



정보보호 인증 통합 플랫폼

Compline 제품 소개서

2024



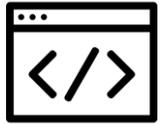
취약점은 있지만 취약점 통합 관리는?



DB취약점



WEB/WAS취약점



소스코드취약점



보안관제



서버취약점



네트워크취약점



모의해킹



PC취약점

다양한 취약점 진단

정보보안 수준을 유지하기 위하여
다양한 정보보안 대상 자산에
대해 취약점 진단 필요

분산된 취약점 데이터의 통합

진단 대상 별 발생하는 모든
취약점 데이터에 대한
통합 관리 필요

조직/업무 단위 취약점 현황

조직 및 업무 단위의 정보보안
수준 관리를 위해 취약점에 대한
분류가 필요

취약점 조치 관리

발견된 취약점에 대해 조치
이력을 관리하여 지속적인
정보보안 수준 상태 확인 필요

정보보안 수준관리는 어떻게??

HOW TO ?



취약점(기술적/관리적)
진단 절차 수립



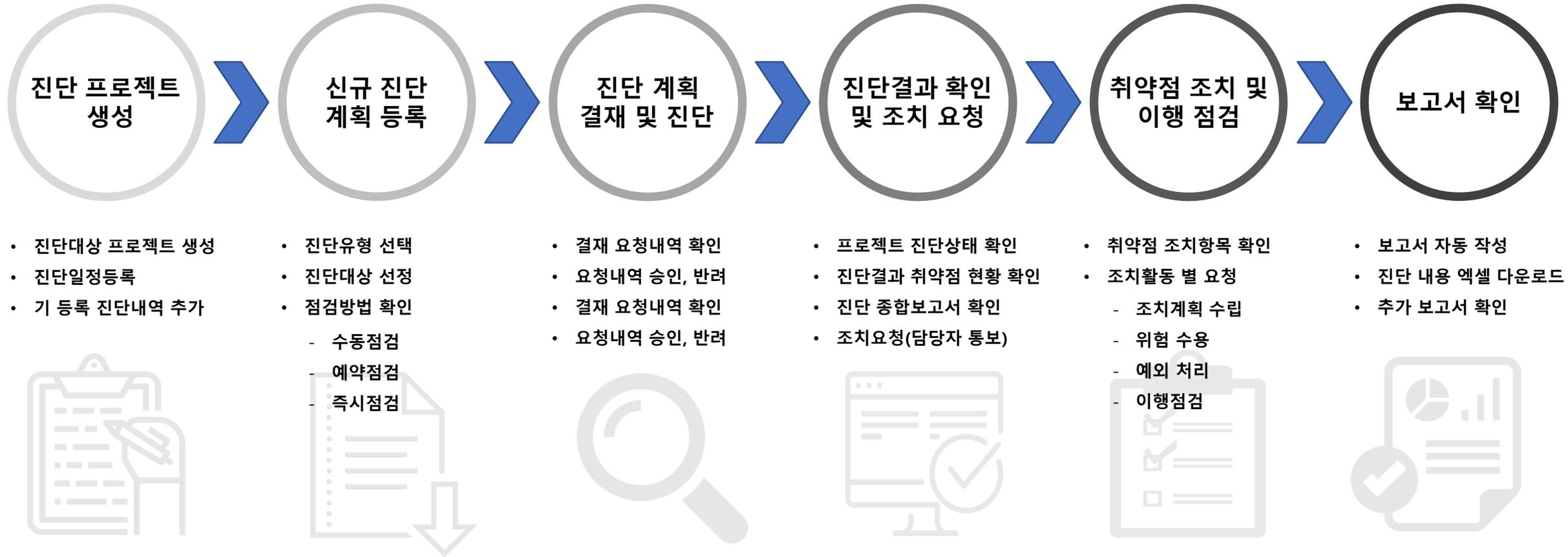
보안 취약점
데이터 통합 및 시각화



상시 취약점 관리 현황
모니터링/리포트

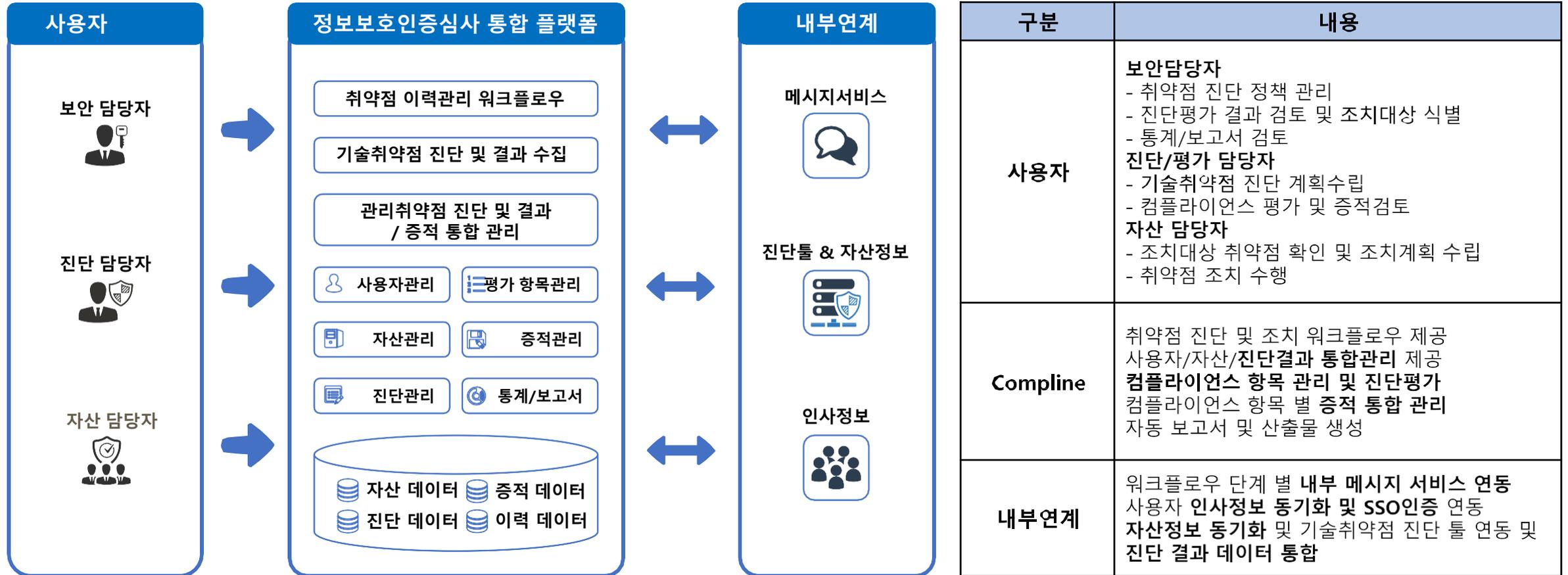
정보보안 수준 통합관리

취약점 점검업무 표준 프로세스



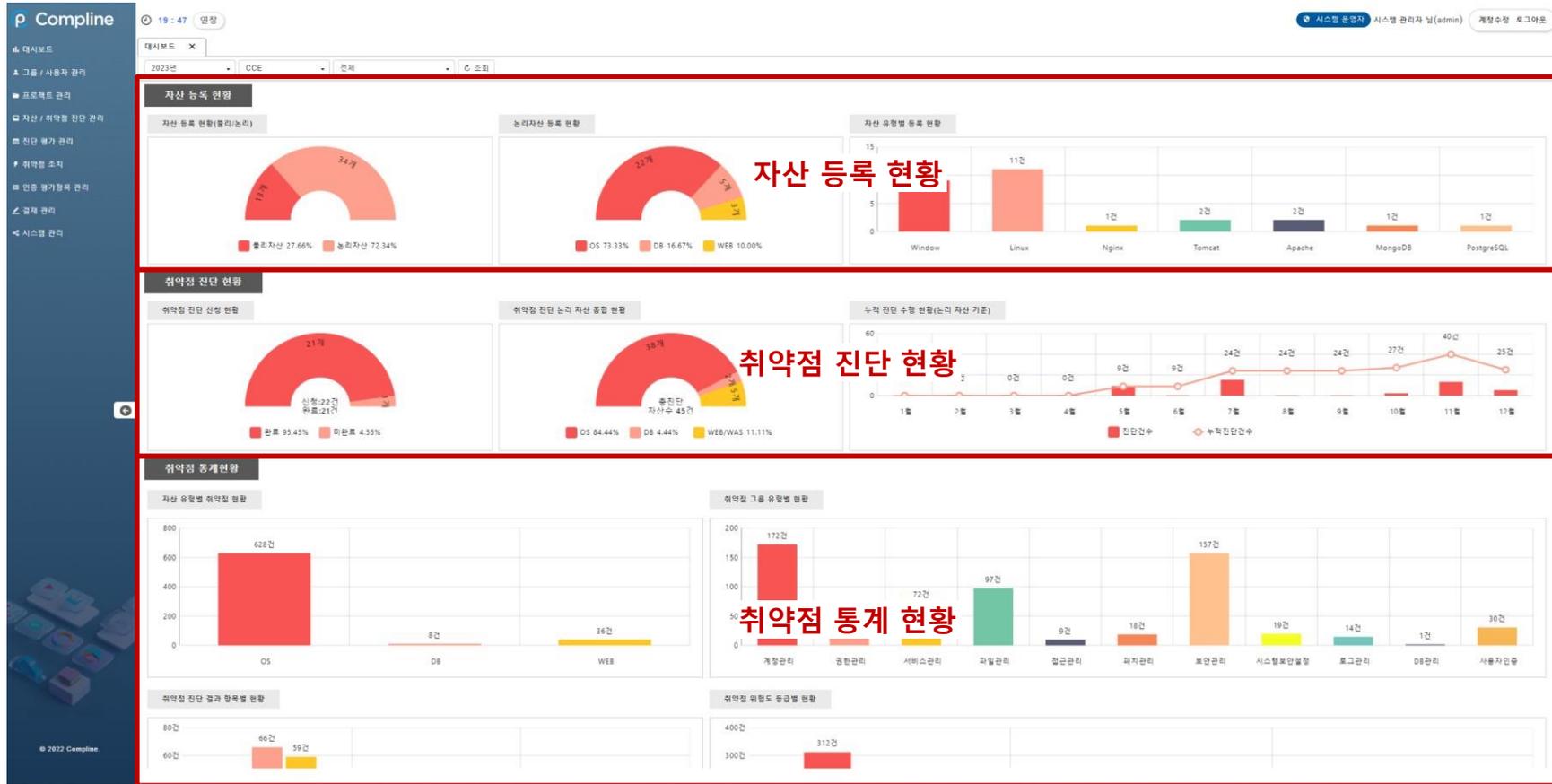
정보보안 인증 통합관리

솔루션 구성 개요



전체 현황 조회

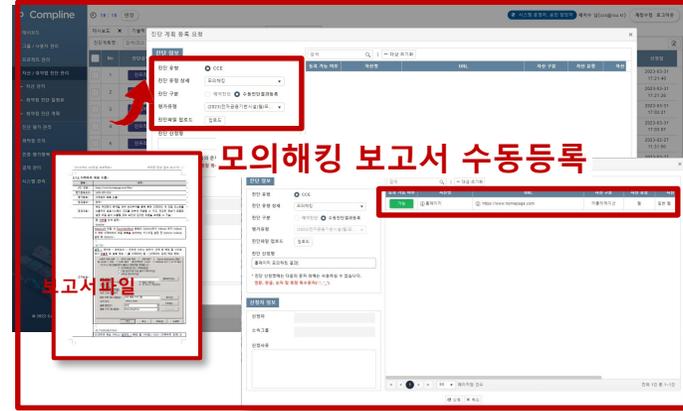
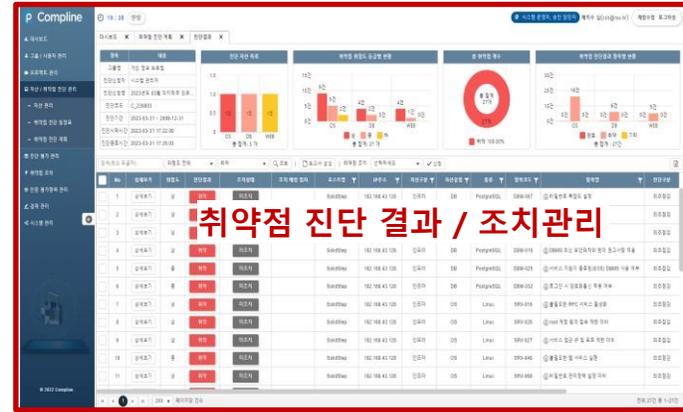
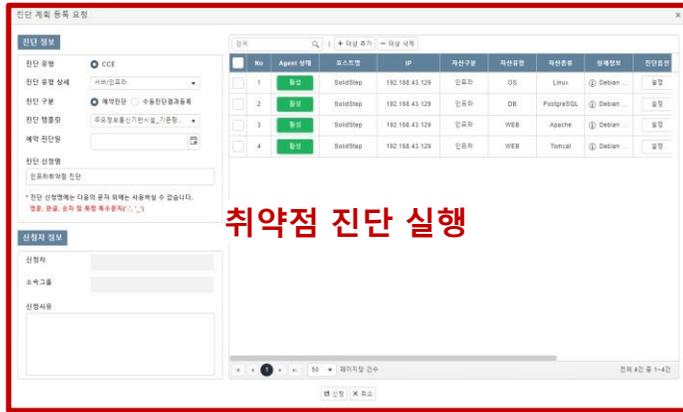
통합 대시 보드



