Hope
Health Care Information System

Introduction

System Status		
☐	Operational	The system is operating and in production.
☒	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Other	Explain: Click here to enter text.

Hope Health Care Information System (HHCIS) is a general information system for small and medium-sized hospitals. It covers the main management functions of hospitals and the main links of patients in hospitals.

HHCIS is not simply a software, it is a result of the perfect unification of the hospital's management thinking, the hospital's business experience of various departments and the latest computer technology.

Advantages: This system can bring convenient and fast services to patients, promote standardized management of hospitals, and greatly reduce medical errors.

Functions

HHCIS contains following functions:

Outpatient Management

Inpatient and Ward Management

Medical File Management

Drug Management

Medical Device Management

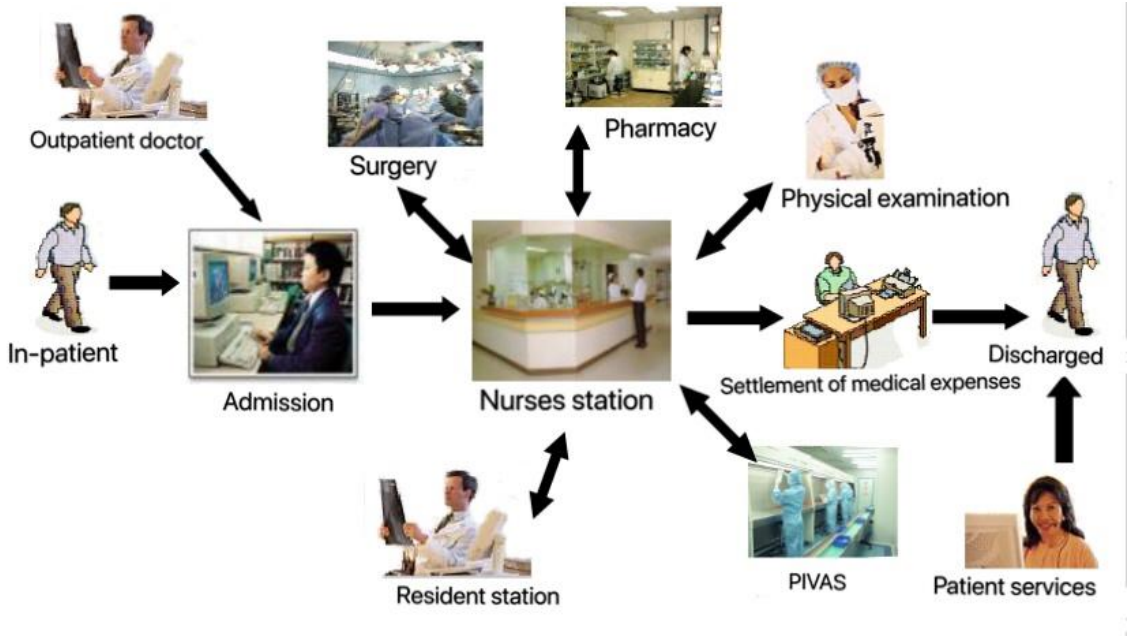
Financial Management

Human Resource Management

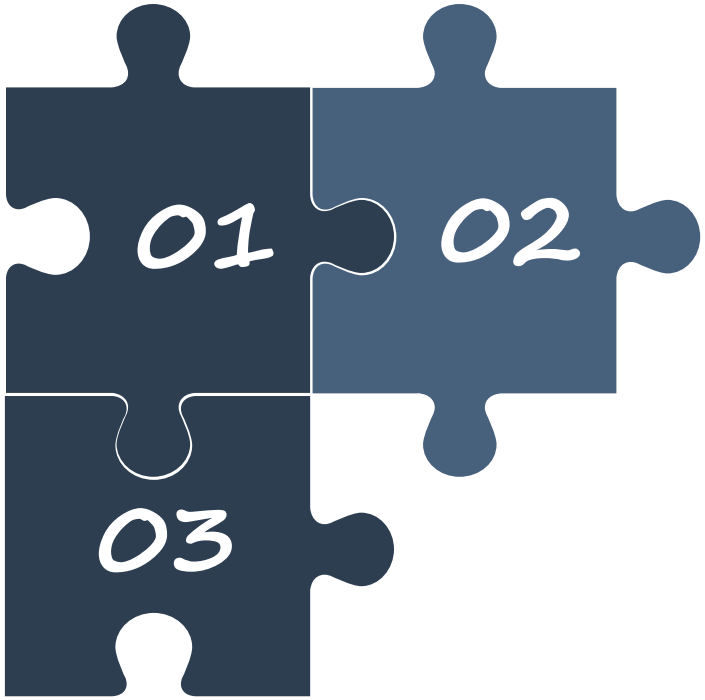
.....

