



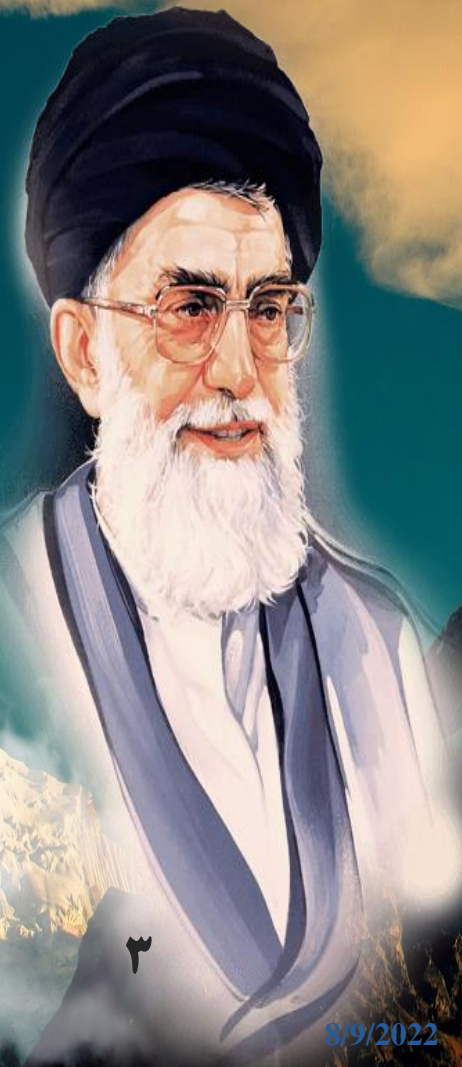
8/9/2022

سرمایه ها و دارائی های سایبری

# بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

8/9/2022

سرمایه گذاری در آیفون های سایبری



انتخاب ملت ایران در مقابل جبهه استکبار «ایستادگی، عدم تسلیم و وابستگی، حفظ استقلال و تقویت درونی نظام و کشور» است.

برای مشرف عادلانه و عمل مثل فقر حرکت به سمت اقتصاد دانش بنیان باید کرد.

مادر جنگ به این نتیجه رسیدیم که باید روی پای خودمان بایستیم

۳  
8/9/2022

سرمایه گذاری های سایبری

# مدیریت سرمایه ها و دارایی ها سایبری

## IT Asset Management (ITAM)

مدیریت پیکربندی

---

# مدیریت دارایی فناوری اطلاعات (ITAM)

❑ تهیه فهرست دارایی‌ها آسان به نظر برسد، اما اطمینان از معتبر و به روز بودن نسخه‌های نرم افزاری و سخت افزاری، چندان ساده نیست.

❑ اینجاست که «مدیریت دارایی فناوری اطلاعات» یا ITAM مطرح می‌شود. امروز به شما خواهیم گفت مدیریت دارایی فناوری اطلاعات (ITAM) چیست و تا چه اندازه برای مدیریت موثر دارایی‌های IT سازمان‌ها ضروری است.



# مدیریت دارایی فناوری اطلاعات (ITAM)

- این سیستم، مجموعه افراد، فرآیندها و ابزارهایی را شامل می‌شود که برای مدیریت و محافظت از دارایی‌های IT یک سازمان ایجاد می‌شوند.
- به بیان دیگر، مدیریت دارایی در فناوری اطلاعات، هر نوع اطلاعات، سیستم یا سخت افزار متعلق به کسب و کار است که در جریان فعالیت‌های تجاری مورد استفاده قرار می‌گیرد. در واقع، دارایی‌ها می‌توانند هم شامل دارایی‌های فیزیکی مانند سخت افزارها و سرورها باشند و هم شامل دارایی‌های غیرفیزیکی مانند نرم افزار، سفارشات خرید و قراردادهای آنها.
- متخصصان از طریق ITAM، سخت‌افزارها و نرم‌افزارهای موجود سازمان را بررسی می‌کنند و تصمیمات جامعی در مورد تمامی جنبه‌های مربوط به چرخه عمر دارایی می‌گیرند.

# مدیریت دارایی فناوری اطلاعات (ITAM)

- فرآیند مدیریت دارایی فناوری اطلاعات، به معنی جمع‌آوری فهرست دقیق و کاملی از سخت افزار، نرم افزار و دارایی‌های سازمان و استفاده از این اطلاعات برای تصمیم‌گیری‌های آگاهانه تجاری در مورد خریدها و توزیع‌های مرتبط با فناوری اطلاعات است.
- می‌توانید ITAM را مجموعه‌ای از شیوه‌های تجاری در نظر بگیرید که عملکردهای مالی، موجودی و قراردادی را برای بهینه‌سازی هزینه‌ها، پشتیبانی از مدیریت چرخه عمر و تصمیم‌گیری‌های استراتژیک، در محیط فناوری اطلاعات ترکیب می‌کند. ITAM معمولاً به عنوان زیرمجموعه‌ای از فرآیند مدیریت خدمات فناوری اطلاعات (ITSM) به شما می‌رود.



# مدیریت دارایی فناوری اطلاعات (ITAM)

- مدیریت دارایی فناوری اطلاعات (ITAM)، فرآیند فهرست نویسی، ردیابی و نگهداری دارایی‌های فناوری یک سازمان است که توانایی ردیابی و تحلیل قطعات مالی و قراردادی را در برابر موجودی واقعی ترکیب می‌کند تا موفقیت خدمات را با درک بهتر نحوه پشتیبانی دارایی‌های فناوری اطلاعات از کسب و کار فراهم کند. این روش به عنوان یک راه‌حل جامع برای موفقیت سازمان به حساب می‌آید.
- این روش، چارچوبی را در اختیارتان قرار می‌دهد تا بتوانید چرخه عمر هر دارایی فناوری اطلاعات را از زمانی که برای اولین بار مورد استفاده قرار می‌گیرد تا زمانی که بازنشسته و از رده خارج می‌شود و همچنین حرکت بین آنها را مستند سازی و مدیریت کنید. یک نرم افزار ITAM، به شما امکان می‌دهد تا به راحتی موجودی سخت افزار و نرم افزار، صاحبان دارایی‌ها، تکالیف و سایر اطلاعات خود را در یک مکان مدیریت کنید.
- برنامه‌های ITAM برای کمک به انجام موفق فرآیند مدیریت دارایی فناوری اطلاعات در دسترس سازمان‌ها قرار می‌گیرد. این روش، قادر است دارایی‌های سخت افزار، نرم افزار و شبکه را در سراسر سازمان شناسایی کرده، سپس داده را ضبط کند و در دسترس قرار دهد.





# اهمیت مدیریت دارایی فناوری اطلاعات

- از آنجا که سیستم ITAM، چیزی فراتر از ایجاد موجودی دارایی است، برای استفاده مداوم از داده‌ها جهت به حداکثر رساندن بازده، به حداقل رساندن ریسک و افزایش ارزش تجاری مورد استفاده قرار می‌گیرد.
- مدیران دارایی فناوری اطلاعات با جلوگیری از خریدهای غیرضروری دارایی و استفاده مطلوب و بهینه از منابع فعلی، می‌توانند هزینه‌های دریافت مجوز و پشتیبانی نرم افزار را کاهش دهند، ضایعات را حذف کنند و کارایی را بهبود ببخشند.
- مدیریت دارایی فناوری اطلاعات (ITAM)، به افزایش درک کسب و کار از ارزش تجاری فناوری اطلاعات کمک می‌کند، درک و ارتباط میان بخش IT و سایر بخش‌ها را بهبود می‌بخشد و قوانین و الزامات نظارتی تایید شده را نیز اعمال می‌کند.
- سیستم ITAM، از طریق پشتیبانی فناوری اطلاعات، بهره‌وری را بهبود می‌بخشد و هزینه‌های سربار مدیریت محیط فناوری اطلاعات را محدود می‌کند.
- مدیریت موثر دارایی‌های فناوری اطلاعات، همچنین می‌تواند دید و کنترل دارایی‌های فناوری اطلاعات را بهبود ببخشد و قطعات مفقود شده سخت افزاری و نرم افزاری را به سرعت شناسایی و جایگزین کند.
- این سیستم قادر است با ارائه اطلاعات دقیق در مورد دارایی‌های تحت تاثیر یک مشکل یا تغییر، از سایر فرآیندهای (ITIL کتابخانه زیرساخت فناوری اطلاعات) پشتیبانی کند.
- ITAM، کسب و کارها را با امکان انتقال سریع‌تر و دقیق‌تر تغییرات در سطح سازمان، چابک‌تر می‌کند.
- داده‌های دارایی و پیکربندی فناوری اطلاعات، در عواقب رویدادها و اتفاقات غیر منتظره بسیار حیاتی و کارآمد است. یک ITAM مناسب می‌تواند به مدیران کمک کند تا تاثیر چنین رویدادهایی را به سرعت شناسایی کرده و برای بازیابی خدمات با اطمینان بیشتری تصمیم‌گیری کنند.

# مزایای مدیریت دارایی فناوری اطلاعات

- ❑ صرفه جویی در هزینه‌ها
- ❑ کاهش ریسک
- ❑ افزایش رضایتمندی مشتریان
- ❑ افزایش کارایی
- ❑ افزایش بهره‌وری

❑ این روزها با دیجیتالی شدن نحوه عملکرد سازمان‌ها و مدیریت مدرن دارایی‌ها، کسب و کارها از اصول **DevOps** و **SRE** استقبال می‌کنند. آنها برای اینکه بتوانند عملکرد و خدمات جدید را به سرعت و بدون احتمال خطر ارائه دهند، به فرایندها و ابزارهای مدیریت دارایی نیاز دارند. با توجه به افزایش اعتماد به سیستم عامل‌ها و خدمات زیرساختی، مدیریت موثر دارایی‌ها می‌تواند سازمان‌ها را قادر به مدیریت مصرف خدمات درخواستی کند. با افزایش امکان کنترل مسئولیت‌های اختصاص داده شده، تیم‌ها می‌توانند ضمن جلوگیری از هزینه‌های غیرضروری، میزان بهره‌وری را افزایش دهند.