- **자산등록 현황 조회**
 - 자산등록 현황(물리/논리)
 - 논리자산 등록현황
 - 자산 유형 별 등록 현황
- **취약점 진단 현황**
 - 취약점 진단 신청현황
 - 취약점 진단 논리자산 종합현황
 - 자산 유형 별 등록 현황
- **취약점 통계 현황**
 - 자산 유형 별 취약점 현황
 - 취약점 그룹 유형 별 현황
 - 취약점 진단 결과 항목 별 현황

전체 현황 조회

취약점관리 주요 기능



기능구분	기능 상세
인프라 진단	<ul style="list-style-type: none"> 진단툴 SolidStep 연동을 통한 원격 진단 및 취약점 결과 자동 수집 수집된 취약점 결과 정보 현황 제공 진단 계획 별 진단 결과 보고서 자동 생성 취약점 별 조치 요청 및 조치 이력 관리
모의해킹	<ul style="list-style-type: none"> 모의해킹 보고서 파일 업로드를 통한 취약점 결과 데이터 자동 등록 취약점 항목 상세 수행 내역 및 조치가이드 저장 취약점 별 조치 요청 및 조치 이력 관리
보안장비	<ul style="list-style-type: none"> 수동(진단담당자)진단에 의한 진단 결과내역 엑셀 일괄 업로드를 통한 취약점 결과 자동 등록 취약점 별 조치 요청 및 조치 이력 관리
기타	<ul style="list-style-type: none"> 진단 결과 예외/위험수용 처리 및 향후 동일 취약점 발생 시 예외/위험수용 상태 값 유지

자산관리

자산 그룹 별 자산 관리 지원

The screenshot displays the Compline asset management dashboard. On the left, a sidebar lists navigation options like '그룹 / 사용자 관리' and '자산 / 취약점 진단 관리'. The main area is divided into several sections:

- 자산 현황 (Asset Status):** A table showing counts for OS (38), WEB (5), DB (2), NETWORK (1), and a total of 46 assets.
- 자산 현황 조회 (Asset Status Query):** A series of donut charts showing the distribution of assets by category: OS (38), WEB (5), DB (2), and NETWORK (1). Further breakdowns show WEB assets as Jboss (1), Tomcat (2), and Apache (2); and NETWORK assets as Cisco (1).
- 자산 그룹 조회 (Asset Group Query):** A list of asset groups with columns for Agent status, Hostname, IP, Asset Group, Asset Type, and Asset Category.
- 자산 상세 조회 (Asset Detail Query):** A detailed view of a specific asset (GWAPP-1) showing its hostname, IP, asset group, type, and category, along with system information and evaluation details.

- **자산현황 조회**
 - OS, WEB, DB, N/W 별 조회
- **자산그룹 조회**
 - 서버/인프라
 - 보안장비
 - 어플리케이션
- **세부 조회**
 - 자산 IP정보 조회
 - 자산 유형 별 조회
 - 자산 종류 별 조회
 - 자산 상세 정보 확인
- **자산 상세 정보 조회**

자산관리

평가유형 별 자산 관리 지원

The screenshot displays the Compline Asset Management dashboard. The left sidebar contains navigation menus for '자산관리' (Asset Management) and '평가유형 별 자산 분류' (Asset Classification by Evaluation Type). The main content area features a '자산 현황' (Asset Status) table, three donut charts for 'ALL', 'OS', and 'WEB' asset types, and an '자산목록' (Asset List) table.

Asset Type	Count
OS	1 개
WEB	1 개
DB	0 개
NETWORK	0 개
합계	2 개

Agent 상태	호스트명	IP	자산 구분	자산 유형	자산 종류	상세 정보	서비스명	전단응답	담당자(정)	담당자(부)
정상	SolidStep	192.168.43.128	인프라	OS	Linux	Debian Linux SolidStep 3.16.0-4...	M-SC01	설정		
정상	SolidStep	192.168.43.128	인프라	WEB		ebian Linux SolidStep 3.16.0-4...	M-SC01	설정		

- 평가유형 별 자산분류
 - 전자금융기반시설
 - ISMS
 - 정보보호 상시평가제
 - 주요정보통신 기반시설
 - 국가정보원 정보보안 관리실태평가
 - ISO27001
 - ISMS-P
 - PCI DSS
 - 기타
- 자산목록
 - 자산현황 별 조회

취약점 진단 관리

취약점 진단 계획 등록 및 진단 요청(진단 툴 연동)

인프라 취약점 진단 목록

No	진단유형	진단신청명	자산유형 (전체, 성공, 진단중, 실패)	진행상태	진단결과	진단예약일시	진단시작시간	결과수집일시	신청자	신청일
1	인프라	2023년도 03월 마지막주								
2	인프라	2023년도 03월 마지막주								
3	인프라	2023년도 03월 마지막주								
4	인프라	2023년도 03월 마지막주								
5	인프라	이름이 잘못히 들어지는								
6	인프라	이름이 잘못히 들어지는								
7	인프라	이름이 잘못히 들어지는								
8	인프라	2023_02_23_진단								
9	인프라	02_27_인프라자산_진단								
10	모의해킹	홈페이지모의해킹결과								
11	모의해킹	홈페이지_모의해킹								
12	인프라	정기WEB진단								
13	인프라	정기DB진단								
14	인프라	정기OS진단								

진단 계획 세부 정보

진단 정보

- 진단 유형: 서버/인프라(CCE)
- 진단 구분: 예약 진단
- 진단 템플릿: 피연필크_전자금융기반시설
- 예약 진단일: 2023-03-31 10:00
- 진단 신청명: 2023년도 03월 마지막주 인프라 정기점검

신청자 정보

- 신청자: 시스템 관리자
- 소속그룹: 개인 정보 보호팀
- 신청사유: 2023년도 03월 마지막주 인프라 정기점검 4 회차

승인자 정보

- 승인자: 채지수
- 소속그룹: 개인 정보 보호팀
- 승인/반려 사유: 2023년도 03월 마지막주 인프라 정기점검 승인합니다.