Example: *Inpatient and Ward Management*

- This system can help patients to register for hospitalization, and has functions such as providing advance payment, entry of guarantor information, discharge registration, and patient recall.
- For doctors, they can directly enter doctor's orders, write medical records, and apply for examinations in the system.
- For nurses, entry of patient signs (temperature, pulse, breathing, etc.) can be done quickly.
- When a patient discharges from the hospital, the system can automatically make a payment according to the doctor's order and provide a payment review form.



Types of Users



Technical personnel: System Administrator, Database Administrator, Web Administrator, Network Administrator, Firewall Administrator, Client Administrator, Test Team, Development Team

System Administrator: Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups

Database Administrator: Monitor the warning log of the database, and make regular backup and deletion; password management; authorization ; assign resources

Employees: Hospital Staff

Hospital Staff: Input, query and manage patient information; query hospital resources and medical documents; salary payment; human resource management; do office work

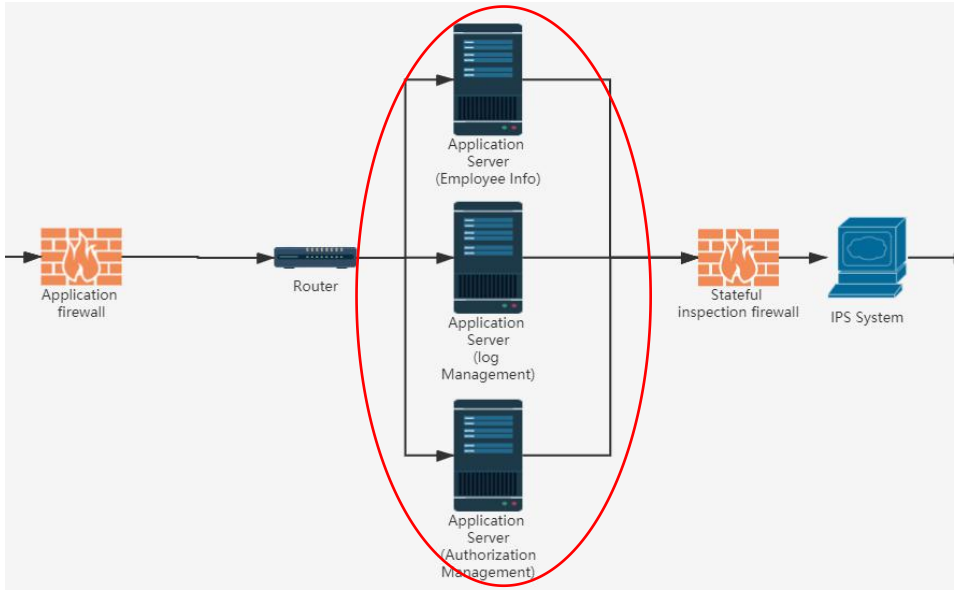
External: Patients, Insurance Company

Patients: Access to the hospital website for inquiry; make an appointment online

Insurance Company: If a patient has bought medical insurance, the insurance company can obtain the patient's medical information from the system and make insurance compensation

17 Control Families

Audit and Accountability(AU)



ID	Control Description	Sensitive Level---High
AU-1	Audit and Accountability Policy and Procedures	AU-1
AU-2	Audit Events	AU-2 (3)
AU-3	Content of Audit Records	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4
AU-5	Response to Audit Processing Failures	AU-5 (1) (2)
AU-6	Audit Review, Analysis and Reporting	AU-6 (1) (3) (4) (5) (6) (7) (10)
AU-7	Audit Reduction and Report Generation	AU-7 (1)
AU-8	Time Stamps	AU-8 (1)
AU-9	Protection of Audit Information	AU-9 (2) (3) (4)
AU-10	Non-repudiation	AU-10
AU-11	Audit Record Retention	AU-11
AU-12	Audit Generation	AU-12 (1) (3)