- ❑ بهبود استفاده از دارایی‌ها و از رده خارج کردن اموال قدیمی
- ❑ علاوه بر این، کنترل بیشتر، با اعمال سیاست‌های امنیتی و قانونی، ریسک‌ها و تهدیدات را کاهش می‌دهد و در نهایت، به نفع کل سازمان است.

❑ پشتیبانی از روش‌های **ITIL**

# مدیریت دارایی‌ها

- استاندارد ( NIST (National Institute of Standard and technology ) است.  
است.
- داخل این استاندارد چارچوبی به نام ( CSF (Cyber Security Framework ) وجود دارد که به کار بیشتر سازمان‌های متوسط و حتی بزرگ می‌آید. در این چارچوب اولین مرحله‌ای که برای امنیت اطلاعات ذکر شده است ID.AM یا Identify Asset Management به معنای مدیریت دارایی‌ها است.

# مدیریت دارایی‌ها

- داده‌ها، پرسنل، دستگاه‌ها، سیستم‌ها و امکانات سازمان، با توجه به اهمیت نسبی آنها برای اهداف سازمانی، شناسایی و مدیریت می‌شوند.
- تنها راهی که می‌توانید تهدیدات سازمانی خود را تحلیل و خود را ایمن کنید، دانستن وسعت آن تهدیدات است.
- یعنی شما در ابتدا باید بدانید که دقیقاً چه چیزهایی دارید. این دانش به بخش “شناسایی و مدیریت” کمک خواهد کرد.

# مدیریت دارایی ها

- مدیریت دارایی ها IT Asset Management یا (ITAM) یکی از فرآیندهای اصلی در چارچوب ITIL است.
- این فرآیند وظیفه دارد تا اطمینان حاصل کند که دارایی های مورد نیاز برای ارائه سرویس ها به دقت کنترل می شوند و اطلاعات دقیق و قابل اطمینان در خصوص آن دارایی ها نیز در مواقع نیاز، در دسترس هستند.
- این اطلاعات شامل جزئیات مربوط به نحوه پیکربندی دارایی و ارتباطات بین دارایی ها است.

# مدیریت دارایی‌ها

|                  |   |
|------------------|---|
| IDENTIFY<br>(ID) | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy  |
|                  | Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.   |
|                  | Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.   |
|                  | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.   |
|                  | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.  |
|                  | Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. |
|                  |   |

# مدیریت دارایی ها



# فرآیندهای مدیریت فن آوری اطلاعات

- مدیریت تقاضا
- مدیریت امنیت اطلاعات
- مدیریت ظرفیت سرویس (Capacity Management)
- طراحی سرویس (Service Design)
- مدیریت توسعه و نسخه
- مدیریت تغییرات
- انتقال سرویس (Service Transition)
- مدیریت رخدادهای
- مدیریت دانش
- مدیریت پیکربندی و دارایی (IT Asset Management)
- مدیریت رویداد در (Event Management)
- اجرای سرویس (Service Operation)
- مدیریت مشکل (Problem Management)
- مدیریت دسترسی (Access Management)
- بهبود مستمر سرویس (Continual Service Improvement)



# مدیریت پیکربندی و دارایی

□ سرویس‌های IT معمولاً از یک مجموعه Component های مجزا تشکیل شده اند، مانند سرورها، نرم افزار و میان افزار و اطلاعات پیکربندی مخصوص به خود. مدیریت پیکربندی و دارایی در ITIL یا به اختصار SACM در مورد برنامه ریزی دقیق و مدیریت روابط و ویژگی های تمام این اجزاء (Components) در سراسر هریک از سرویس‌های زیرساخت شما می‌باشد.

□ به بیان دیگر، SACM ترکیبی از دو فرآیند مهم است:

❖ مدیریت دارایی که اشاره به دارایی هایی دارد که شما از آنها برای ارائه سرویس‌های IT استفاده می‌کنید.

❖ مدیریت پیکربندی که پیکربندی و ارتباط بین اجزاء مختلف (Components) سرویس‌های متفاوت IT را پیگیری می‌کند.

ITIL *Service Asset and Configuration Management* aims to maintain information about Configuration Items (CIs) required to deliver an IT service, including their relationships

# اهداف مدیریت پیکربندی و دارایی

- SACM در مورد حصول اطمینان از اینکه شما قادر به شناسایی و کنترل تمام دارایی های زیرساخت خود هستید و می توانید از طریق ذخیره، گزارش گیری و حسابرسی موثر، یکپارچگی بین آنها را مدیریت کنید.
- بطور خاص، ITIL اهداف مدیریت پیکربندی و دارایی را این چنین عنوان می کند:
  - اطمینان از اینکه دارایی ها زیر نظر سازمان IT شناسایی، کنترل و به درستی در سراسر چرخه حیات خود محافظت می شوند.
  - شناسایی، کنترل، ذخیره، گزارشگیری، حسابرسی و تایید سرویس ها و سایر آیتم های پیکربندی ((CIS، شامل نسخه ها، مبانی، اجزای سازنده، ویژگی ها و روابط آنها.
  - برای مدیریت و حفاظت از یکپارچگی CI ها در طول چرخه حیات سرویس با استفاده از مدیریت تغییر برای اطمینان از اینکه تنها اجزای مجاز مورد استفاده قرار می گیرند و تنها تغییرات مجاز انجام می شوند.
  - اطمینان از یکپارچگی CI ها و پیکربندی های لازم برای کنترل سرویس ها از طریق ایجاد و نگهداری یک سیستم مدیریت پیکربندی دقیق و کامل (CMS).
  - نگهداری اطلاعات دقیق پیکربندی در مورد وضعیت فعلی، برنامه ریزی شده و وضعیت گذشته سرویس ها و سایر CI ها
  - پشتیبانی مؤثر و کارآمد از فرآیندهای مدیریت سرویس از طریق ارائه اطلاعات دقیق پیکربندی که به مردم امکان می دهد تا بتوانند در زمان مناسب تصمیم گیری کنند. برای مثال، صدور مجوز تغییرات و انتشار نسخه ها، یا برطرف کردن مشکلات و رخدادها.

# مدیریت پیکربندی و دارایی

- ❑ The CMS is used to store information on all Configuration Items (CIs) under the control of Configuration Management.
- ❑ CIs can be of various types: the CMS almost always covers services and IT infrastructure, but might also cover other item types like policies, project documentation, employees, suppliers, etc.
- ❑ The structure of the CMS is defined by the *Configuration Model*, which specifies the types of CIs managed through the CMS, including their attributes and relationships.
- ❑ The Configuration Model is often maintained as a (set of) documents or data models. It also manifests itself, for example, in the table structure of the databases used to store configuration information.

# مدیریت پیکر بندی و دارایی

## CI types and sub-types

- ❑ CI types and sub-types managed in the CMS, usually in the form of a tree structure as in the following example:
  - ❑ Main types (e.g. Service, Hardware, Software, Document, Staff ...)
  - ❑ Sub-types (e.g. Server, Printer, ... - refinement of the main type into sub-types)
  - ❑ ... further sub-types as appropriate

## Attributes

- ❖ (Attributes to be managed for each CI type)

# مدیریت پیکربندی و دارایی

## Status values

- ❑ (allowed status values describing the lifecycle of the CI types)

## Relationships between CI types

- ❑ E.g.
  - ❑ "Is a component of"
  - ❑ "Is associated with"
  - ❑ "Uses"
  - ❑ "Is a new version of"
  - ❑ "Will be replaced by", ...

# مدیریت پیکربندی و دارایی

## ❑ Authorities and controls

- ❑ CI type owner

- ❑ Authorities for creating, authorizing, modifying or deleting the CIs of this type, as appropriate, normally assigned as access rights in the CMS and relevant sub-systems

- ❑ Applicable controls, guidelines and policies (e.g. mechanisms to ensure that only authorized personnel is able to apply changes to the CIs and modify the related CI records in the CMS, or controls/procedures to ensure the configuration data remain consistent when CIs are added or removed)

- ❑ Applicable guidelines and policies

- ❑ Reporting, auditing and verification requirements

# مدیریت پیکربندی و دارایی

## Configuration Item Records - CI Records

□ The details of actual CIs ("instances of CI types") are stored in CI Records. The exact set of attributes to be maintained for a CI will vary depending on the CI type at hand, as specified in the Configuration Model.

❖ *CI Records typically contain the following information:*

❖ Identifier

❖ (Unique identifier - ID)

❖ Name

❖ Description

❖ CI owner

❖ (CI owner/ person in charge)

❖ CI type

# مدیریت پیکربندی و دارایی

- Manufacturer information
  - Manufacturer name
  - Serial number
  - License number/ reference to license contract
- Version information
- Location
  - Physical location, if applicable
  - Logical location, if applicable (e.g. URL or directory on a fileserver)
- Modification history of the CI Record
  - Date of CI Record creation
  - Modifications
    - Date
    - Person in charge
    - Description of modification



# مدیریت پیکربندی و دارایی

## ❑ Status history

- ❑ (description of the life cycle of a CI with status values, as for example "Undergoing Test", ..., "Active", ..., "Undergoing Maintenance", ..., "Out of Operation", ...)
- ❑ Present status and version
- ❑ Status and version history (historical Changes to the status of the CI or Changes planned for the future)
  - ❑ Status change
  - ❑ Description
  - ❑ Time and date of the Change in status

# مدیریت پیگردی و دارایی

- Licensing information
- Document references
  - Contractual documentation
  - Operating documentation
  - User documentation
  - Emergency-relevant documentation
  - Other documentation

# مدیریت پیگردی و دارایی

## References to Configuration Items (CIs) - Note

- ❑ CIs are typically referenced from other service management systems.
- ❑ In an Incident Management system, for example, an Incident Record will contain a reference to one or more affected CIs. So these relationships are recorded in Incident Records rather than the CI records.