No	Agent 상태	호스트명	IP	자산구분	자산유형	자산종류	상세정보	진단유선
1	활성	SolidStep	192.168.43.128	인프라	OS	Linux	Debian ...	설정
2	활성	SolidStep	192.168.43.128	인프라	WEB	Apache	Debian ...	설정

인프라 취약점 진단 목록

- 진단 계획 수립 및 신청
- 진단 신청 명 생성
- 진단유형 정보 확인
- 진행상태 및 결과 확인
- 접수/등록일자 확인

진단 계획 세부 정보

- 진단 정보 확인
- 진단 신청자 정보 확인
- 진단 승인자 정보 확인
- 진단 장비 확인
- 자산 유형/종류 별 확인

진단 프로젝트 관리

프로젝트(그룹) 별 관리적/기술적 진단 내역 관리

평가유형 구분	평가유형 기술 분류	개별진단 평가명	기준년도	상태	평가 시작일	평가 종료일
<input type="checkbox"/> 관리적 평가	-	전자금융기기반시설 평가	2023년	완료	2023-01-01	2023-10-26
<input type="checkbox"/> 관리적 평가	-	주요정보통신기기반시설 평가	2023년	진행중	2023-01-01	2023-12-31
<input checked="" type="checkbox"/> 기술적 평가	보안장비	정기 보안장비 취약점 진단평가	2023년	완료	2023-02-01	2023-02-17
<input type="checkbox"/> 관리적 평가	-	ISO27001	2023년	진행중	2023-02-01	2023-02-28
<input type="checkbox"/> 관리적 평가	-	2023년 PCI-DSS 대응	2023년	진행중	2023-03-01	2023-06-30
<input type="checkbox"/> 관리적 평가	-	2023년도 ISMS-P 진단평가	2023년	완료	2023-03-01	2023-05-31
<input type="checkbox"/> 관리적 평가	-	2023년도 전자금융기기반시설 관리체계 평가	2023년	완료	2023-01-02	2023-06-30

- 프로젝트 단위 관리
 - 관리적 진단평가 추가
 - 기술적 진단평가 추가
 - 모의해킹 보고서 첨부
 - 프로젝트 단위 보고서 자동 생성
 - 증적 파일 일괄 다운로드

모의해킹 진단 결과 통합

모의해킹 결과 직접 작성 및 등록

The screenshot displays the Compline system interface. On the left is a navigation menu with options like '대시보드', '그룹 / 사용자 관리', '프로젝트 관리', '자산 / 취약점 진단 관리', '진단 평가 관리', '기술적 진단 평가', '관리적 진단 평가', '취약점 조치', '인증 평가항목 관리', '결과 관리', and '시스템 관리'. The main area shows a table of assessment results with columns for ID, Name, Status, and Action. Three report preview windows are overlaid on the table:

- 모의해킹 진단결과 일반사항 등록**: A form for registering general information for a penetration test, including a title, URL, and a description of the environment.
- 모의해킹 진단결과 상세 수행 내역 작성**: A rich text editor for documenting the detailed steps and findings of the penetration test.
- 모의해킹 진단 결과 취약점 조치가이드 작성**: A rich text editor for writing remediation guides for identified vulnerabilities, such as configuring Apache SSL settings.

- **모의해킹 취약점 등록**
 - 대상 자산 별 모의해킹 대상 취약점 항목 별 진단 결과 및 수행 내역, 조치 가이드 작성 환경 제공
- **솔루션 내 진단 결과 작성 가능**
 - 수행 결과 및 조치가이드 작성이 가능한 문서 편집 환경 제공
 - 작성 후 결과 데이터로 즉시 통합
 - 결과보고서로 출력 가능

모의해킹 진단 결과 통합

모의해킹 결과 보고서 파일 등록(보고서 파일 분석 및 데이터화)

모의해킹 진단결과 보고서 등록 가능

업로드 파일을 분석하여 등록대상 자산을 식별

지정된 양식의 모의해킹 보고서 파일 등록 가능

- 모의해킹 보고서 등록
 - 보고서 파일 업로드
 - 업로드 파일 내 취약점 정보 자동 등록
 - 취약점 상세 정보 제공
- 기 운영 중 모의해킹 보고서 포맷 적용
 - 기 운영 중인 모의해킹 결과 보고서를 활용하여 일괄 등록 양식으로 기능 제공

기술 취약점 진단 이력관리

취약점 데이터 통합에 따른 조치이력관리 워크플로우 제공

The screenshot displays the Compline dashboard with the following components:

- Header:** Compline logo, user information (시스템 운영자, 관리자(admin)), and navigation tabs (대시보드, 취약점 진단 계획, 진단결과).
- Summary Cards:**
 - 진단 자산 목록:** Bar chart showing 1 asset.
 - 취약점 위험도 등급별 현황:** Bar chart showing 5 high, 5 medium, 0 low, 0 critical, and 0 unknown vulnerabilities.
 - 총 취약점 개수:** Donut chart showing 6 total vulnerabilities, with 100% being critical.
 - 취약점 진단결과 항목별 현황:** Bar chart showing 6 vulnerabilities across categories: 양호 (0), 취약 (6), 기타 (0).
- Table:** A table listing 6 vulnerabilities with columns for No, 상세보기, 위험도, 진단상태, 조치상태, 조치 예정 일자, 자산명, URL, 자산구분, 자산유형, 종류, 항목코드, and 조치요청.

No	상세보기	위험도	진단상태	조치상태	조치 예정 일자	자산명	URL	자산구분	자산유형	종류	항목코드	조치요청
1	상세보기	높음	취약	이행점검 승인완료		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-FIN-017	① [전자금융] 사용자 입*
2	상세보기	다소높음	취약	이행점검 승인완료		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-027	① 데이터 평문전송
3	상세보기	다소높음	취약	이행점검 승인완료		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-027	① 데이터 평문전송
4	상세보기	다소높음	취약	예외처리 승인완료		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-029	① 디렉토리 목록 노출
5	상세보기	다소높음	취약	조치완료		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-040	① 불필요한 파일 노출 여
6	상세보기	다소높음	취약	미조치		① 홈페이지	① https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-041	① 크로스 사이트 스크립

- **진단결과 통계정보 제공**
 - 진단 자산 목록 조회
 - 취약점 위험도 등급 별 조회
 - 취약점 개수 확인
 - 취약점 진단결과 항목 별 조회
- **항목 별 조치 요청**
 - 진단결과 상세 조회
 - 조치 요청
 - 예외/위험 수용 처리
 - 결과 및 조치상태 확인

기술 취약점 진단 이력관리

취약점 진단 결과 상세 정보 제공

The screenshot displays the Compline interface with several overlapping windows:

- 진단 이력 (Vulnerability History):** A table showing a list of vulnerabilities. One entry is highlighted with a red box and labeled "진단이력 조회 (모의해킹 예시)".
- 취약점 정보 (Vulnerability Information):** A window showing details for a specific vulnerability, including its name, ID, and status.
- 취약점 상세내역 (Vulnerability Details):** A window showing a list of vulnerabilities, including their names, URLs, and remediation status.
- 조치 가이드 (Remediation Guide):** A window providing detailed instructions for remediation, such as "중요정보의 전송을 최소화하여 사용자 도정으로부터의 위험을 줄여 주기와 같이 클라이언트 측에 기록하지 않음".
- 조치 이력 (Remediation History):** A table showing the history of remediation actions, including the date, user, and details of the remediation.

