SERVICE DESIGN (ITIL)

Service Design is a stage of the ITIL service lifecycle that focuses on **designing new IT services or modifying existing services** so that they meet **current and future business requirements**. It ensures that services are **efficient, secure, reliable, and cost-effective** throughout their lifecycle.

---

1. Design of Architecture, Processes, Policies, Documentation, and Allowing for Future Business Requirements

Design of Architecture

Service architecture defines the **technical structure** of an IT service. It includes hardware, software, network components, and integration methods. A well-designed architecture ensures **high availability, scalability, performance, and security**.

Design of Processes

Processes define **how services are delivered and supported**. Service Design ensures that processes such as incident management, change management, and capacity management are clearly defined, efficient, and aligned with business goals.

Design of Policies

Policies provide **rules and guidelines** that govern service usage, security, compliance, and operational behavior. Proper policies ensure consistency, accountability, and regulatory compliance.

Design of Documentation

Documentation includes:

- Service descriptions
- Operating procedures
- Support manuals
- Escalation guidelines
  Clear documentation ensures smooth service operation, knowledge transfer, and reduced dependency on individuals.

Allowing for Future Business Requirements

Service Design must consider:

- Business growth
- New technologies
- Changing customer demands
  Designing with scalability and flexibility ensures services remain useful over time.

---

2. Service Design Package (SDP)

The **Service Design Package (SDP)** is a comprehensive document that describes **all aspects of a service design**. It acts as a blueprint for service transition and operation.

Contents of SDP

- Service objectives and requirements
- Architecture and infrastructure design
- Service level targets
- Capacity and availability plans
- Security and continuity requirements
- Operational and support processes

Importance of SDP

- Ensures consistent service implementation
- Reduces risks during transition
- Improves communication among stakeholders

---

3. Service Catalog Management

Service catalog management ensures that **accurate and up-to-date information about all live IT services** is available to customers and stakeholders.

Service Catalog

The service catalog contains:

- Service descriptions
- Service availability
- Pricing (if applicable)
- Support and contact details

Objectives

- Improve service visibility
- Enable informed customer decisions
- Support service request handling

Benefits

- Improved transparency
- Better customer satisfaction
- Efficient service delivery

---

4. Service Level Management

Service Level Management (SLM) ensures that **IT services meet agreed business expectations**.

Key Elements

- Service Level Agreements (SLAs)
- Operational Level Agreements (OLAs)
- Underpinning Contracts (UCs)

Activities

- Defining service level requirements
- Monitoring service performance
- Reporting service achievements
- Identifying improvement opportunities

Importance

SLM aligns IT performance with business needs and ensures accountability for service quality.

---

5. Designing for Capacity Management

Capacity Management ensures that **IT infrastructure and services can meet current and future demand** in a cost-effective manner.

Objectives

- Prevent performance issues
- Optimize resource usage
- Plan for future growth

Types of Capacity Management

- **Business Capacity Management:** aligns IT capacity with business needs
- **Service Capacity Management:** focuses on service performance
- **Component Capacity Management:** manages individual infrastructure components

Benefits

- Improved performance
- Cost control
- Better planning and forecasting

---

6. IT Service Continuity Management (ITSCM)

IT Service Continuity Management ensures that **IT services can be recovered quickly after disruptions**.

Objectives

- Minimize business impact
- Support business continuity
- Protect critical services

Key Activities

- Risk assessment
- Business impact analysis (BIA)
- Disaster recovery planning
- Regular testing and review

Importance

ITSCM ensures business operations can continue even during major incidents or disasters.

---

7. Information Security Management

Information Security Management ensures the **confidentiality, integrity, and availability (CIA)** of information and IT services.

Objectives

- Protect sensitive data
- Prevent unauthorized access
- Ensure data accuracy and availability
- Comply with legal and regulatory requirements

Key Components

- Access control
- Authentication and authorization
- Encryption
- Security monitoring and audits
- Incident response

Importance

Information security protects organizational assets, builds customer trust, and reduces risk.

SERVICE TRANSITION (ITIL)

Service Transition is a phase of the ITIL service lifecycle that focuses on **planning, building, testing, and deploying new or changed services** into the live environment. The main objective is to ensure that **changes to services are introduced with minimal risk and disruption**, while maintaining service quality and business continuity.