# مدیریت پیکربندی و دارایی

Incident Record – Contents - *An Incident Record typically contains the following information:*

- ❖ Unique ID
  - ❖ (Unique ID of the Incident - usually allocated automatically by the system)
- ❖ Date and time of recording
- ❖ Method of notification
  - ❖ (e.g. telephone, e-mail, intranet portal, event monitoring system)
- ❖ Service Desk agent
  - ❖ (If applicable, [Service Desk](#) agent registering the Incident)
- ❖ Caller/ user data
  - ❖ (If applicable, caller/ user contact information)
- ❖ Callback method
- ❖ Description of symptoms
- ❖ Affected users, locations and/ or business areas
- ❖ Affected service(s)

# مدیریت پیکربندی و دارایی

## ❖ Incident priority

❖ Incident Priority, a function of the following components (for further information, refer to the checklist [Incident Prioritization Guideline](#)):

❖ Urgency (available time until the resolution of the Incident)

❖ Impact (damage caused or potential damage to the business or the IT infrastructure)

❖ Priority (for example expressed in priority codes like "Critical", "High", "Medium", "Low", "Very Low"): The result from the combination of urgency and impact

❖ Major Incident flag (to indicate that the Incident is treated as a Major Incident)

## ❖ Relationships to CIs

❖ (Links to primary [Configuration Items \(CIs\)](#) affected by the Incident)

# مدیریت پیکربندی و دارایی

## Incident category

- ❖ Incident category, usually selected from a category-tree according to the following example (Incident categories should be harmonized with Problem categories to support matching between Incidents and Problems):
  - ❖ Hardware error
    - ❖ Server A
      - ❖ Component x
        - ❖ Symptom a
        - ❖ Symptom b
        - ❖ ...
      - ❖ Component y
      - ❖ ...
    - ❖ Server B
    - ❖ ...
  - ❖ Software error
    - ❖ System A
    - ❖ System B
    - ❖ ...
  - ❖ Network error
  - ❖ ...

# مدیریت پیگردی و دارایی

- ❑ Links to related Incident Records
  - ❑ (if a similar outstanding Incident exists, to which the new Incident is able to be attributed)
- ❑ Links to related Problem Records
  - ❑ (Links to related Problem Records - if any outstanding Problems exist, to which the new Incident is able to be attributed)
- ❑ Incident status change history
  - ❑ Date and time
  - ❑ Person in charge
  - ❑ Reason for status change
  - ❑ New Incident status

# مدیریت پیکربندی و دارایی

- ❑ Activity log/ resolution history
  - ❑ Most service desk systems allow maintaining a simple log of steps carried out to resolve the Incident. Some systems, however, also provide the means to assign “Tasks” to Incidents. Akin to the Incidents they are assigned to, Tasks are typically characterized by properties like name, description, owner, priority, etc. and contain a status history and activity log of their own.
- ❑ Closure data
  - ❑ Closure categories (if required, revised product and Incident categorizations)
  - ❑ Problems raised (if the Incident is likely to recur and preventive action is necessary)
  - ❑ Resolution type (elimination of the root cause vs. application of a Workaround; if the Incident was resolved by applying a Workaround: indication of applied Workaround)
  - ❑ Customer feedback (is the Incident resolved from the customer’s/ user’s point of view?)



# مدیریت پیکر بندی و دارایی

## Relationships to other CIs

- ❑ E.g.
  - ❑ "Is a component of"
  - ❑ "Is associated with"
  - ❑ "Uses"
  - ❑ "Is a new version of"
  - ❑ "Will be replaced by", ...
  - ❑ ... including relationships to services supported by the CI.

# آیتم‌های پیکربندی (CI)

- ❑ چرخه حیات CI ها همچون موردها کسب و کار ((business cases, برنامه ریزی های مدیریت سرویس، برنامه ریزی های چرخه حیات سرویس، بسته طراحی سرویس، برنامه ریزی های تغییر و انتشار نسخه و تست طرح های برنامه ریزی شده و سایر موارد.
- ❑ CI های سازمانی (همچون استراتژی کسب و کار سازمان، الزامات قانونی که نیاز به مدیریت دارد و سایر موارد).
- ❑ CI های خارجی همچون توافقات و نیازهای مشتری خارجی،
- ❑ CI های واسط ( Interface CIs) که برای ارائه سرویس کاربر نهایی از طریق واسط فراهم کننده سرویس، مورد نیاز هستند، همچون یک escalation document که مشخص می کند چگونه رخدادها بین دو ارائه دهنده سرویس انتقال می یابد.
- ❑ دارایی های سرویس می تواند هر گونه منابع یا قابلیت هایی باشد که به ارائه یک سرویس کمک می کند. بر خلاف CI ها، که به طور خاص توسط فناوری اطلاعات مدیریت می شود، دارایی های سرویس نمی تواند همیشه توسط فناوری اطلاعات مدیریت شود. به عنوان مثال دانش و اطلاعات یک کارمند فناوری اطلاعات، یک دارایی سرویس محسوب می شود. توانایی کلی یک تیم برای پاسخگویی به یک رخداد یا مشکل نیز یک دارایی سرویس به حساب می آید.

# آیتم‌های پیکربندی (CI)

بطور کلی، دامنه SACM شامل مدیریت کل چرخه حیات هر CI می‌شود، از جمله واسط‌ها گرفته تا ارائه دهندگان خدمات داخلی و خارجی که در آنجا دارایی‌ها و آیتم‌های پیکربندی وجود داشته و نیازمند کنترل هستند.

این نیز برای کسب و کار فوق العاده ارزشمند است. مزیت‌های آن عبارتست از:

- مدیریت بهتر هزینه سرویس‌ها
- بهبود برنامه ریزی و ارائه تغییرات و نسخه‌ها
- رفع مؤثرتر رخدادهای و مشکلات، تحقق بیشتر SLA
- کاهش ریسک‌های مربوط به عدم رعایت استانداردهای مهم قانونی، نظارتی و رویه‌ای

در طول مسیر، مدیریت پیکربندی و دارایی سرویس تقریباً با تمام فرآیندهای فناوری اطلاعات دیگر شما، از جمله مدیریت تغییر، مدیریت مالی، مدیریت رخداد و مشکلات و موارد دیگر، ارتباط برقرار خواهد کرد.

# فعالیت‌های کلیدی SACM

## ۱. برنامه ریزی

□ ITIL توصیه می‌کند تا برای هر یک از سرویس‌هایی که ارائه می‌دهید، یک برنامه مدیریت سرویس (Service Management Plan) ایجاد کنید. این برنامه اساساً یک سند است که به اجزاء مهم یک سرویس پیش از اجرای آن می‌پردازد. معمولاً این برنامه، دامنه و هدف سرویس، فعالیت‌ها و رویه‌های (و حتی نقش‌ها و افراد) مورد نیاز، ارتباط با سایر فرایندها و همچنین ابزارها و CI‌های مورد استفاده را تحت پوشش قرار می‌دهد.

□ برنامه‌های مدیریت خدمات عموماً جزئیات بیشتری را در بر می‌گیرند: مشخص کردن نحوه ارتباط مدیریت فرآیند مدیریت تغییر و فرآیند مدیریت پیکربندی با یکدیگر، نحوه و زمان حسابرسی داده‌های CI و بسیاری موارد دیگر.

# فعالیت‌های کلیدی SACM

## ۲. شناسایی

- این اساسا یک فهرست کامل از تمام CI ها در زیرساخت شما ایجاد می کند. شما قطعا در این فعالیت، هر بیت از اطلاعات مربوط به CI خود که برای عملیات موثر، لازم هستند، از نسخه قطعات سخت افزار یا نرم افزاری گرفته تا همه مستندات، پیکربندی ها، جزئیات مالکیت را ثبت می کنید.
- ویژگی های احتمالی که ممکن است بخواهید ثبت کنید عبارتند از:
  - برای انجام این کار، ITIL توصیه می کند که تمام شناسه های منحصر به فرد CI را (به عنوان مثال، شماره ها) تخصیص داده و همچنین تمام ویژگی های مرتبط با CI از جمله مالک) را ثبت کنید.
  - شناسه منحصر بفرد CI و نوع CI. هر CI باید شماره شناسایی منحصر به فرد داشته باشد تا به راحتی قابل شناسایی باشد.
  - نام و تعریف CI
  - شماره های نسخه، زیرا نسخه های مختلفی از همان CI وجود دارد.
  - اطلاعات مکان و مالک، بنابراین شما می دانید کجا آن را پیدا کنید.
  - وضعیت های فعلی (در مرحله سفارش، در حال تولید و ..).
  - اطلاعات تامین کننده، مستندات مرتبط در صورت لزوم

# فعالیت‌های کلیدی SACM

## ۳. کنترل

- در اینجا، ITIL توصیه می‌کند که تمام CIها از یک فرایند سختگیرانه برای افزودن، تغییر و حذف از CMS یا CMDB خود استفاده کنند. هدف این است که اطمینان حاصل کنید تغییرات از هر نوع بدون پیروی از روال‌های مورد تایید شما برای فرآیندهای متنوعی مانند مدیریت مجوز، مدیریت تغییر، مدیریت نسخه و حتی استقرار رخ نمی‌دهد.
- در طول این فرآیند، شما باید سیاست‌ها و روش‌های خود را برای مواردی مانند کنترل مجوزهای نرم‌افزاری (برای اجتناب از عدم رعایت و جلوگیری از اتلاف مالی)، کنترل دسترسی به امکانات و سیستم‌ها و نحوه ثبت یک خط‌مبنا برای دارایی‌ها و CIهای خود قبل از انتشار، ایجاد کنید تا یک روش دقیق برای تأیید موفقیت عملیات در محیط واقعی در اختیار داشته باشید.