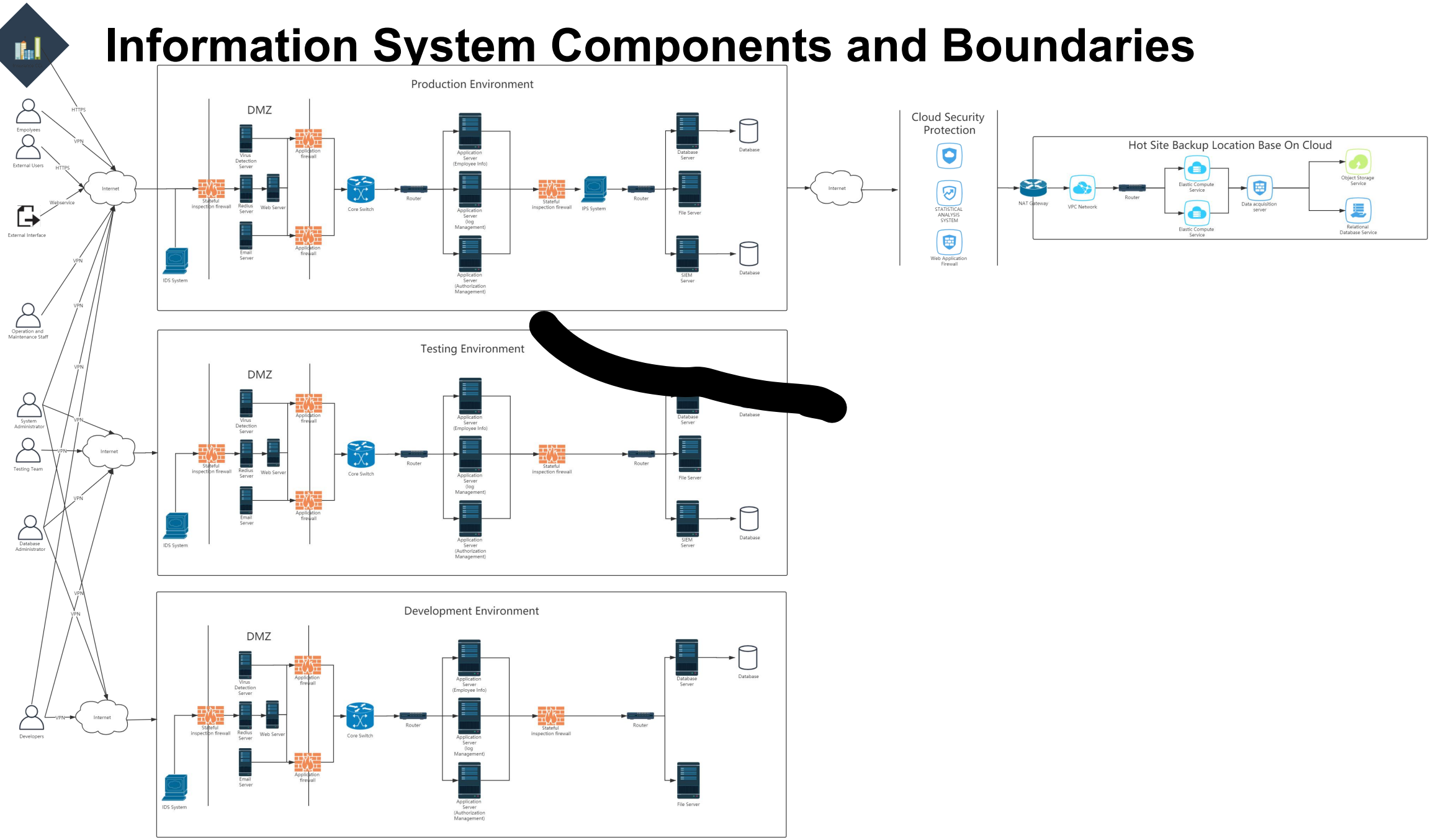
AU-2 Audit Events

- HHCIS is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. All these events need to be audited continually.
- The organization review and update audit events annually, and update in time when significant changes occur.