---

1. Service Asset and Configuration Management (SACM)

Definition

Service Asset and Configuration Management is the process responsible for **identifying, controlling, recording, and verifying service assets and configuration items (CIs)** throughout their lifecycle.

Purpose

SACM ensures that **accurate and reliable information** about IT assets and configurations is available when needed to support other service management processes.

Key Components

- **Service Assets:** Resources and capabilities that contribute to service delivery.
- **Configuration Items (CIs):** Components such as hardware, software, documentation, and people that must be managed.
- **Configuration Management System (CMS):** Repository that stores CI information and relationships.

Activities

- Planning and management
- Configuration identification
- Configuration control
- Status accounting
- Verification and audit

Benefits

- Improved change control
- Reduced service disruption
- Better impact analysis and troubleshooting

---

2. Transition Planning and Support

Definition

Transition Planning and Support coordinates **resources, schedules, and activities** required to move new or changed services into production.

Purpose

The purpose is to ensure that **service transitions are planned, controlled, and efficient**, minimizing risks to ongoing operations.

Key Activities

- Developing transition strategies
- Planning timelines and resources
- Risk assessment and mitigation
- Coordination between stakeholders

Importance

This process ensures consistency across multiple service transitions and avoids conflicts between simultaneous changes.

---

3. Release and Deployment Management

Definition

Release and Deployment Management ensures that **new or changed services are built, tested, and deployed successfully** into the live environment.

Purpose

The objective is to deliver service releases that meet customer expectations and business requirements with minimal disruption.

Key Concepts

- **Release Unit:** A set of components released together.
- **Deployment:** Installation and activation of releases.

Activities

- Release planning
- Build and test
- Deployment
- Early life support
- Review and closure

Benefits

- Reduced deployment risks
- Improved service quality
- Faster time to value

---

4. Change Management

Definition

Change Management controls the **lifecycle of all changes** to minimize the risk of disruptions to IT services.

Purpose

To ensure that **only authorized, evaluated, and tested changes** are implemented.

Types of Changes

- **Standard Change:** Pre-approved and low risk
- **Normal Change:** Requires assessment and approval
- **Emergency Change:** Implemented urgently to restore service

Activities

- Change logging and categorization
- Impact and risk assessment
- Change authorization
- Change implementation
- Review and closure

Benefits

- Reduced incidents caused by change
- Improved service stability
- Better governance and compliance

---

5. Knowledge Management

Definition

Knowledge Management ensures that **useful information and knowledge** are captured, stored, shared, and used effectively.

Purpose

To enable informed decision-making, improve efficiency, and reduce dependency on individuals.

Knowledge Management System

- Known Error Database
- Service documentation
- Best practices and lessons learned

Activities

- Knowledge creation
- Knowledge storage
- Knowledge sharing
- Knowledge utilization

Benefits

- Faster incident resolution
- Improved service quality
- Better staff productivity

---

6. Key Roles of Staff in Service Transition

Change Manager

Responsible for controlling and coordinating changes to ensure minimal disruption.

Configuration Manager

Maintains accurate configuration data and ensures integrity of the configuration management system.

Release Manager

Plans, schedules, and oversees service releases and deployments.

Knowledge Manager

Ensures effective management and availability of knowledge across the organization.

Service Transition Manager

Coordinates all transition activities and ensures alignment with business objectives.

SERVICE OPERATION (ITIL)

Service Operation is the stage of the ITIL service lifecycle responsible for the **day-to-day delivery, monitoring, and support of IT services**. Its goal is to ensure that IT services are delivered **efficiently, reliably, and in line with agreed service levels**, while minimizing business disruption.

---

1. Balancing Conflicting Goals in Service Operation

Service Operation must continuously balance **competing and often conflicting objectives**, such as:

Reliability vs Cost

High reliability requires redundancy, monitoring, and skilled staff, which increases cost. Service Operation aims to find an optimal balance where services are reliable without excessive spending.

Stability vs Responsiveness

Maintaining stable systems may limit rapid changes, while business demands quick responses. Service Operation balances controlled changes with timely service restoration.

Quality vs Efficiency

High service quality may require more resources, while efficiency focuses on cost reduction. The challenge is to maintain acceptable service quality at optimal cost.

Proactive vs Reactive Support

Proactive monitoring reduces incidents but requires investment, while reactive support focuses on fixing issues after they occur. Service Operation aims to strengthen proactive management.

