. 2 physical processors / 2 (number of processors covered by a license) equals 1. You will need one license to cover a 2-processor server.  · You have a 4-processor server. 4 physical processors / 2 (number of processors covered by a license) equals 2. You will need two licenses to cover a 4-processor server.  · You have an 8-processor server. 8 physical processors / 2 (number of processors covered by a license) equals 4. You will need four licenses to cover an 8-processor server.  Determining the number of virtual instances running  If you want to run additional VMs but do not require the highly virtualized environment that Datacenter provides (which is unlimited VMs), then you can simply purchase additional Standard edition licenses and assign them to a single physical server to increase your VM entitlements on that server. Each Standard edition license provides you with the rights to run up to two VMs, so to determine the number of Windows Server Standard edition licenses you need, count the total number of total VMs that you will run on the server; divide that number by two, and round up to the nearest whole number.  For example, if you assign 2 Standard edition licenses to a single server, you will be able to run a total of 4 VMs on that server. If you add additional Standard edition licenses to that server the number of allowed VMs on that particular server will increase by two for a total of six VMs on that server.  Once the number of licenses needed to cover a physical processor and/or additional VMs is determined, the higher of those two numbers represents the total number of licenses required.  For example, if you are running 4 virtual machines on a 2-processor server, you will require 1 license to cover the 2 processors; but you will need an additional license to run 4 virtual machines, which means you will need a total of 2 licenses. | The number of licenses you will need depends on the number of physical processors on the server and the number of server instances that you will be running. (This only applies for Standard edition because Datacenter edition allows for unlimited VMs.) The larger of these two numbers determines the number of total licenses required.  Determining the number of physical processor licenses  Each license covers up to two physical processors, so to determine the number of licenses needed to fully license a physical server, simply count the number of physical processors in the server, divide that number by two and that tells you the number of licenses that will be needed.  Here are some examples:  - You have a 2-processor server. 2 physical processors / 2 (number of processors covered by a license) equals 1. You will need one license to cover a 2-processor server.  - You have a 4-processor server. 4 physical processors / 2 (number of processors covered by a license) equals 2. You will need two licenses to cover a 4-processor server.  - You have an 8-processor server. 8 physical processors / 2 (number of processors covered by a license) equals 4. You will need four licenses to cover an 8-processor server.  Determining the number of virtual instances running  If you want to run additional VMs but do not require the highly virtualized environment that Datacenter provides (which is unlimited VMs), then you can simply purchase additional Standard edition licenses and assign them to a single physical server to increase your VM entitlements on that server. Each Standard edition license provides you with the rights to run up to two VMs, so to determine the number of Windows Server Standard edition licenses you need, count the total number of total VMs that you will run on the server; divide that number by two, and round up to the nearest whole number.  For example, if you assign 2 Standard edition licenses to a single server, you will be able to run a total of 4 VMs on that server. If you add additional Standard edition licenses to that server the number of allowed VMs on that particular server will increase by two for a total of six VMs on that server.  Once the number of licenses needed to cover a physical processor and/or additional VMs is determined, the higher of those two numbers represents the total number of licenses required.  For example, if you are running 4 virtual machines on a 2-processor server, you will require 1 license to cover the 2 processors; but you will need an additional license to run 4 virtual machines, which means you will need a total of 2 licenses. | Accurate |
| Can I use one Standard license to cover a 1-processor server? | Q10. Can I use one Standard license to cover a 1-processor server?  Answer: Yes. The Standard edition license will allow you to license up to two physical processors on a single server; however it does not require that the server has two physical processors. | Yes. The Standard edition license will allow you to license up to two physical processors on a single server; however, it does not require that the server has two physical processors. | Accurate |
| Can I split my Windows Server 2012 license across multiple servers? | Q11. Can I split my Windows Server 2012 license across multiple servers?  Answer: No. Each license can only be assigned to a single physical server. | No. Each license can only be assigned to a single physical server. | Accurate |
| Can I assign a Windows Server 2012 license to a virtual machine? | Q12. Can I assign a Windows Server 2012 license to a virtual machine?  Answer: No. A license is assigned to the physical server. Each license will cover up to two physical processors. | No. A license is assigned to the physical server. Each license will cover up to two physical processors. | Accurate |
| Can I mix Datacenter and Standard licenses on the same server? | Q13. Can I mix Datacenter and Standard licenses on the same server?  Answer: No. All of the processors on a given server must be licensed with the same version and edition. You can run different editions or older versions of Windows Server software as guests within VMs, but you are not allowed to assign multiple licenses of different versions or editions to the same physical server to license the processors on the server. | No. All of the processors on a given server must be licensed with the same version and edition. You can run different editions or older versions of Windows Server software as guests within VMs, but you are not allowed to assign multiple licenses of different versions or editions to the same physical server to license the processors on the server. | Accurate |