- 취약점 진단이력 조회
 - 진단결과 조회
 - 진단결과 수집 일자 조회
 - 취약점 개수 확인
 - 취약점 진단결과 항목 별 조회
- 취약점 진단 정보 상세
 - 취약점 정보 조회
 - 취약점 상세내역 조회
 - 조치 가이드 조회
 - 조치이력 조회

정보보호 컴플라이언스 진단 평가 통합

컴플라이언스 평가 관리

[주요 인증/심사 및 컴플라이언스 진단 평가 제공]

전자금융기반시설 주요정보통신기반 ISMS ISMS-P ISO27001 자체보안성심의

컴플라이언스 유형 관리

컴플라이언스 항목 관리

컴플라이언스 진단 평가

진단 결과 및 증거 등록

컴플라이언스 항목관리 및 진단 평가 가능

기능구분	기능 상세
컴플라이언스 항목 관리	<ul style="list-style-type: none"> 연도 별 컴플라이언스 유형 및 항목 정보 관리 기능 제공 항목 별 진단/평가 가이드정보 및 유사항목 매핑을 통한 컴플라이언스 간 항목 유사정보 제공 자체 보안성 심의 항목 생성 및 진단평가 기능 제공
컴플라이언스 진단 평가	<ul style="list-style-type: none"> 등록된 컴플라이언스 별 진단 평가 생성 및 등록된 평가자에 의한 평가 결과 등록 진단 평가 항목 별 관련 법령 정보 제공 항목 별 평가 근거 증거 파일 등록 업로드 증거에 대한 미리보기 기능 지원
컴플라이언스 취약점 조치	<ul style="list-style-type: none"> 취약점 별 조치담당자 지정 및 조치요청 조치에 따른 이행 점검 프로세스 제공
보고서 자동생성	<ul style="list-style-type: none"> 컴플라이언스 별 진단평가 결과 보고서 자동 생성 컴플라이언스 별 진단결과 증거 일괄 다운로드

정보보호 컴플라이언스 진단 평가 통합

인증심사 평가(컴플라이언스) 항목 관리

인증심사 유형

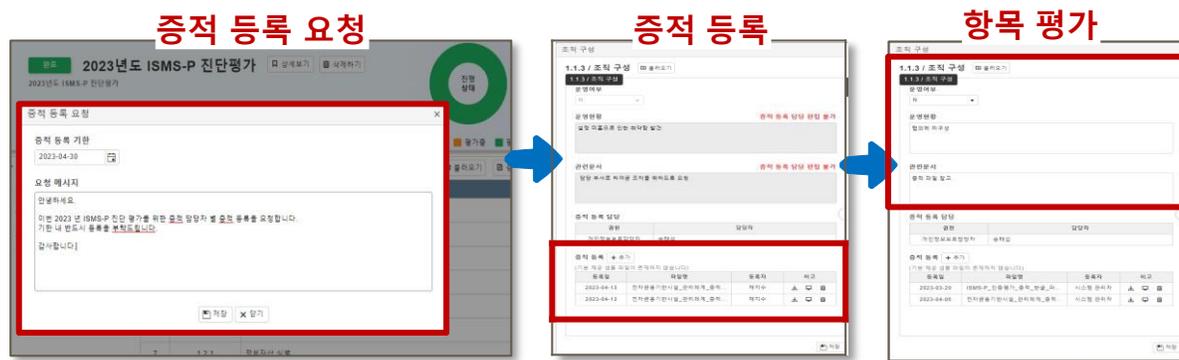
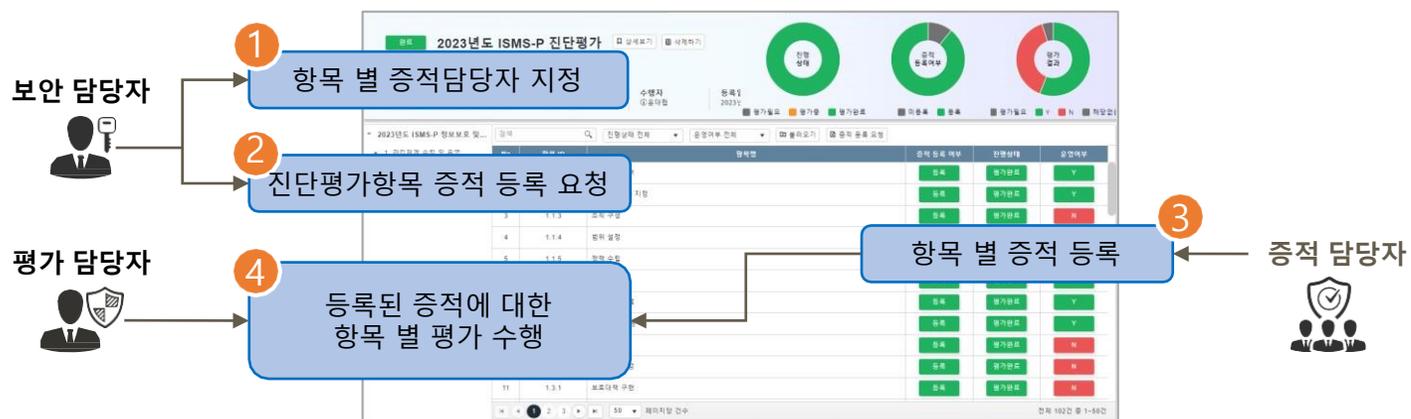
평가유형: 전자금융기반시설 | 기준년도: 2023 | 위험도 기준: 5단계(높음~낮음) | 점수산출 기준: 위험도 | 등록일자: 2022년 08월 17일