---

2. Event Management

Definition

Event Management is the process responsible for **monitoring all events that occur throughout the IT infrastructure** to detect, interpret, and respond appropriately.

Types of Events

- **Informational events:** Normal operations
- **Warning events:** Indicate potential issues
- **Exception events:** Indicate service disruption

Key Activities

- Event detection
- Event filtering
- Event correlation
- Event response

Importance

Event Management enables **early detection of issues**, reduces downtime, and supports proactive service management.

---

3. Incident Management

Definition

Incident Management is responsible for **restoring normal service operation as quickly as possible** following a service disruption.

Objectives

- Minimize business impact
- Restore service quickly
- Maintain user satisfaction

Key Activities

- Incident identification
- Incident logging
- Categorization and prioritization
- Diagnosis and escalation
- Resolution and recovery
- Incident closure

Importance

Effective incident management ensures **service availability and reliability**.

---

4. Problem Management

Definition

Problem Management focuses on **identifying and eliminating the root causes of incidents** to prevent recurrence.

Types of Problem Management

- **Reactive:** Resolving problems after incidents occur
- **Proactive:** Identifying potential problems before incidents occur

Key Activities

- Problem detection
- Root cause analysis
- Known error management
- Problem resolution
- Review and closure

Importance

Problem Management reduces incident frequency and improves long-term service stability.

---

5. Request (Event) Fulfillment

(Often referred to as Request Fulfillment in ITIL)

Definition

Request Fulfillment handles **standard service requests** from users, such as access requests, password resets, or information requests.

Objectives

- Provide efficient request handling
- Maintain service consistency
- Improve user satisfaction

Key Activities

- Request logging
- Approval and authorization
- Request fulfillment
- Closure and communication

Importance

This process improves operational efficiency and user experience.

---

6. Asset Management

Definition

Asset Management controls and tracks **IT assets throughout their lifecycle**, from acquisition to disposal.

Types of Assets

- Hardware assets
- Software assets
- Licenses
- Documentation

Key Activities

- Asset identification
- Asset tracking
- Financial management
- Compliance management
- Asset retirement

Importance

Asset Management helps in **cost control, compliance, and efficient resource utilization**.

---

7. Service Desk

Definition

The Service Desk is the **single point of contact** between users and the IT service provider.

Functions

- Incident and request handling
- Communication and updates
- User support and guidance
- Escalation management

Types of Service Desk

- Local service desk
- Centralized service desk
- Virtual service desk
- Follow-the-sun service desk

Importance

The Service Desk plays a key role in **customer satisfaction and service quality**.

---

8. Technical and Application Management

Technical Management

Definition

Technical Management provides **technical expertise** and support for IT infrastructure components such as servers, networks, and databases.

Responsibilities

- Infrastructure maintenance
- Technical support
- Capacity and performance optimization

Application Management

Definition

Application Management supports **software applications throughout their lifecycle**.

Responsibilities

- Application maintenance
- Performance tuning
- Issue resolution
- Support for upgrades and changes

---

9. Key Roles and Responsibilities for Staff

Service Desk Analyst

Handles incidents and service requests and communicates with users.

Incident Manager

Coordinates incident resolution and ensures service restoration.

Problem Manager

Identifies root causes and prevents recurring incidents.

Technical Support Staff

Provides expert support for infrastructure components.

Application Support Staff

Manages application-related issues and enhancements.

Operations Manager

Oversees daily service operations and ensures performance targets are met.

CONTINUAL SERVICE IMPROVEMENT (CSI)

Continual Service Improvement (CSI) is a phase of the ITIL service lifecycle that focuses on **ongoing improvement of IT services, processes, and overall service management practices**. CSI ensures that IT services continuously align with changing business needs by identifying improvement opportunities and implementing measurable enhancements.

---

1. Training and Awareness

Definition

Training and awareness ensure that **staff understand ITIL processes, service improvement objectives, and their individual responsibilities** within CSI.

Objectives

- Develop required skills and competencies
- Increase awareness of service improvement goals
- Promote a culture of continuous improvement

Key Elements

- ITIL process training
- Technical and functional skill development
- Awareness programs on policies and best practices
- Knowledge sharing sessions

Importance

Well-trained staff can identify improvement opportunities more effectively and implement changes consistently and accurately.