| Can I attach another license of a different version or edition of Windows Server to increase my virtualization rights? | Q14. Can I attach another license of a different version or edition of Windows Server to increase my virtualization rights?  Answer: Yes, you can assign additional Windows Server licenses to a server to increase your virtualization rights. However the newly assigned licenses will need to adhere to their associated licensing rules. For example, if you have a Windows Server Enterprise edition license on a four processor server and want to attach Windows Server 2012 Standard edition licenses to increase your virtualization rights, you will need to ensure that all processors on that server are licensed with Windows Server 2012 Standard edition license as well, which will require a total of two Windows Server 2012 Standard licenses (as each license covers up to two processors). | Yes, you can assign additional Windows Server licenses to a server to increase your virtualization rights. However, the newly assigned licenses will need to adhere to their associated licensing rules. For example, if you have a Windows Server Enterprise edition license on a four-processor server and want to attach Windows Server 2012 Standard edition licenses to increase your virtualization rights, you will need to ensure that all processors on that server are licensed with Windows Server 2012 Standard edition license as well, which will require a total of two Windows Server 2012 Standard licenses (as each license covers up to two processors). | Accurate |
| If I want to use the bits from an earlier version or edition, what are my options? | Q15. If I want to use the bits from an earlier version or edition, what are my options?  Answer: If you have Windows Server 2012 Datacenter edition you will have the right to downgrade your bits to any prior version or lower edition. If you have Windows Server 2012 Standard edition, you will have the right to downgrade your bits to any prior version of Enterprise, Standard or Essentials editions.  The ability to run downgrade bits does not change the licensing or support terms in which you can use the product; the purchased product (Windows Server 2012) rights apply. This means that the license will continue to cover two physical processors and the virtualization rights do not change. In addition, the Client Access License (CAL) corresponding to the purchased version will apply, as an exception, if you are running a previous version of one of the eligible downgrades you can use the corresponding CAL version if one exists.  Here are a few examples.  The information outlines the downgrade and licensing rights for different software licenses. For a Datacenter 2012 license, the downgrade version is Datacenter 2008, with bit rights applicable to Datacenter 2008, while licensing rights remain with Datacenter 2012. A Standard 2012 license can be downgraded to Enterprise 2008 R2, with bit rights for Enterprise 2008 R2, and licensing rights for Standard 2012. Another Standard 2012 license allows downgrading to Standard 2008, with corresponding bit rights, and retains licensing rights for Standard 2012. Lastly, a Standard 2012 license can be downgraded to Essentials 2012, with bit rights for Essentials 2012, while maintaining licensing rights for Standard 2012.  1 The license will cover up to two processors. 2 The license entitles up to two virtual machines. | If you have Windows Server 2012 Datacenter edition you will have the right to downgrade your bits to any prior version or lower edition. If you have Windows Server 2012 Standard edition, you will have the right to downgrade your bits to any prior version of Enterprise, Standard or Essentials editions. The ability to run downgrade bits does not change the licensing or support terms in which you can use the product; the purchased product (Windows Server 2012) rights apply. This means that the license will continue to cover two physical processors and the virtualization rights do not change. In addition, the Client Access License (CAL) corresponding to the purchased version will apply, as an exception, if you are running a previous version of one of the eligible downgrades you can use the corresponding CAL version if one exists. Here are a few examples.  The information outlines the downgrade and licensing rights for different software licenses.  - For a Datacenter 2012 license, the downgrade version is Datacenter 2008, with bit rights applicable to Datacenter 2008, while licensing rights remain with Datacenter 2012.  - A Standard 2012 license can be downgraded to Enterprise 2008 R2, with bit rights for Enterprise 2008 R2, and licensing rights for Standard 2012.  - Another Standard 2012 license allows downgrading to Standard 2008, with corresponding bit rights, and retains licensing rights for Standard 2012.  - Lastly, a Standard 2012 license can be downgraded to Essentials 2012, with bit rights for Essentials 2012, while maintaining licensing rights for Standard 2012.  1 The license will cover up to two processors. 2 The license entitles up to two virtual machines. | Accurate |
| Is Enterprise edition going away as part of Windows Server 2012 and why? | Q16. Is Enterprise edition going away as part of Windows Server 2012 and why?  Answer: Yes. Enterprise edition will be retired as part of the Windows Server 2012 release. Windows Server 2012 Standard edition will include all the premium features previously included in Enterprise edition in the past and the price to purchase the rights to 4 instances of Windows Server 2012 will actually be less expensive than the price of Windows Server 2008 R2 Enterprise edition today. Due to these changes, we have been able to simplify the product lineup while reducing the price per instance of Windows Server for these customers. | Yes. Enterprise edition will be retired as part of the Windows Server 2012 release. Windows Server 2012 Standard edition will include all the premium features previously included in Enterprise edition in the past and the price to purchase the rights to 4 instances of Windows Server 2012 will actually be less expensive than the price of Windows Server 2008 R2 Enterprise edition today. Due to these changes, we have been able to simplify the product lineup while reducing the price per instance of Windows Server for these customers. | Accurate |