# فعالیت‌های کلیدی SACM

## ۴. اندازه‌گیری وضعیت و گزارش‌گیری

□ ITIL پیشنهاد می‌کند تا در طول چرخه حیات هر CI، وضعیت کامل هر یک از CIها همچون تغییرات پیشنهاد شده، وضعیت تغییرات تایید شده و غیره را ثبت کنید. داشتن قابلیت مشاهده و تهیه گزارش‌ها درک عمیقی از وضعیت فعلی و وضعیت قبلی CIهای شما و حتی قابلیت مشاهده و ارائه گزارش‌های وضعیت، درک عمیقی از وضعیت فعلی و وضعیت قبلی CI به شما می‌دهد و همچنین می‌تواند به شما در تشخیص CIهای غیر مجاز در طول فرآیند کمک کند.

□ گزارش‌ها معمولاً شامل موارد زیر هستند:

□ لیستی از CIها و تنظیمات اولیه آنها

□ فهرستی از CIهای غیرمجاز

□ بروزرسانی‌های انجام شده در تغییرات اخیر یا استثنائات

□ فهرستی از دارایی‌های سخت افزاری و نرم افزاری

# فعالیت‌های کلیدی SACM

## ۵. تایید و حسابرسی

- در هر زمانی باید تضمین شود که داده‌های شما در CIها دقیق و درست هستند. انجام بررسی‌های به موقع و منظم و نیز حسابرسی‌ها امری ضروری بوده و ITIL توصیه می‌کند که آنها را برای جلوگیری از اختلاف بین محیط واقعی خود و نحوه مستندسازی آن، انجام دهید.
- در اصطلاح ITIL، تأییدیه یک فعالیت مداوم است که پیوسته اطمینان حاصل می‌کند CMDB تمام CIها را بطور دقیق نشان می‌دهد. از سوی دیگر، حسابرسی بطور رسمی تر به تایید دقیق بودن رکودها و همچنین فرآیندهای بکار گرفته شده و رعایت شدن استانداردها (از جمله SLA و غیره) می‌پردازد.
- تایید و حسابرسی می‌تواند در هر زمانی و بصورت تصادفی یا بر اساس یک زمانبندی برنامه ریزی شده انجام شود. ابزارهایی نیز برای اتوماسیون این فرآیند در دسترس هستند، برای مثال مقایسه پیکربندی سرورهای طراحی شده با پیکربندی اصلی که شما ثبت کرده‌اید. همچنین حسابرسی‌ها اغلب پیش از تغییرات عمده یا استقرار نسخه‌ها انجام می‌شود تا از وقوع رخداد‌های احتمالی یا اختلال در سرویس جلوگیری کند.



# فعالیت‌های کلیدی SACM

## ۶. مدیریت اطلاعات

- اطمینان از یکپارگی پیکربندی و داده مربوط به دارایی و سیستم‌ها به یک اندازه اهمیت دارد. شما باید به عنوان بخشی از فرآیند مدیریت پیکربندی و دارایی، بطور منظم از CMS بکاپ تهیه کرده و اطلاعات دقیق در مورد نسخه های قدیمی و آرشیو شده CI را نگهداری کنید.
- همچنین باید اقدامات لازم را برای اطمینان از صحت داده ها در سراسر کل چرخه حیات انجام دهید.

# اتوماسیون فرآیندهای مدیریت دارایی ها

- امکان تعریف قواعد گردش کار برای فرآیندهای مدیریت دارایی.
- آگاه سازی خودکار تغییرات و عملیات‌های صورت گرفته بر روی دارایی ها.
- امکان تعریف تاییدیه های خودکار برای تایید درخواست‌ها مطابق با رویه های سازمان.
- با ایجاد قواعد فرم، از مقدار دهی صحیح دارایی ها اطمینان حاصل کنید.

# بهروش های مدیریت دارایی رو با نرم افزار ITSM

- کنترل همه دارایی های IT سازمان رو بدست بگیرید.  
امکان پوشش خودکار شبکه با پروتکل های WMI و SNMP و یا استفاده از ابزار دانا کلاینت (شناسایی همه کامپیوترها، سرورها و تجهیزات شبکه).
- ردیابی دارایی ها در کل چرخه حیات از زمان خرید، تحویل به افراد، ثبت استهلاک و در نهایت خارج کردن از مدار  
امکان ثبت اطلاعات اداری مانند شماره اموال و شماره سریال، مشخص کردن تحویل گیرنده، تعیین واحد سازمانی و تغییر وضعیت دارایی ها
- ایجاد ارتباط بین دارایی و سرویس های فناوری اطلاعات  
استفاده از ماژول CMDB، انواع CI ها، ارتباط CI ها و مشاهده به صورت نمودار  
تار عنکبوتی

# بهروش های مدیریت دارایی رو با نرم افزار ITSM

□ مدیریت دارایی های نرم افزاری

امکان شناسایی نرم افزارهای در حال استفاده بر روی همه سیستم های شبکه و دسته بندی آنها

□ کاهش ریسک مدیریت تغییر در سازمان

یکپارچگی ماژول مدیریت دارایی با ماژول های مدیریت پیکربندی و مدیریت تغییر و اطلاع از تاثیر تغییرات بر روی دارایی ها

□ مشاهده اطلاعات آماری از دارایی ها

داشبوردهای پیش فرض و امکان ایجاد داشبوردهای جدید برای مشاهده تصویر ۳۶۰ درجه از همه دارایی ها در قالب نمودارها و جداول آماری بر اساس شرایط مورد نظر.

# بهروش های مدیریت دارایی رو با نرم افزار ITSM

- گزارش گیری از دارایی ها  
استفاده از گزارش های پیش فرض و یا ایجاد گزارش های جدید در سیستم گزارش ساز پیشرفته
- مشاهده مشخصات سخت افزاری و نرم افزاری سرورها و کامپیوترها در هر زمان  
شناسایی دقیق پیکربندی سخت افزاری سیستم ها مانند پردازشگر، حافظه کارت های شبکه، گرافیک، دیسک، لوازم جانبی مانند پرینترها و بسیاری از اطلاعات جزئی دیگر و مشاهده آنها در هر زمان تنها با یک کلیک
- دسترسی به سوابق تغییرات هر دارایی  
نگه داری تاریخچه تغییرات هر دارایی در طول زمان
- نگهداری دارایی ها  
ارتباط ماژول مدیریت دارایی با ماژول سرویس و نگه داری و امکان تعریف برنامه های سرویس و بازدید دوره ای.
- پشتیبانی آسان تر دارایی ها  
امکان انتخاب دارایی های مرتبط در فرم تیکت توسط کارکنان سازمان با توجه به سطح دسترسی و همچنین دارایی های مرتبط هر فرد یا تیم کاری.

# پوشش شبکه و شناسایی کامپیوترها و تجهیزات شبکه

- به استفاده از سامانه شبکه خودتون رو به صورت دستی و یا زمانبندی شده پوشش کنید.
- پروتکل های WMI و یا SNMP همه تجهیزات شبکه، سرور ها و کامپیوتر ها رو شناسایی و به پایگاه داده اضافه می کند.
- در هر بار پوشش مجدد، تغییرات سخت افزاری و نرم افزاری هر دارایی ردیابی و ثبت می شود و شما از تغییرات صورت گرفته با خبر خواهید شد.
- پوششگر شبکه مشخصات سیستم ها را استخراج و ثبت می کند، کاری که انجام آن به صورت دستی غیر ممکن است. بنابراین با کلیک روی هر دارایی به صورت دقیق پیکربندی سخت افزاری، سیستم عامل و نرم افزار های نصب شده روی هر سیستم رو مشاهده خواهید کرد.

# پویش شبکه و شناسایی کامپیوترها و تجهیزات شبکه

جستجوی تیکت

ذخیره

نحوه تشخیص یکنایی سیستم

بر اساس مشخصات سخت افزاری (BIOS UUID + MACAddress)  بر اساس نام سیستم

انگهی استاندارد  فرم ثبت دارایی

تنظیمات پویش شبکه تنظیمات داناکلاینت

Ping Count  Ping Timeout  ms

تست ارتباط با سیستم های هدف به روش Ping (اکیداً توصیه می شود)

خواندن اطلاعات نرم افزارهای نصب شده (تنها برای پویش از نوع ویندوزی)

خواندن مشخصات مانیتور- کیبورد - موس (تنها برای پویش از نوع ویندوزی)

زمان انتظار برای دریافت پاسخ:  ثانیه

حذف سوابق پویش پس از

# ابزار کلاینت همیشه بروز باشید

- کلاینت یک ابزار سبک و کم حجم است که میتونید اون رو به صورت دستی و یا از طریق اکتیو دایرکتوری، بر روی همه سیستم عامل های ویندوز در شبکه خود نصب کنید.
- این ابزار پس از نصب به صورت خودکار مشخصات سخت افزاری و نرم افزاری سیستم را استخراج کرده و برای سرور ارسال خواهد کرد.
- کلاینت تغییرات سخت افزاری و نرم افزاری سیستم را ردیابی میکند و به صورت منظم به سرور ارسال می کند، بنابراین شما همیشه به مشخصات بروز شده سیستم ها دسترسی خواهید داشت.



# مدیریت چرخه حیات دارایی ها منطبق بر ITIL

- محل قرار گیری و تحویل گیرنده هر یک از دارایی ها رو مشخص کنید.
- اطلاعات اداری مانند شماره اموال و بارکد هر دارایی رو ثبت کنید.
- با کلیک روی نام هر یک از کاربران سازمان، فهرست دارایی های تحویل داده شده به او را مشاهده کنید و در زمان خاتمه همکاری دارایی ها به فرد دیگر و یا به انبار انتقال دهید.
- لیست کاملی از تیکت های ثبت شده مرتبط با هر دارایی را مشاهده کنید و رخداد های تکرار شده مرتبط با آن دارایی را شناسایی کنید و در صورت نیاز اقدامی اساسی صورت دهید.
- دارایی های استهلاک دارایی ها را ثبت کنید و دارایی های فرسوده را از رده خارج کنید.