---

2. Ongoing Scheduling

Definition

Ongoing scheduling refers to the **continuous planning and scheduling of improvement activities** rather than treating improvement as a one-time effort.

Objectives

- Ensure regular review of services and processes
- Prioritize improvement initiatives
- Align improvements with business cycles

Key Activities

- Scheduling service reviews
- Planning improvement releases
- Aligning CSI initiatives with organizational priorities

Importance

Ongoing scheduling ensures that improvement activities are **systematic, measurable, and sustainable** over time.

---

3. Roles Created in CSI

CSI Manager

Responsible for coordinating and managing all CSI activities across the organization.

Process Owner

Ensures that specific processes are effective, efficient, and continuously improved.

Service Owner

Responsible for the overall quality and performance of a specific IT service.

CSI Analyst

Analyzes performance data and identifies improvement opportunities.

Importance of Defined Roles

Clear roles ensure accountability, ownership, and effective execution of improvement initiatives.

---

4. Ownership Assigned

Definition

Ownership assignment ensures that **each service, process, and improvement initiative has a clearly defined owner** responsible for its success.

Objectives

- Establish accountability
- Ensure decision-making authority
- Enable continuous monitoring

Types of Ownership

- Service ownership
- Process ownership
- Improvement initiative ownership

Importance

Ownership prevents ambiguity, ensures responsibility, and supports consistent improvement efforts.

---

5. Activities Identified to Be Successful in CSI

Performance Measurement

- Define Key Performance Indicators (KPIs)
- Establish metrics aligned with business goals

Data Collection and Analysis

- Gather operational and performance data
- Identify trends, gaps, and root causes

Improvement Identification

- Identify opportunities for improvement
- Prioritize based on impact and feasibility

Implementation of Improvements

- Plan and execute improvement initiatives
- Manage changes effectively

Review and Evaluation

- Measure improvement outcomes
- Validate success against objectives

Continual Feedback

- Collect feedback from customers and stakeholders
- Refine improvements based on feedback

CSI Improvement Model (Conceptual View)

CSI often follows a structured approach such as:

- What is the vision?

- Where are we now?
- Where do we want to be?
- How do we get there?
- Did we get there?
- How do we keep the momentum going?

This model ensures **continuous measurement and refinement**.

DATA CENTER MANAGEMENT

Data Center Management refers to the **planning, design, implementation, operation, monitoring, and protection of data center facilities** that host critical IT infrastructure such as servers, storage systems, networking devices, power systems, and cooling systems. The primary objectives are **high availability, reliability, scalability, security, performance, and cost efficiency**.

---

1. Data Center Architecture, Requirements & Prerequisites

Data Center Architecture

Data center architecture defines the **overall blueprint** of the data center. It integrates:

- Physical infrastructure (building, floors, racks)
- IT infrastructure (servers, storage, network devices)
- Electrical systems
- Cooling systems
- Security systems
- Monitoring and management tools

A good architecture ensures **fault tolerance, scalability, redundancy, and efficient resource utilization**.

Requirements

- Business workload analysis (applications, users, data volume)
- Availability and uptime requirements
- Performance and latency expectations
- Compliance and regulatory requirements
- Disaster recovery and backup needs

Prerequisites

- Feasibility study
- Risk assessment
- Budget approval
- Skilled manpower
- Vendor and technology selection

---

2. Required Physical Area for Equipment and Unoccupied Space

Equipment Area

This includes space for:

- Server racks and cabinets
- Storage arrays
- Network switches and routers
- UPS systems
- Cooling units

Unoccupied Space (White Space)

White space is intentionally kept empty for:

- Future expansion
- Improved airflow and cooling
- Maintenance activities
- Equipment replacement

Insufficient space leads to **overheating, poor maintenance access, and scalability issues**.

---

3. Required Power to Run All the Devices

Power is the **lifeline of a data center**.

Power Planning Includes:

- Load calculation of all IT and non-IT equipment
- Redundant power feeds (N+1, 2N)
- UPS systems for short-term backup
- Diesel generators for long-term outages

- Power Distribution Units (PDUs)

Objectives

- Zero downtime
- Stable voltage and frequency
- Protection against power surges

---

4. Required Cooling and HVAC

IT equipment generates significant heat. Cooling systems maintain:

- Optimal temperature
- Controlled humidity

Cooling Components

- HVAC systems
- Precision air conditioners
- Chillers and cooling towers
- Hot aisle/cold aisle configuration
- Raised floor air distribution

Poor cooling leads to **hardware failure, reduced lifespan, and downtime**.