| Is Web Server going away as part of Windows Server 2012 and why? | Q17. Is Web Server going away as part of Windows Server 2012 and why?  Answer: Yes. The Web Server product was designed primarily for end customers and service providers that wanted to host web sites. However, consistent feedback from these customers and partners has been that they prefer to use an edition of Windows Server that does not restrict usage to running web workloads.  Despite the removal of Web Server edition, web workloads running on a Windows Server 2012 edition will continue to receive the "CAL waiver" that is in effect for these workloads today. Windows Server  CALs will not be required to access the licensed server if it is only being used to run web workloads. See Product Use Rights for details. | Yes. The Web Server product was designed primarily for end customers and service providers that wanted to host web sites. However, consistent feedback from these customers and partners has been that they prefer to use an edition of Windows Server that does not restrict usage to running web workloads. Despite the removal of Web Server edition, web workloads running on a Windows Server 2012 edition will continue to receive the "CAL waiver" that is in effect for these workloads today. Windows Server CALs will not be required to access the licensed server if it is only being used to run web workloads. See Product Use Rights for details. | Accurate |
| Are the HPC products going away as part of Windows Server 2012 and why? | Q18. Are the HPC products going away as part of Windows Server 2012 and why?  Answer: While the HPC edition is being retired, Microsoft will be delivering the HPC Pack 2012 as a free download that can be used with any Windows Server 2012 Standard or Datacenter license. As a result, customers who want to run HPC workloads will be able to do SO on any of their Windows Server 2012 licensed servers (Click here for a free download.). HPC workloads running on Windows Server 2012 Standard or Datacenter editions will continue to receive the "CAL waiver" that is currently in effect for these workloads. Windows Server CALs will not be required to access instances of Windows Server in the Windows Server 2012 licensing model if these instances are simply running HPC workloads. See Product Use Rights for details. | While the HPC edition is being retired, Microsoft will be delivering the HPC Pack 2012 as a free download that can be used with any Windows Server 2012 Standard or Datacenter license. As a result, customers who want to run HPC workloads will be able to do so on any of their Windows Server 2012 licensed servers. HPC workloads running on Windows Server 2012 Standard or Datacenter editions will continue to receive the "CAL waiver" that is currently in effect for these workloads. Windows Server CALs will not be required to access instances of Windows Server in the Windows Server 2012 licensing model if these instances are simply running HPC workloads. See Product Use Rights for details. | Accurate |
| If I have Software Assurance in place at the time that Windows Server 2012 is generally available, when will my grant be reflected in my licensing records? | Q19. If I have Software Assurance in place at the time that Windows Server 2012 is generally available, when will my grant be reflected in my licensing records?  Answer: While you will immediately be able to use the new product and will own the perpetual rights to the edition of Windows Server 2012 that you are transitioning to, your grant will not be reflected in the license position database until you renew your agreement and purchase Software Assurance on the granted licenses. If you do not renew your Software Assurance, your license position will not be reflected in the license position database; however the fact that you had Software Assurance in place at the time of Windows Server 2012 General Availability will establish your proof of license for the new product. | While you will immediately be able to use the new product and will own the perpetual rights to the edition of Windows Server 2012 that you are transitioning to, your grant will not be reflected in the license position database until you renew your agreement and purchase Software Assurance on the granted licenses. If you do not renew your Software Assurance, your license position will not be reflected in the license position database; however, the fact that you had Software Assurance in place at the time of Windows Server 2012 General Availability will establish your proof of license for the new product. | Accurate |
| If I have Datacenter edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q20. If I have Datacenter edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Datacenter edition, you will be entitled to Windows Server 2012 Datacenter edition. Today, a Datacenter license covers up to 1 processor. A Windows Server 2012 Datacenter license will cover up to 2 processors. So for every two current Datacenter licenses with Software Assurance, you will receive one Windows Server 2012 Datacenter edition license. | If you have Software Assurance on Datacenter edition, you will be entitled to Windows Server 2012 Datacenter edition. Today, a Datacenter license covers up to 1 processor. A Windows Server 2012 Datacenter license will cover up to 2 processors. So for every two current Datacenter licenses with Software Assurance, you will receive one Windows Server 2012 Datacenter edition license. | Accurate |
| If I have Enterprise edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q21. If I have Enterprise edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Enterprise edition, you will be entitled to receive two Standard edition licenses for each Enterprise edition license you have.  If you are considering moving to a more highly virtualized or private cloud environment, you should consider taking advantage of the Software Assurance Step-Up\* benefit to upgrade to Datacenter edition prior to the Windows Server 2012 general availability since the Step-Ups from Enterprise edition to Datacenter edition will be removed from the price lists at that time.  \* If you have an Enterprise Agreement and already have an SA Step-Up from Enterprise edition to Datacenter edition on your Channel Price Sheet (CPS), you will be able to Step-Up from Enterprise edition to Datacenter edition until the end of your enrollment. | If you have Software Assurance on Enterprise edition, you will be entitled to receive two Standard edition licenses for each Enterprise edition license you have. If you are considering moving to a more highly virtualized or private cloud environment, you should consider taking advantage of the Software Assurance Step-Up\* benefit to upgrade to Datacenter edition prior to the Windows Server 2012 general availability since the Step-Ups from Enterprise edition to Datacenter edition will be removed from the price lists at that time.  \* If you have an Enterprise Agreement and already have an SA Step-Up from Enterprise edition to Datacenter edition on your Channel Price Sheet (CPS), you will be able to Step-Up from Enterprise edition to Datacenter edition until the end of your enrollment. | Accurate |