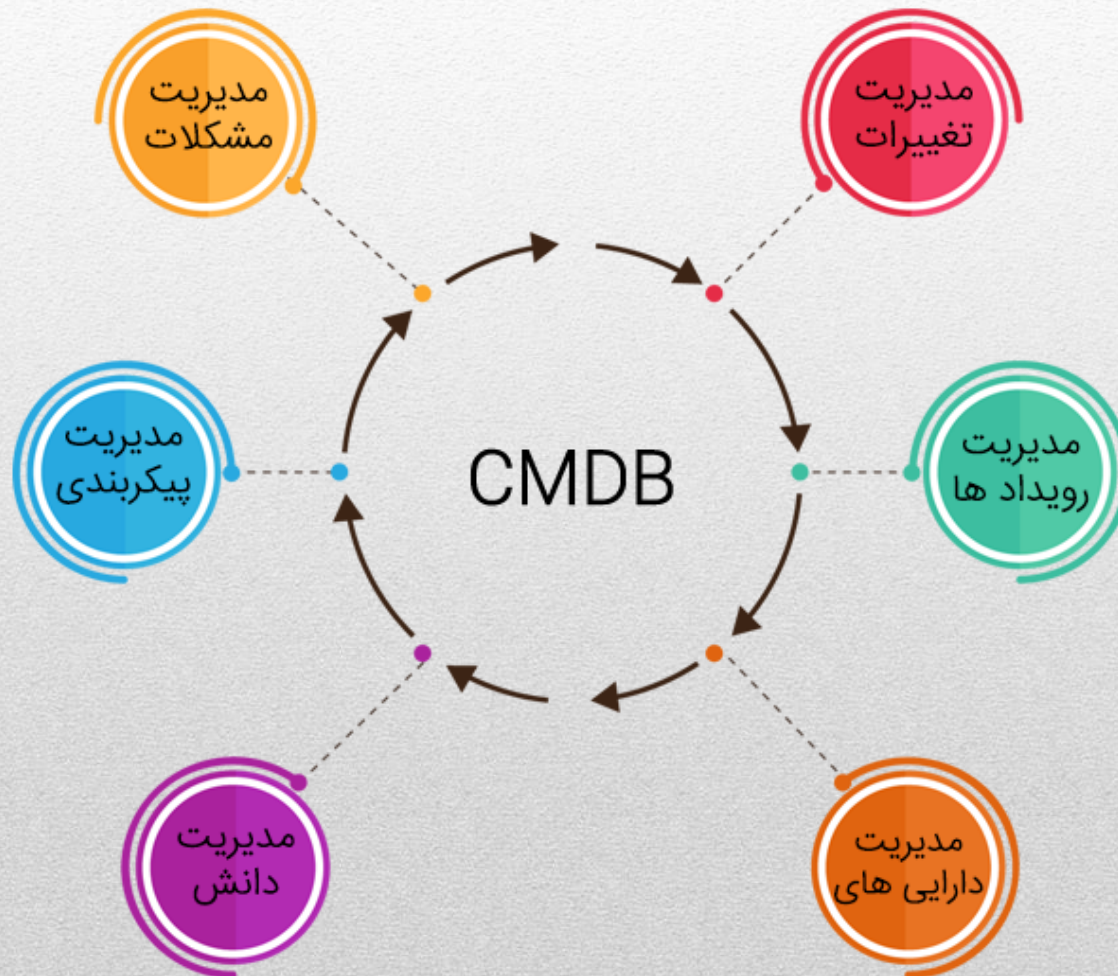
# ماژول CMDB ارتباط دارایی‌ها

- ارتباط دارایی‌ها، افراد و سایر CIها رو در ماژول مدیریت پیکربندی (CMDB) مشخص کنید.
- از انواع ارتباط پیش فرض و یا سفارشی برای ایجاد ارتباط استفاده کنید.
- با ایجاد یک CMDB جامع، فرآیند مدیریت مشکل و مدیریت تغییر رو بهینه کنید.
- با کلیک روی هر CI وابستگی اون به سایر CIها رو به صورت بصری مشاهده کنید.

# ارتباط CMDB با سایر فرآیندهای ITIL

- سیستم CMDB یا مدیریت پیکربندی رو می تونیم پایه‌ای ترین و مهم ترین جزء در چارچوب ITIL به طوری که تقریباً همه فرآیندهای دیگر ITIL به اون وابستگی دارند.
- در نرم افزار یکپارچگی کاملی بین سایر بخش های نرم افزار مثل:
  - مدیریت تغییرات (Change Management)
  - مدیریت مشکلات (Problem Management) و
  - مدیریت رخداد ها (Incident Management) با CMDB وجود داره.

# ارتباط CMDB با سایر فرآیندهای ITIL

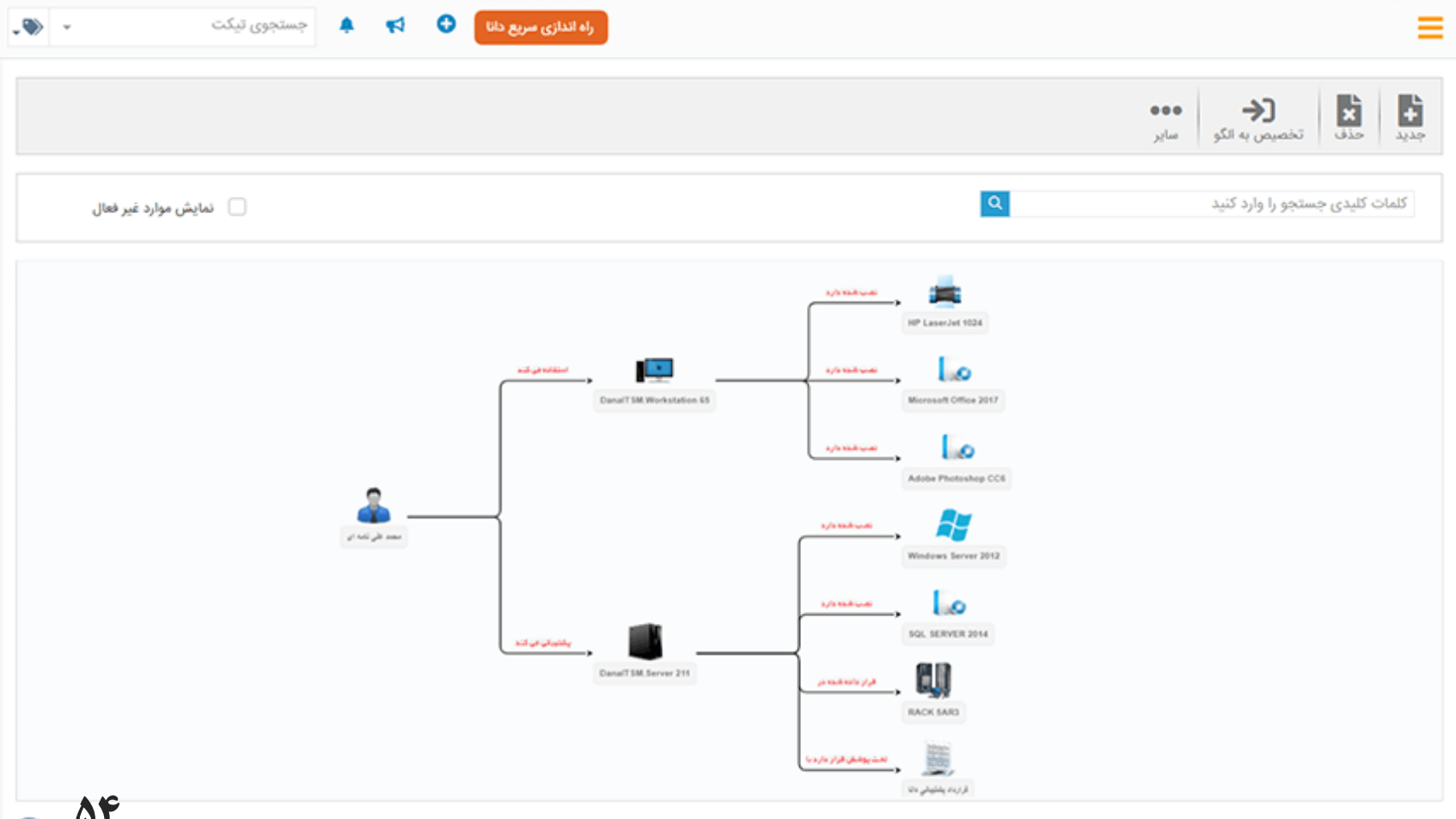


# ارتباط CMDB با سایر فرآیندهای ITIL

□ تصویر ۳۶۰ درجه از ارتباط CI ها

□ ارتباط CI ها رو به صورت یک نقشه تار عنکبوتی نشون میده و با کلیک روی هر CI میتونید به جزئیات بیشتر دسترسی پیدا کنید

# ماژول ارتباط داراییها



## افزایش طول عمر دارایی ها با سرویس و نگه داری پیش گیرانه (IPM)

- یکپارچگی کامل ماژول مدیریت دارایی با ماژول سرویس و نگه داری.
- امکان تعریف برنامه‌های زمانی سرویس یا بازدید دوره ای دارایی ها.
- امکان تعریف دستور کار برای روش انجام سرویس با توجه به نوع دارایی
- گزارش گیری دقیق از روند اجرای برنامه های سرویس و نگه داری.
- ارجاع دستور کارها در زمان مقرر به نیروهای داخلی و یا پیمانکاران.