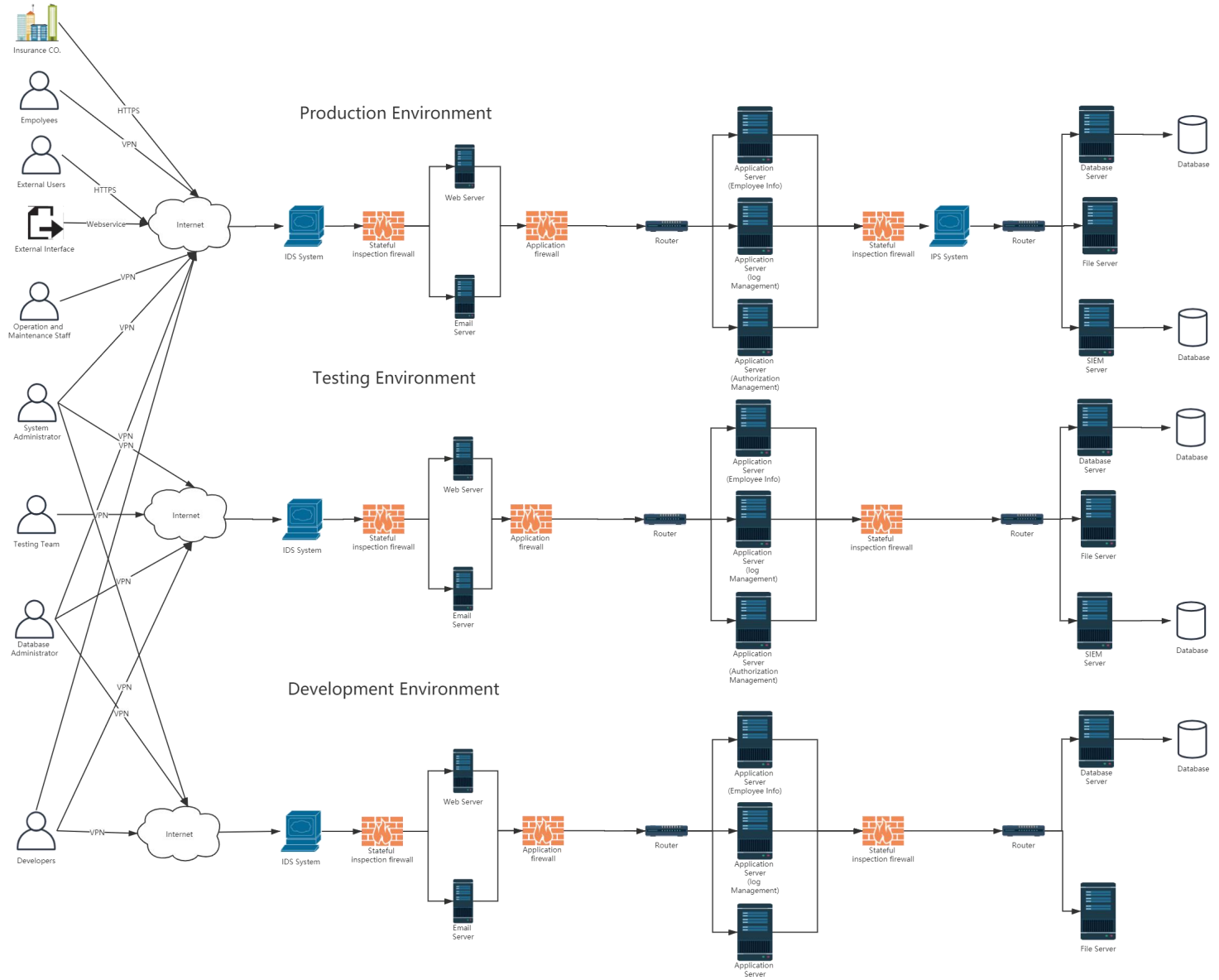
AU-5 Response to Audit Processing Failures

- HHICS must alert designated organizational officials in the event of an audit processing failure. In the event of an audit processing failure, HHICS must configure the audit log to (1) stop generating audit records or (2) overwrite the oldest audit records.
- HHICS provides a warning to system administrator within ten minutes when allocated audit record storage volume reaches 85% of repository maximum audit record storage capacity.
- The information system provides an alert in ten minutes to system administrator when the following audit failure events occur:audit failure of password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage.