항목 ID	항목명	평가 여부	순번	등록일자
FISM-001	정보보안 관련법규 위반에 관한 제재기준 및 절차수립 및 운영 여부	On		2022년 08월 17일
FISM-002	정보기술(IT)부문계획 매년 수립 및 운영 여부	On		2022년 08월 17일
FISM-003	정보처리시스템 관련 전담조직 운영 여부	On		2022년 08월 17일
FISM-004	전자금융업무 관련 전담조직 운영 여부	On		2022년 08월 17일
FISM-005	IT 아웃소싱(이하 'IT차회사' 포함) 통제/관리 조직(인력포함) 운영 여부	On		2022년 08월 17일
FISM-010	정보보호최고책임자(CISO) 지정 여부	On		2022년 08월 17일
FISM-011	정기적으로 수행되는 일차원 정보보안 관련법규 준수여부 점검결과에 대한 임원(정보보호 최고경영자)보고 여부	On		2022년 08월 17일
FISM-012	정보보호 관련 상황률 심의·의결하는 정보보호위원회 설치 및 운영 여부	On		2022년 08월 17일
FISM-013	정보보호위원회 구성의 적정성	On		2022년 08월 17일
FISM-014	정보보호위원회 심의·의결 사항에 관한 적정성	On		2022년 08월 17일
FISM-015	정보보호위원회 심의·의결 사항에 관한 임원(정보보호최고책임자, 최고경영자) 보고 여부	On		2022년 08월 17일
FISM-016	정보보안점검의 날 지정 및 운영 여부	On		2022년 08월 17일

- 인증 심사 유형 관리
 - 국내/외 다양한 컴플라이언스 유형 및 항목 등록 기능
 - 자체 보안 적합성 평가 항목 등록 및 관리 기능
- 세부 항목 정보 관리
 - 항목ID 별 상세정보 제공
 - 평가 여부 확인
 - 등록일자 확인

컴플라이언스 진단/평가 증거 통합 관리

인증/심사 평가 항목 별 증거 담당자 지정 및 증거 등록 요청



기능구분	기능 상세
컴플라이언스 항목 관리	<ul style="list-style-type: none"> 연도 별 컴플라이언스 유형 및 항목 정보 관리 기능 제공 항목 별 진단/평가 가이드정보 및 유사항목 매핑을 통한 컴플라이언스 간 항목 유사정보 제공 자체 보안성 심의 항목 생성 및 진단평가 기능 제공
컴플라이언스 진단 평가	<ul style="list-style-type: none"> 등록된 컴플라이언스 별 진단 평가 생성 및 등록된 평가자에 의한 평가 결과 등록 진단 평가 항목 별 관련 법령 정보 제공 항목 별 평가 근거 증거 파일 등록 업로드 증거에 대한 미리보기 기능 지원
컴플라이언스 취약점 조치	<ul style="list-style-type: none"> 취약점 별 조치담당자 지정 및 조치요청 조치에 따른 이행 점검 프로세스 제공
보고서 자동생성	<ul style="list-style-type: none"> 컴플라이언스 별 진단평가 결과 보고서 자동 생성 컴플라이언스 별 진단결과 증거 일괄 다운로드

컴플라이언스 진단 평가

인증심사 진단 평가 세부 조회 및 증적 파일 등록

The screenshot displays the 'Compliance' dashboard. The main area shows a table of audit items. A red box highlights a specific item, '원격 로그 서버 사용' (Remote Log Server Usage), which is marked as '평가결과 등록 및 결과 정보' (Evaluation Result Registration and Result Information). Below this, a table titled '증적 등록' (Evidence Registration) shows a list of uploaded files, including a document and a PDF, with a red box highlighting the '증적 파일 등록' (Evidence File Registration) section.

No	항목 ID	항목명
1	ISS-001	보안장
2	ISS-002	원격 로
3	ISS-003	DMZ
4	ISS-004	외부구
5	ISS-005	최신/2
6	ISS-006	보안장
7	ISS-007	보안장
8	ISS-008	방화벽
9	ISS-009	위험도
10	ISS-010	TCP/IP
11	ISS-011	Port S
12	ISS-012	핵심
13	ISS-013	불필요

인증심사 진단 평가 세부 항목

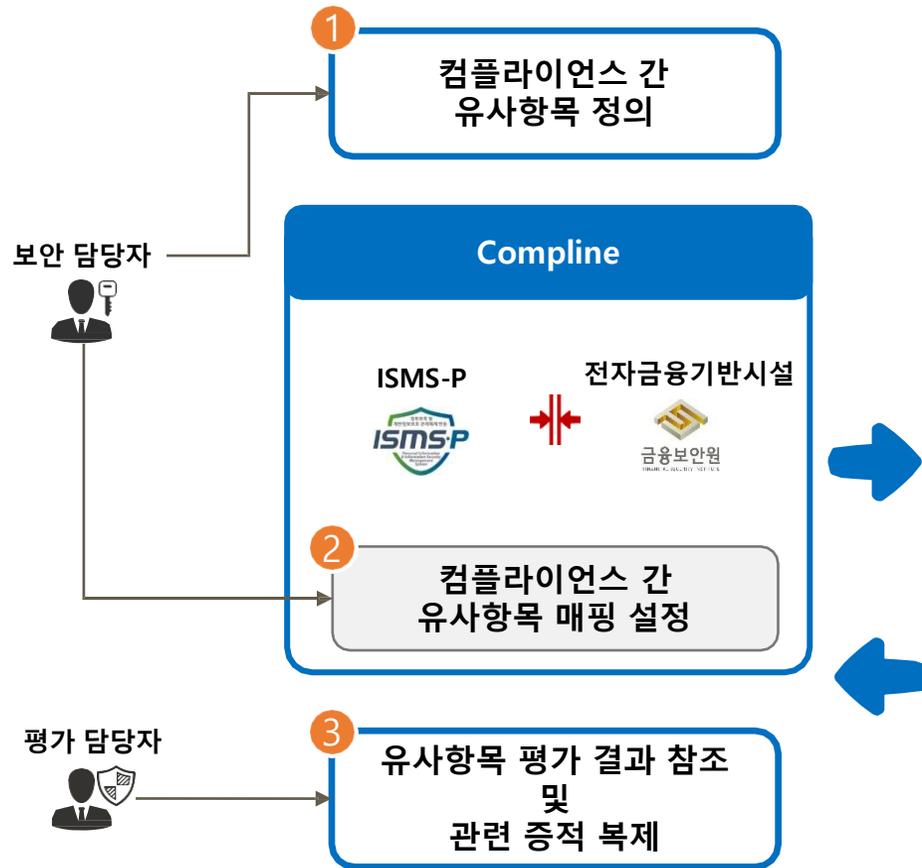
평가결과 등록 및 결과 정보

증적 파일 등록

- 진단 평가 수행
 - 평가기간 확인
 - 담당자/수행자 확인
 - 등록일자 확인
- 진단 평가 세부 항목 제공
 - 세부항목 확인
 - 항목 별 진행상태/평가결과 확인
- 항목 별 증적 파일 통합
 - 평가결과/평가의견/조치방안 확인
 - 증적 파일 등록 확인
 - 항목 별 내용 확인
 - 유사항목 비교