| If I have Standard edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q22. If I have Standard edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Standard edition today, you will be entitled to receive Standard edition at the general availability of Windows Server 2012. You will receive one Windows Server 2012 Standard edition license for each Standard edition license you have. | If you have Software Assurance on Standard edition today, you will be entitled to receive Standard edition at the general availability of Windows Server 2012. You will receive one Windows Server 2012 Standard edition license for each Standard edition license you have. | Accurate |
| If the normal Software Assurance transition grant will not cover all of the processors in my server do I need to purchasing additional licenses? | Q23. If the normal Software Assurance transition grant will not cover all of the processors in my server do I need to purchasing additional licenses?  Answer: No. If you have Software Assurance on Enterprise, Standard or Windows Server 2008 R2 HPC editions when Windows Server 2012 is released and the normal Software Assurance transition grant does not cover all of the processors on your physical server, you can qualify for additional licenses by documenting your environment to show where you have Windows Server 2008 R2 Standard edition or Windows Server 2008 R2 HPC editions running on 4-processor servers and/or Windows Server 2008 R2 Enterprise edition running on an 8-processor server. You will then be entitled to the additional licenses needed to cover these processors.  It is recommended that you complete your self-assessment using the Microsoft Assessment and Planning (MAP) Toolkit or another inventory tool that can accurately archive a time/date-stamped inventory of your hardware with Windows Server installations.  Upon contract expiration, you can renew Software Assurance on all licenses granted as a result of transitioning to the Windows Server 2012 licensing model. | No. If you have Software Assurance on Enterprise, Standard or Windows Server 2008 R2 HPC editions when Windows Server 2012 is released and the normal Software Assurance transition grant does not cover all of the processors on your physical server, you can qualify for additional licenses by documenting your environment to show where you have Windows Server 2008 R2 Standard edition or Windows Server 2008 R2 HPC editions running on 4-processor servers and/or Windows Server 2008 R2 Enterprise edition running on an 8-processor server. You will then be entitled to the additional licenses needed to cover these processors.  It is recommended that you complete your self-assessment using the Microsoft Assessment and Planning (MAP) Toolkit or another inventory tool that can accurately archive a time/date-stamped inventory of your hardware with Windows Server installations.  Upon contract expiration, you can renew Software Assurance on all licenses granted as a result of transitioning to the Windows Server 2012 licensing model. | Accurate |
| If I have Web Server edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q24. If I have Web Server edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Web Server edition, you will receive an additional Windows Server 2012 Standard edition license that you can use while also maintaining your rights to run your current Web Server license. For every two Windows 2008 R2 Web Server edition licenses, you will receive one Windows Server 2012 Standard edition license. If you have an odd number of Windows 2008 R2 Web Server edition licenses, your grant will be based on rounding up to the next whole even number.  You will continue to have the ability to host web content on your new Windows Server 2012 Standard edition license without needing a Windows Server CAL to access the server, but any other workloads that you decide to run on your new server will follow the standard Windows CAL licensing requirements. | If you have Software Assurance on Web Server edition, you will receive an additional Windows Server 2012 Standard edition license that you can use while also maintaining your rights to run your current Web Server license. For every two Windows 2008 R2 Web Server edition licenses, you will receive one Windows Server 2012 Standard edition license. If you have an odd number of Windows 2008 R2 Web Server edition licenses, your grant will be based on rounding up to the next whole even number.  You will continue to have the ability to host web content on your new Windows Server 2012 Standard edition license without needing a Windows Server CAL to access the server, but any other workloads that you decide to run on your new server will follow the standard Windows CAL licensing requirements. | Accurate |
| If I have an HPC edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q25. If I have an HPC edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Windows HPC Server 2008 R2 Suite, you will receive a license grant for Windows Server 2012 Standard edition. For each Windows HPC Server 2008 R2 Suite (which includes both a Windows Server 2008 R2 HPC edition license and Microsoft HPC Pack 2008 R2 Enterprise software) you will receive one Windows Server 2012 Standard edition license.  If you have Software Assurance on Windows Server 2008 R2 HPC edition or Microsoft HPC Pack 2008 R2 Enterprise, you will receive an additional Windows Server 2012 Standard edition that you can use while  also maintaining your rights to run your current HPC licenses. You will receive one Windows Server 2012 Standard edition license for every two Windows Server 2008 R2 HPC edition license or Microsoft HPC Pack 2008 R2 Enterprise licenses you have. If you have an odd number of Windows Server 2008 R2 HPC edition or Microsoft HPC Pack 2008 R2 Enterprise licenses, your grant will be based on rounding up to the next whole number.  You will continue to have the ability to run HPC workloads on your new Windows Server 2012 Standard edition license without needing a Windows Server CAL to access the server, but any other workloads that you decide to run on your new server will follow the standard Windows CAL licensing requirements. | If you have Software Assurance on Windows HPC Server 2008 R2 Suite, you will receive a license grant for Windows Server 2012 Standard edition. For each Windows HPC Server 2008 R2 Suite (which includes both a Windows Server 2008 R2 HPC edition license and Microsoft HPC Pack 2008 R2 Enterprise software) you will receive one Windows Server 2012 Standard edition license.  If you have Software Assurance on Windows Server 2008 R2 HPC edition or Microsoft HPC Pack 2008 R2 Enterprise, you will receive an additional Windows Server 2012 Standard edition that you can use while also maintaining your rights to run your current HPC licenses. You will receive one Windows Server 2012 Standard edition license for every two Windows Server 2008 R2 HPC edition license or Microsoft HPC Pack 2008 R2 Enterprise licenses you have. If you have an odd number of Windows Server 2008 R2 HPC edition or Microsoft HPC Pack 2008 R2 Enterprise licenses, your grant will be based on rounding up to the next whole number.  You will continue to have the ability to run HPC workloads on your new Windows Server 2012 Standard edition license without needing a Windows Server CAL to access the server, but any other workloads that you decide to run on your new server will follow the standard Windows CAL licensing requirements. | Accurate |