# تاریخچه تغییرات و سوابق خرابی های هر دارایی

- بسیاری از مشکلات گزارش شده از طرف کاربران معمولاً پس از انجام تغییرات ناصحیح سخت افزار و نرم افزار رخ می دهند، برای مثال ممکنه ارتقاء سخت افزار و یا نصب نرم افزار های ناسازگار موجب بروز اختلال در عملکرد یک کامپیوتر شود. دانا پرو با ثبت دقیق همه تغییرات به شما در شناسایی منشاء اصلی مشکلات ( Root Cause Analysis) کمک میکند.
- علاوه بر این یکپارچگی با زیر سیستم مدیریت رخداد ها ( Incident Management) می کند تا به آسانی به تاریخچه خرابی ها و رخداد های مرتبط با هر دارایی دسترسی داشته باشیم.

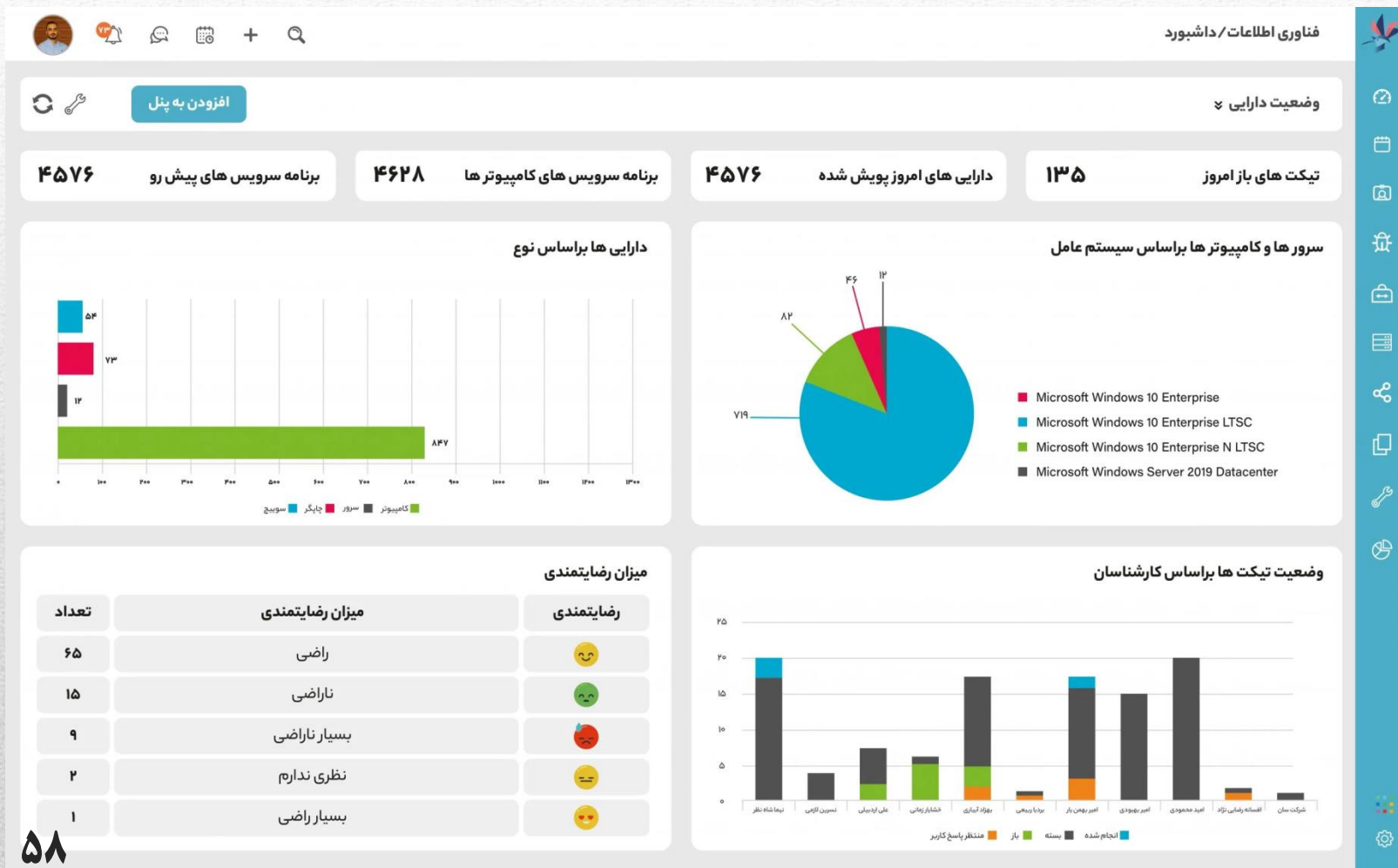


# دسترسی سریع به اطلاعات مورد نیاز

دسترسی به انواع گزارش در قالب نمودارها و فهرست ها، اطلاعات جامع و یکپارچه ای از دارایی های سازمان در اختیار مدیران فناوری اطلاعات و کارشناسان شبکه قرار می دهد که با استفاده از آنها می توان به بسیاری از سوالات به آسانی پاسخ گفت، برای مثال:

- چه تعداد کامپیوتر با RAM کمتر از ۴ GB در سازمان وجود دارد؟
- مشخصات سخت افزاری و منابع سرور اتوماسیون اداری دقیقا چیست؟
- عمر کدام یک از کامپیوترها بیش از ۵ سال است؟
- کامپیوتر و تجهیزات تحویل شده به آقای اربابی در واحد حسابداری کدامند؟
- مهلت اتمام گارانتی کدامیک از کامپیوترها یا تجهیزات در ماه آینده منقضی می شود؟
- بیشتر تیکت ها مربوط به کدام دارایی ها بوده است؟
- بیشتر هزینه های مربوط به دارایی ها برای کدام واحد سازمانی صورت گرفته است؟

# گزارش گیری، تحلیل و مشاهده آمار و اطلاعات دارایی ها



# مدیریت رخداد

- همه ابزار های ضروری و کاربردی برای مدیریت صحیح رخدادها رو در اختیار تیم IT قرار دهید و بهره وری رو به بالاترین نقطه برسونید.
- به کمک ماژول مدیریت رخداد (Incident Management)، همیشه به قواعد SLA وفادار باشید، هزینه ها و قطعی ها رو کاهش دهید و مطابق با بهروش های خدمات ارائه کنید.
-

# مدیریت رخداد

- ❑ بلادرنگ از رخدادهاى جدید با خبر شوید.
- ❑ به قواعد SLA وفادار بمانید و به سرعت و چابک به رخدادها رسیدگی کنید.
- ❑ با اتوماسیون فرآیندها، بار کارى مدیریت رخدادها را تا ۴۰٪ کاهش دهید.
- ❑ چرخه حیات یک رخداد رو به طور کامل و از یک صفحه مدیریت کنید.
- ❑ به کاربران کمک کنید خودشون مشکلاتشون رو رفع کنند.

# اتوماسیون فرآیند گردش کار تیکت ها

- ❑ انتخاب کارشناس مناسب برای تیکت‌های جدید و مطمئن باشید هیچ رخدادی بدون مسئول وجود نداشته، با توجه به مهارت و حجم کاری و زمان حضور افراد، تیکت رو به بهترین کارشناس تخصیص دادن
- ❑ قواعد آگاه سازی خودکار، کاربران رو بلادرنگ از تغییر وضعیت تیکت و روند پیشرفت کارشون باخبر کنید.
- ❑ تعریف قواعد گردش کار، امور روتین مدیریت تیکت‌ها
- ❑ قواعد تأییدیه، روال اخذ مجوز برای انجام برخی از انواع تیکت ها رو اتوماسیون کنید.
- ❑ جلوگیری از تیکت های تکراری، بستن خودکار تیکت ها

# تیکتینگ با سایر نرم افزار های سازمان یکپارچه

- به کمک واسط برنامه نویسی (REST APIs) به سایر نرم افزارها و پورتال های سازمان متصل کنید و امکان ثبت و دریافت تیکت ها رو از طریق اونها فراهم کنید.
- به کمک ابزار اسکریپت نویسی داینامیک، اکشن های جدید بنویسید، API ها و وب سرویس های دیگر رو فراخوانی کنید
- به سیستم های پر کاربرد دیگر متصل کنید برای مثال، Active Directory, Jira, DevOps, SMS Services.