컴플라이언스 유사 항목 정보 제공

컴플라이언스 평가 유사 항목 매핑을 통한 평가 결과 참조 및 관련 증적 복제



ISMS-P 항목에 대한 전자금융기반시설 유사항목 정보 제공(예시)

ISMS-P 항목 정보

항목ID	1.1.3
항목명	조직 구성
항목유형	ISMS-P 항목 정보
위험도	상
배점	0
등록일자	2023-03-20

전자금융기반시설 유사 항목정보

항목명	전자금융기반시설 평가
기준년도	2023년
항목ID	FISM-012
항목명	정보보호 관련 사항을 심의·의결하는 정보보호위원회 설치 및 운영 여부
평가의견	정보보호위원회 미운영
조지가이드	정보보호위원회 설치 후 운영 예정

유사항목 평가 결과 조회

등록일	파일명	비고
2022-11-15	FISM-012.txt	↓ ↑

컴플라이언스 진단 평가 결과 조회

인증심사 진단평가 결과 및 증거 확인

The screenshot displays the 'Compliance' dashboard with a sidebar on the left and a main content area. The main area is titled '진단 평가 정보' (Audit Evaluation Information) and shows details for '전자금융기반시설 평가' (Electronic Financial Infrastructure Evaluation). A table lists various audit items (항목) with columns for 'No', '항목 ID', and '항목명'. A red box highlights the '항목 별 진단 평가 목록' (Item-wise Audit Evaluation List) table. Another red box highlights the '증거 확인' (Evidence Verification) section, which includes a table for '증거 목록' (Evidence List) and a detailed view of '항목 세부 설명' (Item Detailed Description) for FISM-003. The detailed description includes a list of items and their corresponding evidence files.

No	항목 ID	항목명
3	FISM-003	정보처리시스템
4	FISM-004	전자금융업무 관
5	FISM-005	IT 아웃소싱(이하
6	FISM-010	정보보호최고책임
7	FISM-011	장기적으로 수행
8	FISM-012	정보보호 관련 사
9	FISM-013	정보보호위원회
10	FISM-014	정보보호위원회
11	FISM-015	정보보호위원회
12	FISM-016	정보안전점검의
13	FISM-017	정보안전 점검의

항목명	파일명
2022-11-15	FISM-003.txt

- 진단 평가 결과 조회
 - 항목 별 진행상태/평가결과 확인
 - 항목 별 평가결과 확인
- 항목 별 평가 결과 및 증거 확인
 - 평가결과/평가의견/조치방안 확인
 - 증거 파일 등록 및 다운로드
- 인증심사 평가 기준 항목
 - 세부 항목 기준 확인
 - 유사항목 확인 및 진단내역 조회

컴플라이언스 진단 조치 이력관리(이행점검관리)

인증심사 진단평가 결과 조치(이행) 필요 항목에 대한 조치 워크플로우 제공

The screenshot displays the 'Compliance Management' dashboard. It features a sidebar with navigation options like 'Dashboard', 'Groups/User Management', 'Project Management', 'Asset/Requirement Management', 'Audit Management', 'Requirement Setting', 'Compliance Requirement Management', 'Action Management', and 'System Management'. The main content area is titled '관리적 진단평가 관리' and includes several summary cards and a detailed table.

진단 결과 요약정보 제공

- 진단 신청 정보:** 기준년도 2023, 평가유형 전자금융기반시설(관리체계), 진단평가명 전자금융기반시설 평가, 평가기간 2023-01-01 ~ 2023-10-26, 평가자 채지수, 담당자 시스템 관리자.
- 평가 대상 진단내역 요약:** 총 277개 항목 (양호 243개, 취약 34개).
- 조치상태 요약:** 총 34건 (미조치).
- 위험도 별 조치진행상태:** 높음 33개, 다소높음, 보통, 다소낮음, 낮음.

조치 필요 항목 상세 정보 제공

No	상세보기	위험도	진단결과	조치상태	조치 예정 일자	항목ID	항목명
1	상세보기	낮음	취약	미조치		ABC_01	ABC 01 항목
2	상세보기	높음	취약	미조치		FISM-003	정보처리시스템 관련 전달조치 운영 여부
3	상세보기	높음	취약	미조치		FISM-012	정보보호 관련 사항을 심의·의결하는 정보보호위원회 설치 및 운영 여부
4	상세보기	높음	취약	미조치		FISM-013	정보보호위원회 구성의 적정성
5	상세보기	높음	취약	미조치		FISM-015	정보보호위원회 심의·의결 사항에 관한 임원(정보보호최고책임자, 최고경영자) 보고 여부
6	상세보기	높음	취약	미조치		FISM-020	정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 전자금융감독규정에서 정한 기준에 따른 주기(매년)적 교육 시행 여부
7	상세보기	높음	취약	미조치		FISM-021	정보보호 교육 실시 이후, 대상 임직원에게 대한 평가 수행 여부
8	상세보기	높음	취약	미조치		FISM-022	건물 출입통제보안대책의 수립/운영 여부

조치 대상 결과 워크플로우

- 취약, 미이행, 미운영 등 컴플라이언스 항목 별 조치/이행이 필요한 항목에 대한 상태 정보 제공
- 조치/이행 담당자를 지정하여 조치 요청 및 이행여부 확인 워크플로우 제공