---

5. Required Weight

Data centers house heavy equipment.

Weight Considerations

- Fully loaded server racks
- UPS batteries
- Cooling units
- Power systems

The building floor must support **high load capacity**, typically measured in **kg per square meter**. Structural assessment is mandatory to prevent collapse or damage.

---

6. Required Network Bandwidth

Network bandwidth determines **data transfer speed and application performance**.

Planning Includes:

- Internal LAN bandwidth
- External WAN and internet bandwidth
- Redundant network paths
- Support for peak traffic loads

Insufficient bandwidth results in **latency, congestion, and poor user experience**.

---

7. Budget Constraints

Budget constraints directly influence design decisions.

Cost Components

- Capital Expenditure (CAPEX)
  - Servers
  - Network devices
  - Power and cooling equipment
- Operational Expenditure (OPEX)
  - Power consumption
  - Cooling costs
  - Maintenance
  - Staffing

A balance must be achieved between **cost, reliability, and performance**.

---

8. Selecting a Geographic Location

The location of a data center affects **availability, cost, security, and operational efficiency**.

8.1 Safe from Natural Hazards & Manmade Disasters

Ideal locations avoid:

- Flood-prone areas
- Earthquake zones
- Cyclone-prone regions
- Industrial pollution zones
- High-risk security areas

Risk-free locations ensure **business continuity and disaster resilience**.

8.2 Availability of Local Technical Talent

Availability of skilled staff ensures:

- Faster troubleshooting
- Efficient maintenance
- Reduced downtime
- Lower training costs

Remote locations increase operational challenges.

8.3 Abundant and Inexpensive Utilities (Power & Water)

Power and water are critical for:

- IT equipment
- Cooling systems
- Fire suppression systems

Lower utility costs significantly reduce **long-term operational expenses**.

8.4 Selecting an Existing Building

Using an existing building requires:

- Structural evaluation
- Electrical capacity upgrades
- Cooling system modifications
- Enhanced physical security

Existing buildings may reduce cost but increase complexity.

---

9. Characteristics of an Outstanding Design

An outstanding data center design is:

- **Scalable** – supports future growth
- **Redundant** – eliminates single points of failure
- **Energy-efficient** – minimizes power and cooling costs
- **Secure** – protects data and assets
- **Maintainable** – easy access for upgrades and repairs

---

10. Guidelines for Planning a Data Center

Planning guidelines include:

- Capacity forecasting
- Modular design approach
- Redundancy planning
- Compliance with standards (ISO, TIA)
- Disaster recovery planning
- Documentation and change control

Proper planning avoids costly redesigns.

---

11. Data Centre Structures

Types of Structures

- Enterprise data centers
- Colocation data centers
- Modular data centers
- Containerized data centers
- Hyperscale data centers

Each structure serves different business needs.

---

12. Raised Floor Design and Deployment

Raised floors:

- Provide space for cables and cooling air
- Improve airflow management
- Allow flexible cabling
- Simplify maintenance

They are commonly used in large data centers.

---

13. Design and Plan Against Vandalism

Security planning protects against:

- Theft
- Sabotage
- Unauthorized access

Protective Measures

- Fencing and access barriers
- CCTV surveillance
- Biometric access control
- Security guards
- Incident response procedures

Protection ensures **service continuity and asset safety**.

INFRASTRUCTURE IN A DATA CENTER

Data center infrastructure consists of **all physical and logical components** required to deliver IT services reliably and securely. It includes servers, storage, networking, cabling, security systems, monitoring tools, and operational processes.

---

1. Modular Cabling Design

Definition

Modular cabling design is a **structured and standardized approach** to cabling that allows easy expansion, reconfiguration, and maintenance.

Key Components

- Horizontal cabling
- Vertical backbone cabling
- Patch panels
- Cable trays and conduits

Advantages

- Simplified troubleshooting
- Scalability for future growth
- Reduced downtime
- Improved airflow and cooling

Best Practices

- Use standard cable lengths
- Color-coded cables
- Proper labeling and documentation

---

2. Points of Distribution

Definition

Points of Distribution (PoDs) are **centralized locations** where power, cooling, and network connectivity are distributed to IT equipment.