| What are my Software Assurance migration rights by Microsoft purchase program? | Q26. What are my Software Assurance migration rights by Microsoft purchase program?  Answer: Each Microsoft purchase program has different rules for your Software Assurance migration entitlement at the end of your enrollment. See the chart below.  The information outlines the Software Assurance benefits available at the time of release for various licensing programs related to Windows Server 2012.  Under the Enterprise Agreement, users receive perpetual rights to the Windows Server 2012 edition. The Enterprise Agreement Subscription allows users to utilize the Windows Server 2012 edition during their enrollment. At the end of enrollment, they can choose to buy out the original Windows Server 2008 R2 product at the original CPS price or the new Windows Server 2012 product at the buy-out price on the published price list. Alternatively, they can renew their enrollment at the new Windows Server 2012 annual subscription price.  The Enrollment for Education Solutions – School Enrollment offers similar terms, allowing use of the Windows Server 2012 edition during enrollment. At the end, users can buy out the original Windows Server 2008 R2 or the new Windows Server 2012 product at the buy-out price, or renew at the new annual subscription price.  Open Value provides perpetual rights to the Windows Server 2012 edition. The Open Value Subscription and Open Value Subscription – Education Solutions both allow use of the Windows Server 2012 edition during enrollment. At the end, users have the option to buy out the original Windows Server 2008 R2 or the new Windows Server 2012 product at the buy-out price, or renew at the new annual subscription price.  Under the Select/Open program, participants are granted perpetual rights to the current edition of Windows Server 2012. This means that once the software is acquired, the user retains the right to use it indefinitely without the need for renewal or additional fees. This assurance is provided at the time of the software's release, ensuring that users have ongoing access to the specific version of the software they have obtained.  Note: The Enrollment for Core Infrastructure (ECI) follows the same rules as stated for the Enterprise Agreement in the chart above. | Each Microsoft purchase program has different rules for your Software Assurance migration entitlement at the end of your enrollment. See the chart below.  The information outlines the Software Assurance benefits available at the time of release for various licensing programs related to Windows Server 2012.  Under the Enterprise Agreement, users receive perpetual rights to the Windows Server 2012 edition. The Enterprise Agreement Subscription allows users to utilize the Windows Server 2012 edition during their enrollment. At the end of enrollment, they can choose to buy out the original Windows Server 2008 R2 product at the original CPS price or the new Windows Server 2012 product at the buy-out price on the published price list. Alternatively, they can renew their enrollment at the new Windows Server 2012 annual subscription price.  The Enrollment for Education Solutions – School Enrollment offers similar terms, allowing use of the Windows Server 2012 edition during enrollment. At the end, users can buy out the original Windows Server 2008 R2 or the new Windows Server 2012 product at the buy-out price, or renew at the new annual subscription price.  Open Value provides perpetual rights to the Windows Server 2012 edition. The Open Value Subscription and Open Value Subscription – Education Solutions both allow use of the Windows Server 2012 edition during enrollment. At the end, users have the option to buy out the original Windows Server 2008 R2 or the new Windows Server 2012 product at the buy-out price, or renew at the new annual subscription price.  Under the Select/Open program, participants are granted perpetual rights to the current edition of Windows Server 2012. This means that once the software is acquired, the user retains the right to use it indefinitely without the need for renewal or additional fees. This assurance is provided at the time of the software's release, ensuring that users have ongoing access to the specific version of the software they have obtained.  Note: The Enrollment for Core Infrastructure (ECI) follows the same rules as stated for the Enterprise Agreement in the chart above. | Accurate |
| How much will Windows Server 2012 Standard and Datacenter editions cost? | Q27. How much will Windows Server 2012 Standard and Datacenter editions cost?  Answer: For your specific pricing, contact your Microsoft reseller. Actual prices may vary. Microsoft does not determine pricing or payment terms for licenses acquired through resellers.  The information provided outlines the estimated retail prices for two different editions under a volume licensing program. The Datacenter edition is priced at $4,809, indicating it is likely designed for larger-scale operations with extensive needs. In contrast, the Standard edition is available for $882, suggesting it is more suitable for smaller-scale or less demanding environments. These prices reflect the cost associated with obtaining licenses through an open, no-level volume licensing agreement, which typically caters to organizations requiring multiple licenses. | For your specific pricing, contact your Microsoft reseller. Actual prices may vary. Microsoft does not determine pricing or payment terms for licenses acquired through resellers.  The information provided outlines the estimated retail prices for two different editions under a volume licensing program. The Datacenter edition is priced at $4,809, indicating it is likely designed for larger-scale operations with extensive needs. In contrast, the Standard edition is available for $882, suggesting it is more suitable for smaller-scale or less demanding environments. These prices reflect the cost associated with obtaining licenses through an open, no-level volume licensing agreement, which typically caters to organizations requiring multiple licenses. | Accurate |