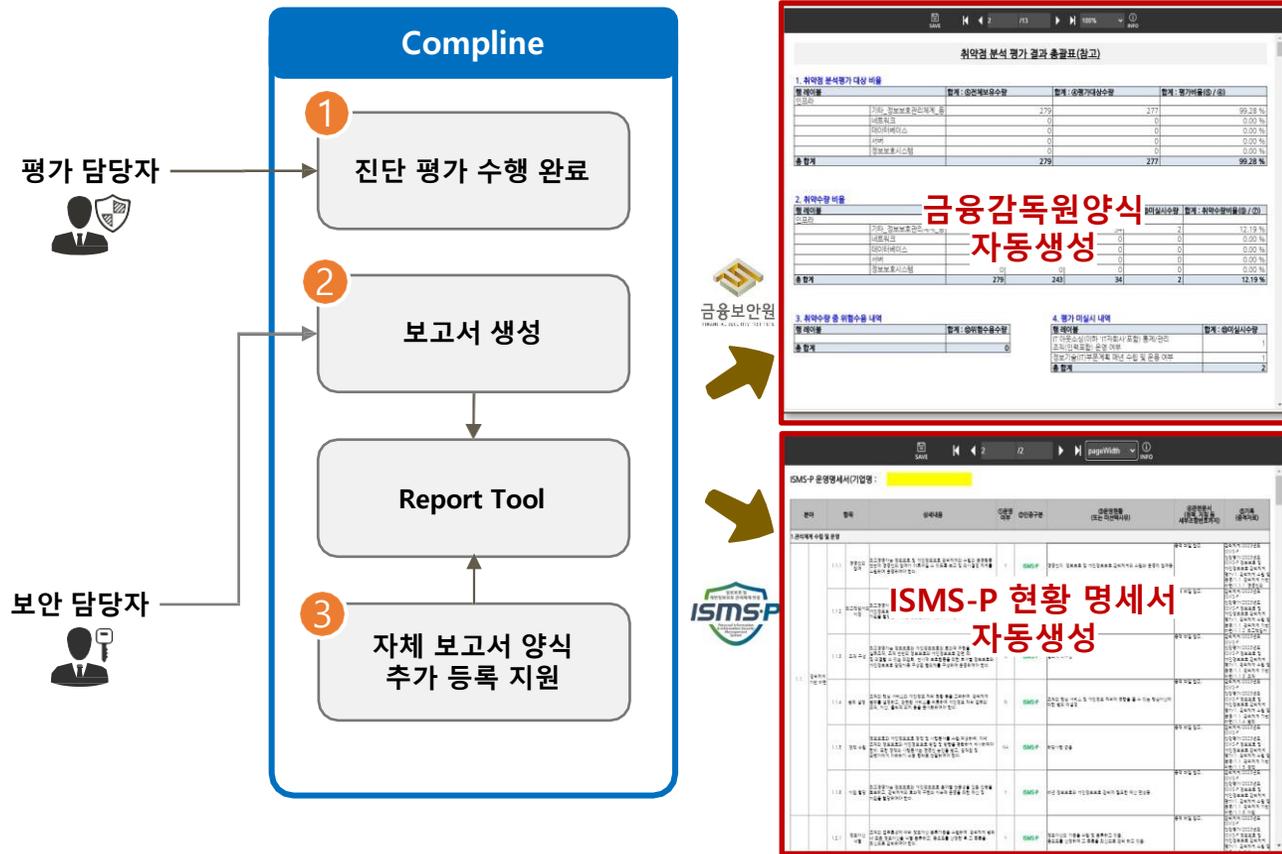
조치 여부에 따른 상태 값 제공

취약 항목 상세정보 제공

- 위험도/조치상태 별 조회
- 취약점 조치 상태 확인/신청
- 항목 별 상세정보 제공

컴플라이언스 보고서 및 산출물 자동 생성

보고서 자동 생성 및 증거 파일 일괄 다운로드



기능구분	기능 상세
컴플라이언스 보고서 및 증거 파일	<ul style="list-style-type: none"> 컴플라이언스 별 평가 결과 기반 제출 보고서 자동 생성 지원 고객사 보고서 양식을 유지하여 자동 보고서 생성 지원 평가 완료 컴플라이언스에 대한 증거 일괄 다운로드 지원
다양한 보고서 파일 포맷 지원	<ul style="list-style-type: none"> 자체 내장 리포트틀을 이용하여 보고서 생성 시 미리보기 지원 미리보기 보고서를 다양한 파일 포맷으로 저장 가능(word, excel, ppt, pdf 등)
내부 보고서 생성 확장	<ul style="list-style-type: none"> 자산, 취약점, 컴플라이언스 평가 정보 등 Comply 솔루션에 저장된 데이터를 기반한 다양한 보고서 생성 커스터마이징 가능 내장된 리포트 틀에 의한 신규 보고서 개발 기간 단축 및 지속적인 확장 가능

다양한 보고서 양식 출력 지원

다양한 양식의 보고서 자동 생성 및 커스터마이징 지원(리포팅 툴 내장)

주요정보통신기반시설 양식

'19년도 0000 소관 기반시설 보호대책(요약)

- 추진목표 ※ I 추진목표 및 전략을 토대로 작성
 - 사이버 위협 탐지·제거를 통한 기반시설 안정적 운용 기반 마련
- 기반시설 현황
 - (시설현황) 0개 관리기관, 0개 기반시설
- 소요예산 및 인력 ※ III 소요예산 및 자원을 토대로 작성

구분	'20(A)	'21(B)	증감(B-A)	증감률
정보보호 예산(백만원)	00,00	00,00	△ 0,00	△ 0.0%
정보보호 인력(내부/위탁)	000/000명	000/000명	△ 00명	△ 0.0%
- 정보보호 추진계획 ※ V.정보보호 추진계획을 토대로 작성
 - (예방) ~~~~
 - (대응·복구) ~~~~
- 정보보호 추진실적 ※ IV.정보보호 추진실적을 토대로 작성
 - '19년도 보호대책 이행 결과
 - (주요 이행과제) 0개 과제(~~~ 등)를 수립·추진하여 0개 완료
 - '20년도 취약점 분석·평가 결과

구분	'19년도 취약점		20년도 취약점			취약점 조치계획		
	도출	조치 완료	'19년도 잔여 (A)	신규 (B)	계 (A+B)	단기 (6개월)	중기 (21년도)	장기 (3년 이내)
관리								
물리								
기술					NaN			
합계	0	0	0	0	0	0	0	0

금융위원회 양식

<참고> 취약점 분석평가 결과보고서 표지 양식

년도
취약점 분석·평가 결과보고서

취약점 분석 평가 결과 총괄표(참고)

1. 취약점 분석평가 대상 비율

항 레이블	합계: ①전체보유수량	합계: ②평가대상수량	합계: 평가비율(②/①)
인프라			
기타_정보보호관리체계_등	0	0	0.00%
네트워크	16	0	0.00%
데이터베이스	34	1	2.94%
서버	218	7	3.21%
정보보호시스템	4	0	0.00%
총 합계	272	8	2.94%

2. 취약수량 비율

항 레이블	합계: ①평가수량	합계: ②양호수량	합계: ③취약수량	합계: ④미실시수량	합계: 취약수량비율(③/①)
인프라					
기타_정보보호관리체계_등	0	0	0	0	0.00%
네트워크	0	0	0	0	0.00%
데이터베이스	9	6	3	0	33.33%
서버	532	417	108	7	20.30%
정보보호시스템	0	0	0	0	0.00%
총 합계	541	423	111	7	20.52%

컴플라인 양식

인프라 보안진단 요약 보고서

<시트 목차>

1. 표지
2. 종합_보안현황
3. 상세취약점현황_OS
4. 상세취약점현황_DB
5. 상세취약점현황_WEB
6. 첨부_진단항목

진 단 명: ~

진 단 기 간: ~

보고서 작성일: 2021-10-26 09:53:55

Reference 레퍼런스

공공기관



금융기관



기업고객





대표번호 : 02-6407-6001



영업문의 sales@intbridge.co.kr



기술문의 : tech@intbridge.co.kr



서울특별시 영등포구 선유로 70,우리벤처타운2 703호

감사합니다.