# روش های ثبت رخداده

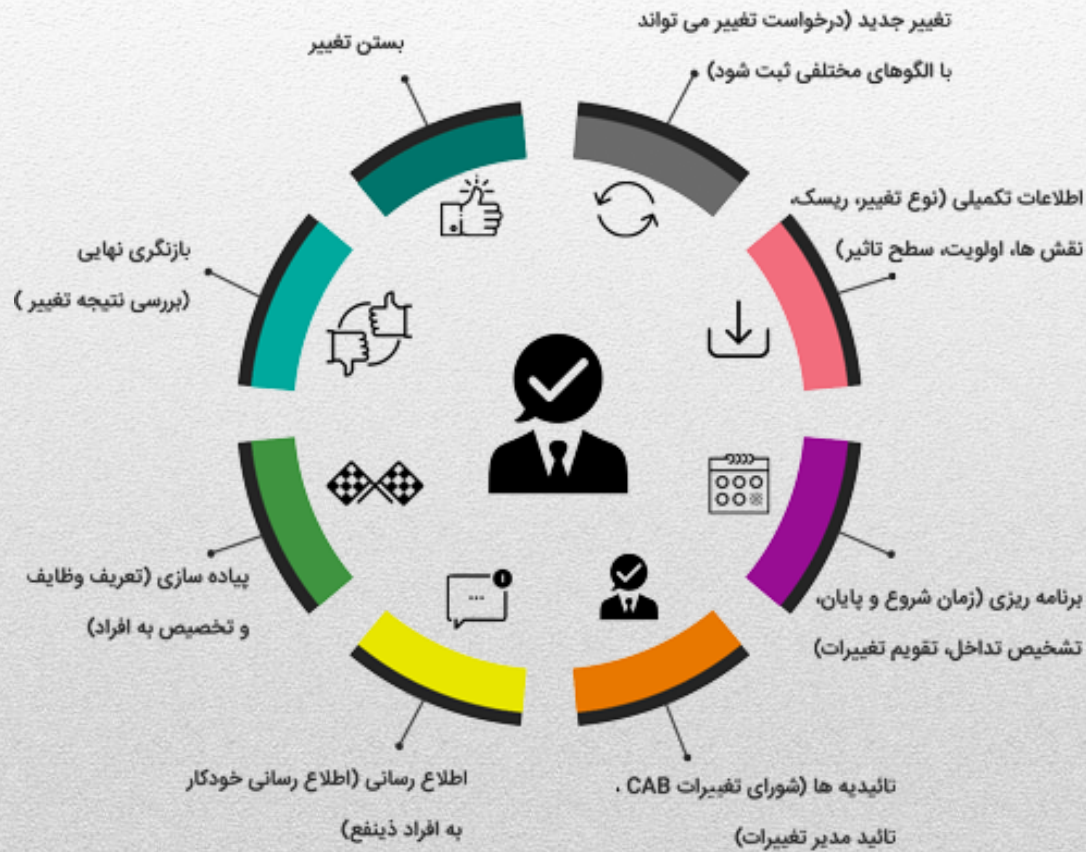
- ❑ به کارکنان سازمان اجازه بدید به روش دلخواه خودشون رخداد (تیکت) ثبت کنند مثل پورتال کاربران، ایمیل، چت آنلاین، تلفن و یا با تلفن همراه.
- ❑ با اتصال نرم افزار های مانیتورینگ شبکه به، بلادرنگ از بروز اختلال در شبکه با خبر شوید.
- ❑ مهم نیست که رخدادها از کدوم روش ثبت میشوند، شما همیشه اونها رو در یک صفحه به صورت متمرکز خواهید دید.
- ❑ همه ایمیل های دریافتی به آدرس مشخص شده رو به تیکت تبدیل می کنه.
- ❑ اگر ماژول چت آنلاین رو فعال کنید، علاوه بر پشتیبانی آنلاین در صورت نیاز میتونید برای کاربر تیکت ایجاد کنید.
- ❑ با اتصال به سیستم تلفنی سازمان، علاوه بر مشاهده اطلاعات تماس ورودی، همه مکالمات رکورد خواهد شد و بهره وری به طور قابل ملاحظه ای افزایش پیدا خواهد کرد.

# فرآیند مدیریت تغییر

- در ITIL هدف اصلی فرآیند مدیریت تغییر، کاهش ریسک و اثرات منفی ایجاد تغییر در زیر ساخت فناوری اطلاعات است. منظور از تغییر، حذف و اضافه یا تغییر هر چیزیه که ممکنه بر سرویس های IT سازمان تاثیر داشته باشه.
- با توجه به اینکه امروزه، تقریباً همه خدمات و عملیات های یک سازمان به سرویس های IT متکی است، هر گونه تغییر ممکن است منجر به بروز اختلال در عملکرد سرویس های IT و در نتیجه ایجاد وقفه در کسب و کار سازمان شود.
- ماژول مدیریت تغییر در نرم افزار ITSM پرو به شما کمک می کنه با پیاده سازی فرآیند تغییر توصیه شده ITIL، ریسک تغییرات رو به حداقل برسونید.



# فرآیند مدیریت تغییر



# مراحل مدیریت تغییر

- ماژول مدیریت تغییر (Change Management)، به صورت پیش فرض همه مراحل توصیه شده در چرخه حیات یک تغییر رو در اختیارتون قرار میده
- برای مثال درخواست تغییر، برنامه ریزی، تایید تغییر، پیاده سازی، بازنگری نهایی و در نهایت بستن تغییر.

# مراحل مدیریت تغییر

جستجوی تیکت

چاپ مشاهده تاریخچه بازگشت حذف ذخیره

مدیر تغییر: آرزو زارعی

نوع تغییر: اضطراری

وضعیت: برنامه ریزی

ریسک: کم

شماره تغییر: ۰۰۰۰۰۱

درخواست کننده تغییر: مدیر سیستم

بسته پیاده سازی تأییدیه برنامه ریزی

جدید برنامه ریزی پیاده سازی بازنگری و بستن

مشخصات درخواست تغییر

موضوع: تعویض رم سرور S-۲۲۸

توضیحات: به علت اختلال در رم سرور اس-۲۲۸ می بایست این رم به صورت فیزیکی در سرور تعویض گردد.

|               |               |                    |                    |
|---------------|---------------|--------------------|--------------------|
| شماره تغییر   | ۰۰۰۰۰۱        | نوع تغییر          | اضطراری            |
| علت تغییر     | تعمیرات       | ریسک               | کم                 |
| اولویت        | بحرانی        | سطح تاثیر          | تاثیر بر کل سازمان |
| گروه          | سخت افزار     | دپارتمان تحت تاثیر | محصول              |
| شورای تغییرات | پشتیبانی بینا | وضعیت              | برنامه ریزی        |

# برنامه ریزی برای جلوگیری از تداخل تغییرات

□ با برنامه ریزی صحیح ، از بروز تداخل تغییرات جلوگیری کنید

□ همه تغییرات فناوری اطلاعات باید به درستی برنامه ریزی بشه تا از نظر زمانی تداخلی با سایر تغییرات ایجاد نشه. ممکنه منابع انسانی مورد نیاز برای انجام و مدیریت تغییرات و یا CI های تحت تاثیر تغییر در بازه زمانی مورد نظر، در تغییر دیگری درگیر باشند، بنابراین باید راهکاری برای تعیین بهترین زمان برای انجام تغییر در دسترس باشد.

□ زیر سیستم مدیریت تغییر دانا، مکانیسمی تحت عنوان تشخیص تداخل داره که از بروز تداخل در برنامه ریزی تغییرات جلوگیری می کنه، همچنین به کمک تقویم تغییرات دانا می تونید به آسونی همه تغییرات برنامه ریزی شده رو مشاهده کنید.

# برنامه ریزی برای جلوگیری از تداخل تغییرات

جستجوی تیکت

چاپ مشاهده تاریخچه بازگشت حذف ذخیره

مدیر تغییر: آرزو زارعی

نوع تغییر: اضطراری

وضعیت: تأییدیه

ریسک: کم

شماره تغییر: ۰۰۰۰۰۱

درخواست کننده تغییر: مدیر سیستم

بسته پیاده سازی تأییدیه

جدید برنامه ریزی پیاده سازی بازنگری و بستن

|                      |             |                      |            |
|----------------------|-------------|----------------------|------------|
| مشاهده تقویم تغییرات | تشخیص تداخل | ۱۳۹۸/۰۳/۰۸ ۱۱:۰۳:۲۲  | زمان شروع  |
|                      |             | ۱۳۹۸/۰۳/۱۱ ۱۱:۰۳:۲۲  | زمان پایان |
|                      |             | خرابی رم سرور اس-۲۲۸ | توجه تغییر |

تأثیرات تغییر: بهبود سرعت و عملکرد رم و کلیه ماشین های مجازی روی سرور

# اتوماسیون فرآیند تایید درخواست‌های تغییر

- برای انجام برخی از تغییرات، لازم هستش با افراد ذینفع و یا متخصص در حوزه مربوطه مشورت بشه. به گروهی از افرادی که به تصمیم‌گیری در مورد تغییر کمک می‌کنند، شورای تغییرات (Change Advisory Board – CAB) گفته میشه. در نرم افزار شما می‌تونید چند تیم CAB ایجاد کنید و افراد ذینفع رو در اون تیم‌ها اضافه کنید.
- شما می‌تونید الزام کنید که برخی از درخواست‌های تغییر باید به تایید همه افراد تیم CAB مربوطه برسه و روش ارسال تاییدیه مثلاً به صورت موازی و یا به ترتیب رو مشخص کنید، در این حالت کل فرآیند تایید هم به صورت خودکار انجام میشه و شما با کلیک بر روی درخواست تغییر از وضعیت تاییدیه‌های اون باخبر میشید.

# سیستم مدیریت تغییرات

□ ریسک تغییرات رو به حداقل برسونید

□ فرآیند استاندارد اعمال تغییرات را منطبق با چارچوب ITIL در سازمان خود پیاده سازی کنید و همه مراحل تغییر شامل درخواست تغییر، ارزیابی ریسک، برنامه ریزی، تأیید و پیاده سازی رو بر اساس بهروش ها پیاده سازی کنید.

□ کاهش ریسک و تاثیر تغییرات بر عملکرد سازمان

□ حصول اطمینان از اینکه همه تغییرات ثبت و طبق فرآیند استاندارد ITIL انجام می شوند

□ مشارکت آسان افراد ذینفع در ارزیابی و اظهار نظر برای انجام و مدیریت تغییرات.

□ یکپارچگی کامل با سایر زیر سیستم های ITIL مانند CMDB و Incident

Management

□ امکان تعریف فرآیند تغییرات متناسب با نیاز های سازمان

# مدیریت امنیت اطلاعات

- فناوری اطلاعات باید قادر باشد به کسب و کارها جهت مدیریت ریسک، تضمین اینکه منابع به شیوه ای درست استفاده شده و در برابر تهدیدات یا ضررهای احتمالی محافظت می شوند، کمک کند.
- همراستا کردن IT با امنیت کسب و کار و اطمینان از مدیریت مؤثر امنیت اطلاعات در همه فعالیت های مدیریت سرویس و سرویس.
- اهداف مدیریت امنیت اطلاعات، تضمین موارد زیر است:
  - اطلاعات در مواقع نیاز، در دسترس و قابل استفاده باشد و سیستمی که این اطلاعات را فراهم می کند، قادر باشد در برابر حملات مقاومت کرده و بعد از خرابی recover شده یا از وقوع خرابی جلوگیری کند. (Availability).
  - اطلاعات، کامل و دقیق باشد و در برابر تغییرات غیر مجاز از آنها محافظت شود.
  - معاملات تجاری، همچنین تبادل اطلاعات بین شرکتها یا شرکای تجاری مورد اعتماد باشد (صحت اطلاعات و عدم انکار).