| Can I use my Windows Server 2008 CAL to access Windows Server 2012? | Q28. Can I use my Windows Server 2008 CAL to access Windows Server 2012?  Answer: No. The CAL accessing the instance of Windows Server must be equivalent or higher in version than the server being accessed. You will need a Windows Server 2012 CAL to access a Windows Server 2012 instance. | No. The CAL accessing the instance of Windows Server must be equivalent or higher in version than the server being accessed. You will need a Windows Server 2012 CAL to access a Windows Server 2012 instance. | Accurate |
| Do I still need a separate CAL to access Remote Desktop Services (RDS) and Active Directory Rights Management Service (ADRMS)? | Q29. Do I still need a separate CAL to access Remote Desktop Services (RDS) and Active Directory Rights Management Service (ADRMS)?  Answer: Yes. The licensing requirements for Remote Desktop Services (RDS) and Active Directory Rights Management Service (ADRMS) have not changed with Windows Server 2012. Customers are still required to purchase an ADRMS or RDS CAL in addition to a Windows Server CAL to access ADRMS or RDS functionality. The CAL accessing the instance of Windows Server must be equivalent or higher in version than the server being accessed. | Yes. The licensing requirements for Remote Desktop Services (RDS) and Active Directory Rights Management Service (ADRMS) have not changed with Windows Server 2012. Customers are still required to purchase an ADRMS or RDS CAL in addition to a Windows Server CAL to access ADRMS or RDS functionality. The CAL accessing the instance of Windows Server must be equivalent or higher in version than the server being accessed. | Accurate |
| What is the price of running Windows Server 2012 on Windows Azure under "preview" and "general availability"? | Q30. What is the price of running Windows Server 2012 on Windows Azure under "preview" and "general availability"?  Answer: Windows Server 2012 and Windows Server 2008 R2 will continue to be available on Azure at the same price. | Windows Server 2012 and Windows Server 2008 R2 will continue to be available on Azure at the same price. | Accurate |
| Can I move Windows Server 2012 licenses and images between Hyper-V and Azure? | Q31. Can I move Windows Server 2012 licenses and images between Hyper-V and Azure?  Answer: Windows Server 2012 licenses just like Windows Server 2008 R2 are not eligible for the license mobility benefits under Software Assurance. You can continue to take advantage of the license mobility rights for other server applications, however Windows Server will continue to be purchased separately from the service provider or Azure. | Windows Server 2012 licenses just like Windows Server 2008 R2 are not eligible for the license mobility benefits under Software Assurance. You can continue to take advantage of the license mobility rights for other server applications, however Windows Server will continue to be purchased separately from the service provider or Azure. | Accurate |
| What are the System Center license requirements for managing Windows Server 2012 instances running on Azure? | Q32. What are the System Center license requirements for managing Windows Server 2012 instances running on Azure?  Answer: You can use the License Mobility benefits under Software Assurance to assign your System Center 2012 license to a Windows Server instance running on Azure. | You can use the License Mobility benefits under Software Assurance to assign your System Center 2012 license to a Windows Server instance running on Azure. | Accurate |
| How do I license Windows Server 2012 on ECI to run some instances on Azure? | Q33. How do I license Windows Server 2012 on ECI to run some instances on Azure?  Answer: You are not able to run your ECI Windows Server license in Azure because Windows Server does not offer mobility right as a standalone license or as a component product within the Core Infrastructure Suite product purchased under an ECI enrollment or outside of ECI. | You are not able to run your ECI Windows Server license in Azure because Windows Server does not offer mobility rights as a standalone license or as a component product within the Core Infrastructure Suite product purchased under an ECI enrollment or outside of ECI. (right/right(s)) | Accurate |
| What are my licensing options for a Disaster Recovery server? | Q34. What are my licensing options for a Disaster Recovery server?  Answer: If you are storing virtual machines for future use in a Disaster Recovery situation you will not need additional licensing for that server. Only when you run an instance on that server will a license be required (see the definition of running an instance below). You should be mindful that any of your replicated virtual instances, when running, need to be running on a server appropriately licensed to support that running instance.  Running Instance means an Instance of software that is loaded into memory and for which one or more instructions have been executed. (You "Run an Instance" of software by loading it into memory and executing one or more of its instructions.) Once running, an Instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.  There are two ways in which you can license a server for Disaster Recovery, by purchasing a Windows Server license or by using the Cold Back-up for Disaster Recovery Software Assurance benefit. Cold Back-up for Disaster Recovery allows you to keep a backup server ready for use in case your primary (production) server fails due to earthquakes, floods or any kind of disaster. If a disaster strikes you can immediately switch over to the Cold Disaster Recovery server. In order to utilize this benefit you must comply with the follow terms:  · The software in the Disaster Recovery server should comply with the use rights associated with the software. · The server cannot be in the same cluster as the production server. · The server cannot be turned on except for updates to the software (patching) or testing. The server may of course be turned on in the event of a disaster for Disaster Recovery. · The Disaster Recovery server and the production instances may run concurrently while recovering from a disaster. At all other times the Disaster Recovery server should be switched off except as above  Remember that in order to utilize this Software Assurance benefit, all licenses in use must have active Software Assurance coverage. This includes any CALs required to access the Disaster Recovery server. This benefit ends when Software Assurance coverage on your licenses ends. You can find more information about the use rights for this benefit in the Product Use Rights document. | If you are storing virtual machines for future use in a Disaster Recovery situation you will not need additional licensing for that server. Only when you run an instance on that server will a license be required (see the definition of running an instance below). You should be mindful that any of your replicated virtual instances, when running, need to be running on a server appropriately licensed to support that running instance.  