Types

- Main Distribution Area (MDA)
- Horizontal Distribution Area (HDA)
- Zone Distribution Area (ZDA)

Importance

- Improves cable management
- Reduces latency
- Enhances scalability and redundancy

---

3. ISP Network Infrastructure and WAN Links

ISP Infrastructure

Data centers connect to one or more ISPs to provide:

- Internet connectivity
- Cloud access
- External communication

WAN Links

WAN links connect the data center to:

- Branch offices
- Disaster recovery sites
- Other data centers

Key Considerations

- Redundant links
- High bandwidth
- Low latency
- SLA-based connectivity

---

4. Network Operations Center (NOC) and Monitoring

Network Operations Center (NOC)

The NOC is a **centralized location** where network and infrastructure operations are monitored and managed.

Functions

- Real-time monitoring
- Incident detection
- Performance management
- Fault resolution
- Capacity planning support

Monitoring Tools

- Network monitoring systems
- Server and application monitoring
- Environmental monitoring

---

5. Data Center Physical Security, Logical Security, and Cleaning

Physical Security

Protects the facility and hardware.

- Access control systems
- CCTV surveillance
- Security guards
- Biometric authentication

Logical Security

Protects data and systems.

- Firewalls
- Intrusion detection/prevention systems
- Authentication and authorization
- Encryption

Cleaning

- Dust control
- Anti-static cleaning
- Scheduled maintenance
  Clean environments reduce hardware failure.

---

6. Reasons for Data Center Consolidation

Definition

Data center consolidation involves **reducing the number of data centers** by merging workloads into fewer, more efficient facilities.

Reasons

- Cost reduction
- Improved resource utilization
- Simplified management

- Reduced energy consumption
- Improved security

---

7. Consolidation Opportunities

Areas for Consolidation

- Server virtualization
- Storage consolidation
- Network consolidation
- Application consolidation

Benefits

- Lower operational costs
- Better performance
- Easier management
- Reduced physical footprint

---

8. Datacenter Servers

Types of Servers

- Rack servers
- Blade servers
- Tower servers
- Hyper-converged servers

Functions

- Application hosting
- Database management
- Virtualization
- Cloud services

Servers form the **core computing resource** of a data center.

---

9. Server Capacity Planning

Definition

Capacity planning ensures that **server resources meet current and future workloads**.

Key Factors

- CPU utilization
- Memory usage
- Storage requirements
- Network throughput

Benefits

- Prevents over-provisioning
- Avoids performance bottlenecks
- Supports scalability

---

10. Disaster Recovery (DR)

Definition

Disaster Recovery ensures **business continuity** during catastrophic events.

DR Components

- Backup systems
- Replication
- Failover sites
- Recovery procedures

DR Strategies

- Cold site
- Warm site
- Hot site

---

11. Data Center Security Guidelines

Objectives

- Protect data and infrastructure
- Ensure availability
- Maintain compliance

Guidelines

- Layered security approach
- Regular audits
- Access control
- Incident response planning

---

12. Internet Security Guidelines

Internet Security

Protects data and systems connected to the internet.

Guidelines

- Firewalls and proxies
- Secure communication protocols
- Web filtering
- Regular patching

---

13. Internet Security (Detailed)

Threats

- Malware
- Phishing
- DDoS attacks
- Man-in-the-middle attacks

Protection Measures

- Antivirus and anti-malware
- IDS/IPS
- Secure DNS
- User awareness training

---

14. Source Security Issues

Definition

Source security issues originate from:

- Insecure software
- Misconfigured systems
- Insider threats
- Weak authentication

Mitigation

- Secure coding practices
- Access controls
- Regular security reviews

---

15. Best Practices for System Administration

Core Practices

- Standardized configurations
- Regular patch management
- Monitoring and logging
- Backup and recovery
- Documentation

Benefits

- Reduced downtime
- Improved reliability
- Enhanced security

---

16. System Administration Work Automation

Definition

Automation involves using tools and scripts to **automate repetitive administrative tasks**.

Areas of Automation

- System provisioning
- Configuration management
- Patch deployment
- Monitoring and alerts
- Backup operations

Benefits

- Reduced human error
- Faster operations
- Consistency