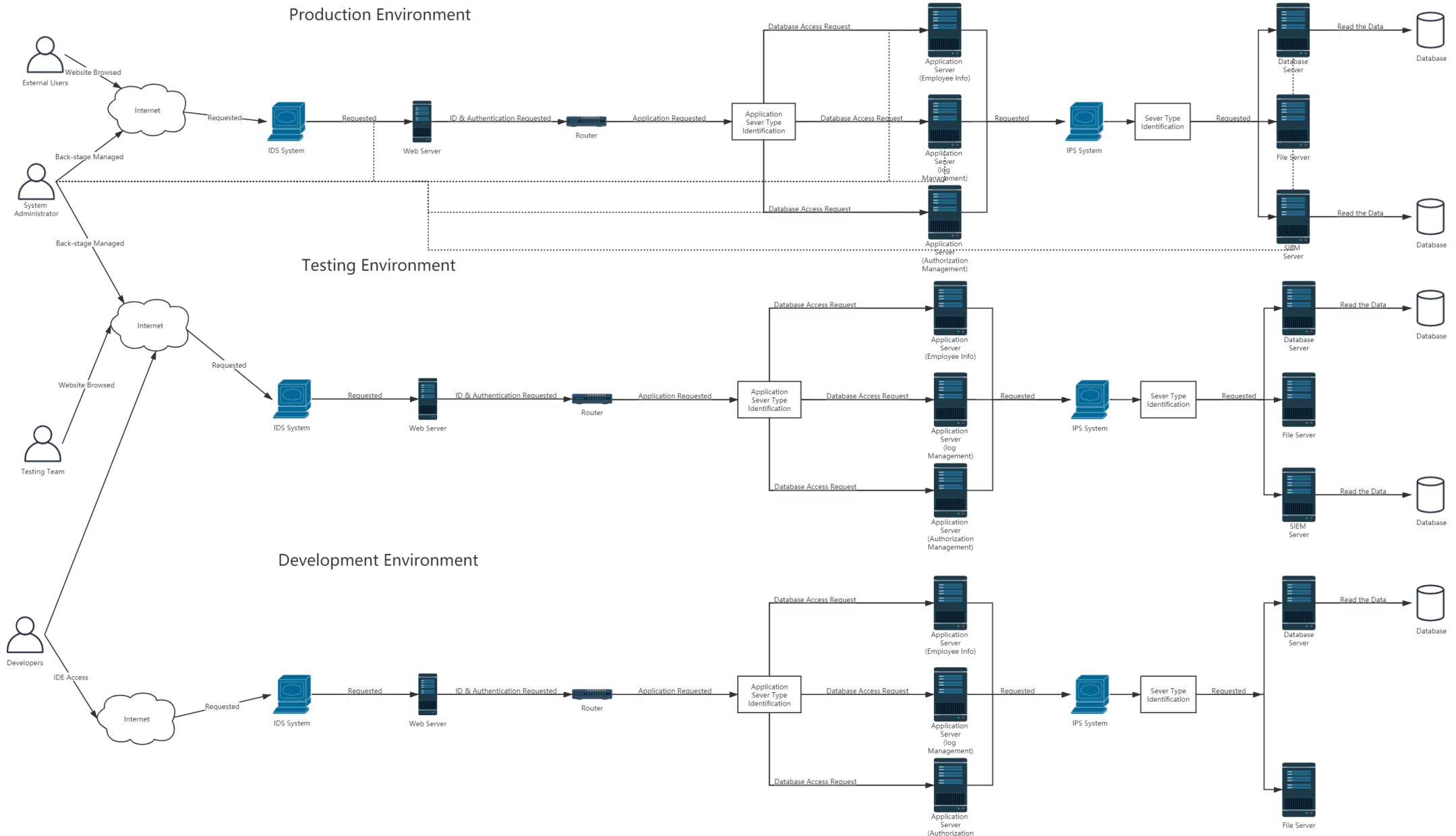
Information System Components and Boundaries



Network Architecture



Data Flow


Production Environment
External Users
Website Browsed
Internet
Requested
IDS System
Requested
Web Server
ID & Authentication Requested
Router
Application Requested
Application Sever Type Identification
Database Access Request
Application Server (Employee Info)
Application Server (log Management)
Application Server (Authorization Management)
Requested
IPS System
Sever Type Identification
Requested
Database Server
File Server
SIEM Server
Read the Data
Database
Back-stage Managed
System Administrator
Testing Environment
Testing Team
Development Environment
Developers
IDE Access

Thanks