Running Instance means an Instance of software that is loaded into memory and for which one or more instructions have been executed. (You "Run an Instance" of software by loading it into memory and executing one or more of its instructions.) Once running, an Instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.  There are two ways in which you can license a server for Disaster Recovery, by purchasing a Windows Server license or by using the Cold Back-up for Disaster Recovery Software Assurance benefit. Cold Back-up for Disaster Recovery allows you to keep a backup server ready for use in case your primary (production) server fails due to earthquakes, floods or any kind of disaster. If a disaster strikes you can immediately switch over to the Cold Disaster Recovery server. In order to utilize this benefit you must comply with the follow terms:  · The software in the Disaster Recovery server should comply with the use rights associated with the software.  · The server cannot be in the same cluster as the production server.  · The server cannot be turned on except for updates to the software (patching) or testing. The server may of course be turned on in the event of a disaster for Disaster Recovery.  · The Disaster Recovery server and the production instances may run concurrently while recovering from a disaster. At all other times the Disaster Recovery server should be switched off except as above.  Remember that in order to utilize this Software Assurance benefit, all licenses in use must have active Software Assurance coverage. This includes any CALs required to access the Disaster Recovery server. This benefit ends when Software Assurance coverage on your licenses ends. You can find more information about the use rights for this benefit in the Product Use Rights document. | Accurate |
| When will the Windows Server 2012 Licensing changes take place? | Q35. When will the Windows Server 2012 Licensing changes take place?  Answer: Licensing changes will become effective at the general availability of Windows Server 2012, which is expected to be in September 2012. | Licensing changes will become effective at the general availability of Windows Server 2012, which is expected to be in September 2012. | Accurate |
| What support is available for an older version of Windows Server? | Q36. What support is available for an older version of Windows Server?  Answer: See the Windows Server Support Lifecycle website for details. | See the Windows Server Support Lifecycle website for details. | Accurate |
| What is Windows Server 2012 Essentials? | Q37. What is Windows Server 2012 Essentials?  Answer: Windows Server 2012 Essentials is the latest version of Windows Small Business Server Essentials. It is a cloud enabled first server with an intuitive user interface. It can run on physical servers with up to two processors and has been designed for small businesses with up to 25 users. | Windows Server 2012 Essentials is the latest version of Windows Small Business Server Essentials. It is a cloud enabled first server with an intuitive user interface. It can run on physical servers with up to two processors and has been designed for small businesses with up to 25 users. | Accurate |
| What are some of the features that are now available in Windows Server 2012 Essentials? | Q38. What are some of the features that are now available in Windows Server 2012 Essentials?  Windows Server 2012 Essentials incorporates best-of-breed 64-bit product technologies to deliver a server environment well-suited for the vast majority of small businesses. The product technologies include:  · Windows Server 2012 operating system · Data protection · "Anywhere" access · Health monitoring · Workload flexibility · Extensibility · Add-ons for many small business solutions, including a connector to Office 365  Customers can use Windows Server 2012 Essentials as a platform to run critical line-of-business applications and other on-premises workloads. It can also provide an integrated management experience when running cloud-based applications and services, such as email, collaboration, online backup, and more. | Windows Server 2012 Essentials incorporates best-of-breed 64-bit product technologies to deliver a server environment well-suited for the vast majority of small businesses. The product technologies include:  · Windows Server 2012 operating system  · Data protection  · "Anywhere" access  · Health monitoring  · Workload flexibility  · Extensibility  · Add-ons for many small business solutions, including a connector to Office 365  Customers can use Windows Server 2012 Essentials as a platform to run critical line-of-business applications and other on-premises workloads. It can also provide an integrated management experience when running cloud-based applications and services, such as email, collaboration, online backup, and more. | Accurate |
| What are the different editions available with Windows Server 2012 Essentials? | Q39. What are the different editions available with Windows Server 2012 Essentials?  There is only one edition-Windows Server 2012 Essentials. It is a flexible offering that provides a platform for running on-premises or cloud-based workloads. | There is only one edition-Windows Server 2012 Essentials. It is a flexible offering that provides a platform for running on-premises or cloud-based workloads. | Accurate |
| Will there be a next version of Windows Small Business Server 2011 Standard? | Q40. Will there be a next version of Windows Small Business Server 2011 Standard?  No. Windows Small Business Server 2011 Standard, which includes Exchange Server and Windows server component products, will be the final such Windows Server offering. This change is in response to  small business market trends and behavior. The small business computing trends are moving in the direction of cloud computing for applications and services such as email, online back-up and line-of- business tools. | No. Windows Small Business Server 2011 Standard, which includes Exchange Server and Windows server component products, will be the final such Windows Server offering. This change is in response to small business market trends and behavior. The small business computing trends are moving in the direction of cloud computing for applications and services such as email, online back-up and line-of-business tools. | Accurate |