# سیستم مدیریت امنیت اطلاعات

- طراحی، پیاده سازی، مدیریت، نگهداری و اجرای فرآیندهای امنیت اطلاعات و کنترل ها
- “هدف قراردادن امنیت The Four P’s است:
- مردم (People)
- فرآیند (Process)
- محصولات (Products)
- شرکا و تولیدکنندگان (Partners)

# سیستم مدیریت امنیت اطلاعات

چارچوب ISMS شامل پنج عنصر اصلی به شرح زیر است:

## ۱. کنترل

شما باید یک چارچوب مدیریتی جهت مدیریت امنیت اطلاعات، تهیه و پیاده سازی سیاست‌های امنیت اطلاعات، تخصیص مسئولیت‌ها و جمع آوری و کنترل اسناد، ایجاد کنید.

## ۲. برنامه ریزی

در مرحله برنامه ریزی از چارچوب تعیین شده، شما مسئول جمع آوری و درک کامل نیازهای امنیتی سازمان بوده و پس از آن باید اقدامات مناسبی را بر اساس بودجه، فرهنگ سازمانی در خصوص امنیت و سایر فاکتورها پیشنهاد دهید.

## ۳. اجرا

سپس، شما طرح برنامه ریزی شده را اجرا کرده و اطمینان حاصل کنید که دارای مکانی ایمن برای اجرای درست سیاست‌های امنیت اطلاعات در این فرآیند هستید.

# سیستم مدیریت امنیت اطلاعات

۴. ارزیابی

هنگامی که سیاست‌ها و برنامه‌های شما آماده اجرا هستند، باید با نظارت درست بر آنها اطمینان حاصل کنید که سیستم‌های شما واقعا امن هستند و فرایندهای شما مطابق با سیاست‌ها، SLAها و دیگر نیازهای امنیتی شما اجرا می‌شوند

۵. نگهداری

در نهایت یک ISMS موثر به معنای آن است که شما به طور مداوم تمام فرآیند را بهبود بخشیده و به دنبال فرصت‌هایی برای بازبینی SLAها، توافق‌نامه‌های امنیتی، نحوه نظارت و کنترل آنها و موارد دیگر هستید.

یک سیستم اطلاعاتی مدیریت امنیت (SMIS) به سادگی یک ابزار یا مخزن است که اطلاعاتی را که از شیوه‌های مدیریت امنیت اطلاعات شما پشتیبانی می‌کند، ذخیره می‌کند. این بخشی از کل سیستم مدیریت دانش سرویس (SKMS) است. در نهایت SMIS باید به عنوان یک مکان اصلی برای ذخیره چیزهایی مانند برنامه‌ها و سیاست‌های امنیتی شما، همچنین تمام اسناد مربوطه، ارزیابی‌ها و برنامه‌های عملی، در نظر گرفته شود.

# ۱۱ کار مهم مدیریت دارایی ها

- ۱- اهداف و استراتژی اجرای خود را تشریح کنید
- ۲- تیمی را برای مدیریت تجهیزات دارایی IT خود ایجاد کنید
- ۳- برنامه ای برای جمع آوری داده های دارایی ایجاد کنید
- ۴- کاربران را به دارایی های خود پیوند دهید
- ۵- وضعیت دارایی های سخت افزاری را بررسی کنید
- ۶- با داشبورد شخصی سازی کنید
- ۷- مدیریت سرویس IT و ITAM را متحد کنید
- ۸- مدیریت و پاسخ به خطرات
- ۹- بازگشت سرمایه (ROI) در مدیریت دارایی را اندازه گیری کنید
- ۱۰- افزودن داده های قرارداد و گارانتی
- ۱۱- بهترین راهکارهای ITAM 4 ITIL را اجرا کنید

# IT ASSET MANAGEMENT

THEN



NOW



## Dashboard

DEMO MODE: Some features are disabled for this installation.

105

total assets

More info

10

total licenses

More info

15

total accessories

More info

24

total consumables

More info

### Recent Activity

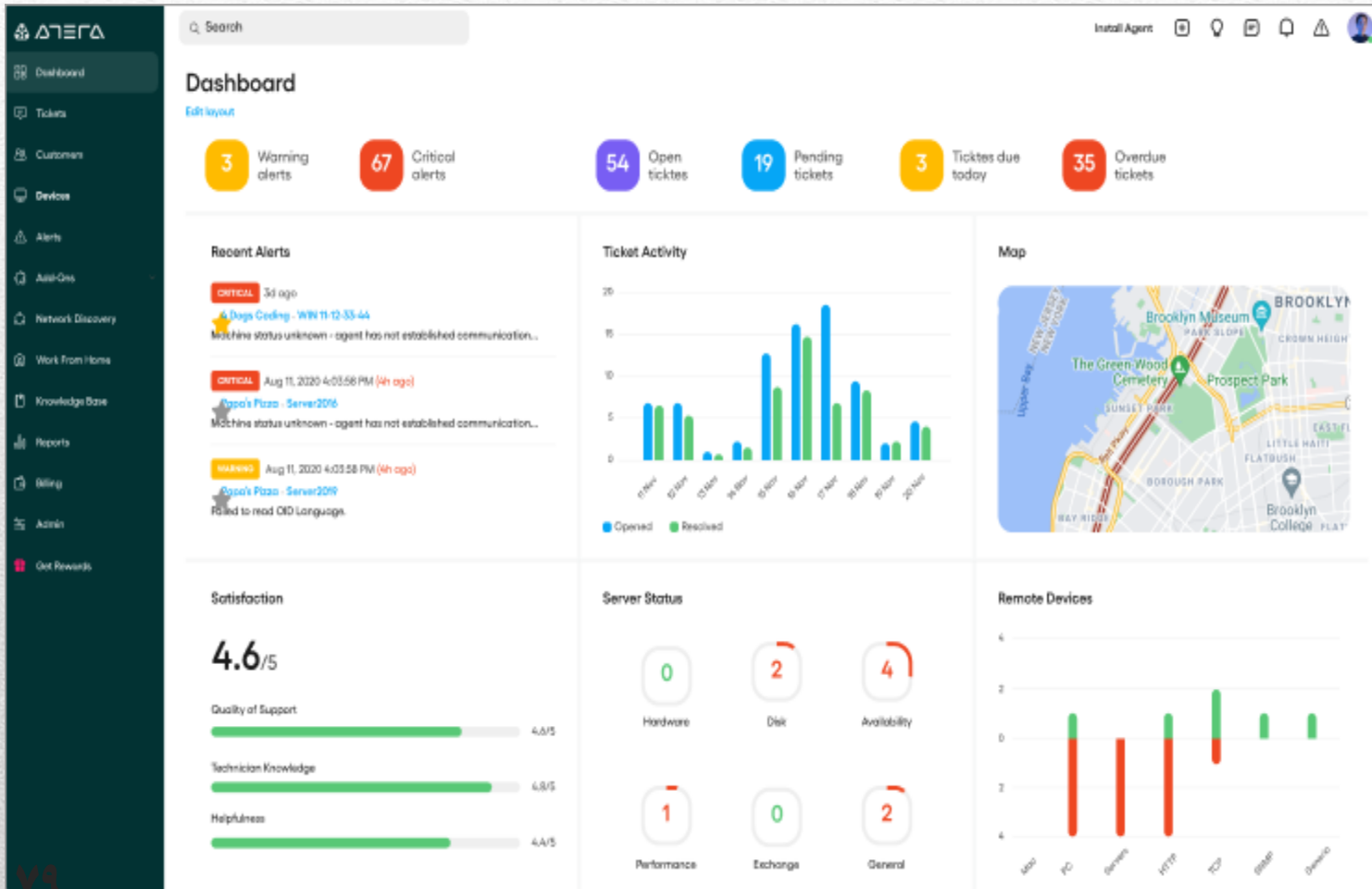
| Date                 | Admin         | Action       | Item                      | To                            |
|----------------------|---------------|--------------|---------------------------|-------------------------------|
| Jul 06, 2017 2:29AM  | Admin Account | checkout     | Voluptas cupiditate       | Secured clear-thinking policy |
| Jul 06, 2017 1:55AM  | Admin Account | checkin      | 000994810341123 - test    | 1233                          |
| Jul 06, 2017 1:55AM  | Admin Account | item created | 000994810341123 - test    |                               |
| Jul 06, 2017 1:55AM  | Admin Account | checkout     | 000994810341123 - test    | 1233                          |
| Jul 06, 2017 1:09AM  | Admin Account | item created | 0009948103411231 - Laptop |                               |
| Jul 06, 2017 1:02AM  | Admin Account | deleted      | Doloremque et             |                               |
| Jul 06, 2017 12:51AM |               | requested    | 023 - 001 (023)           | juv jo                        |
| Jul 06, 2017 12:51AM | sss ddd       | item created | 023 - 001 (023)           |                               |
| Jul 06, 2017 12:50AM | Admin Account | update       | Velit itaque sed.         |                               |

### Assets

Ready to Deploy Pending  
WIP Deployed



# #4) Atera





# True network visibility and control. In under an hour.

Auvik is cloud-based network management software



START FOR FREE





# Asset Management Software

- #1) NinjaOne (Formerly NinjaRMM)
- #2) SuperOps.ai
- #3) Freshservice
- #4) Atera
- #5) Auvik
- #6) Nifty
- #7) xAssets IT Asset Management Software
- #8) AssetExplorer
- #9) Spiceworks IT Asset Management Software
- #10) Snipe-IT
- #11) Asset Panda
- #12) GoCodes
- #13) EZOfficeInventory
- #14) Samanage
- #15) AssetCloud
- #16) InvGate Assets

با تشکر از توجه شما

اللهم صل على محمد وآل محمد