| Will there be a next version of Windows Small Business 2011 Premium Add-on? | Q41. Will there be a next version of Windows Small Business 2011 Premium Add-on?  Answer: No. Windows Small Business Server 2011 Premium Add-on, which includes SQL Server and Windows Server as component products, will be the final such Windows Server offering. | No. Windows Small Business Server 2011 Premium Add-on, which includes SQL Server and Windows Server as component products, will be the final such Windows Server offering. | Accurate |
| If I have Windows Small Business Server 2011 Essentials with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q42. If I have Windows Small Business Server 2011 Essentials with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Small Business Server 2011 Essentials, you will receive one Windows Server 2012 Essentials license.  This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon availability. | If you have Software Assurance on Small Business Server 2011 Essentials, you will receive one Windows Server 2012 Essentials license. This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon availability. | Accurate |
| If I have Windows Small Business Server 2011 Standard edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q43. If I have Windows Small Business Server 2011 Standard edition with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Small Business Server 2011 Standard edition, you will receive two Windows Server 2012 Standard edition license and one Exchange Server Standard 2010 license.  This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon availability. | If you have Software Assurance on Small Business Server 2011 Standard edition, you will receive two Windows Server 2012 Standard edition licenses and one Exchange Server Standard 2010 license. This grant will be reflected upon your agreement renewal; however, you are entitled to use the granted product upon availability. | Accurate |
| If I have Windows Small Business Server 2011 Standard CAL with Software Assurance when Windows Server 2012 is released, what will I be entitled to receive? | Q44. If I have Windows Small Business Server 2011 Standard CAL with Software Assurance when Windows Server 2012 is released, what will I be entitled to receive?  Answer: If you have Software Assurance on Small Business Server 2011 Standard CAL, you will receive one Windows Server 2012 CAL license and one Exchange Server CAL license.  This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon availability. | If you have Software Assurance on Small Business Server 2011 Standard CAL, you will receive one Windows Server 2012 CAL license and one Exchange Server CAL license. This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon availability. | Accurate |
| If I have Windows Small Business Server 2011 Premium Add-on with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive? | Q45. If I have Windows Small Business Server 2011 Premium Add-on with Software Assurance when Windows Server 2012 is released, which edition will I be entitled to receive?  Answer: If you have Software Assurance on Small Business Server 2011 Premium Add-on edition, you will receive one Windows Server 2012 Standard edition license and one SQL Server 2012 Standard edition license.  This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon its availability. | If you have Software Assurance on Small Business Server 2011 Premium Add-on edition, you will receive one Windows Server 2012 Standard edition license and one SQL Server 2012 Standard edition license. This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon its availability. | Accurate |
| If I have Windows Small Business Server 2011 Premium Add-on CAL with Software Assurance when Windows Server 2012 is released, what will I be entitled to receive? | Q46. If I have Windows Small Business Server 2011 Premium Add-on CAL with Software Assurance when Windows Server 2012 is released, what will I be entitled to receive?  Answer: If you have Software Assurance on Small Business Server 2011 Premium Add-on CAL, you will receive one SQL Server 2012 CAL license and one Windows Server 2012 CAL license. This grant will be reflected upon your agreement renewal; however you are entitled to use the granted product upon its availability. | If you have Software Assurance on Small Business Server 2011 Premium Add-on CAL, you will receive one SQL Server 2012 CAL license and one Windows Server 2012 CAL license. This grant will be reflected upon your agreement renewal; however, you are entitled to use the granted product upon its availability. | Accurate |
| How much will Windows Server Essentials cost? | Q47. How much will Windows Server Essentials cost?  Answer: For your specific pricing, contact your Microsoft reseller. Actual prices may vary. Microsoft does not determine pricing or payment terms for licenses acquired through resellers.  The information provided outlines the pricing details for two different editions of a product. The Essentials edition is available for purchase through volume licensing at an estimated retail price of 501 dollars. In contrast, the Foundation edition is not available for direct purchase through volume licensing and is instead offered exclusively through Original Equipment Manufacturer (OEM) channels. This indicates that the Essentials edition is accessible to a broader range of customers, while the Foundation edition is limited to specific hardware manufacturers. | For your specific pricing, contact your Microsoft reseller. Actual prices may vary. Microsoft does not determine pricing or payment terms for licenses acquired through resellers.  The information provided outlines the pricing details for two different editions of a product. The Essentials edition is available for purchase through volume licensing at an estimated retail price of 501 dollars. In contrast, the Foundation edition is not available for direct purchase through volume licensing and is instead offered exclusively through Original Equipment Manufacturer (OEM) channels. This indicates that the Essentials edition is accessible to a broader range of customers, while the Foundation edition is limited to specific hardware manufacturers. | Accurate |
| Are there any licensing changes happening to the Foundation edition as part of Windows Server 2012? | Q48. Are there any licensing changes happening to the Foundation edition as part of Windows Server 2012?  Answer: There are no changes to the Foundation edition licensing or pricing model. To see the full list of features and licensing, go to the Foundation Server 2012 website. | There are no changes to the Foundation edition licensing or pricing model. To see the full list of features and licensing, go to the Foundation Server 2012 website. | Accurate |