

**정보보호 인증 통합 플랫폼**

# Compline 제품 소개서

2023.04

# 취약점은 있지만 취약점 통합 관리는?



DB취약점



WEB/WAS 취약점



소스코드 취약점



보안관제



네트워크 취약점



서버 취약점



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

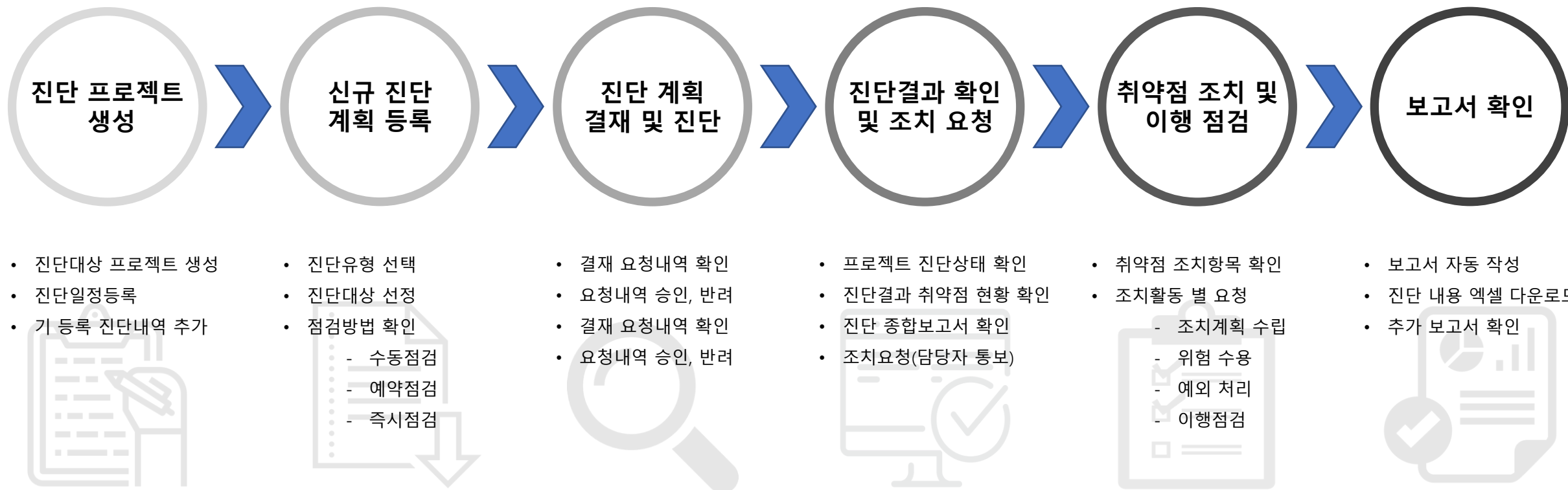
발견된 취약점에 대해 조치 이력을 관리하여 지속적인 정보보안 수준 상태 확인이 필요

# 매년 늘어나는 정보보호 인증 비용

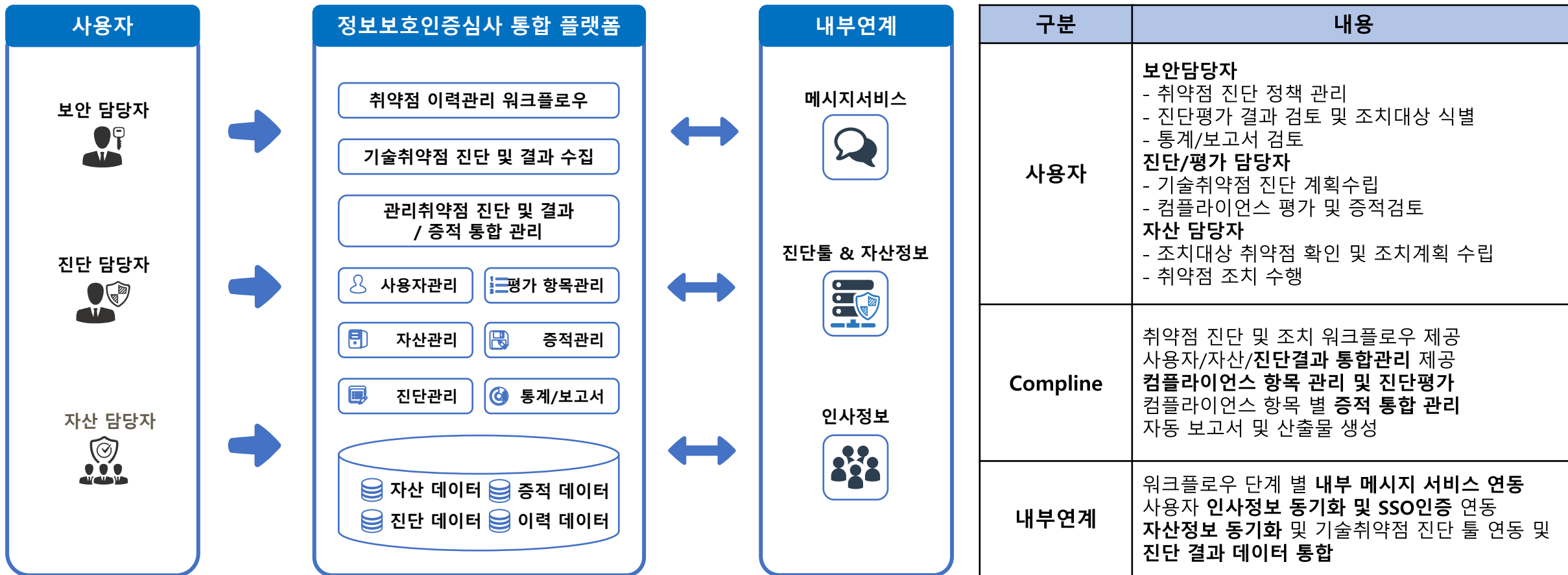
- 주요 정보통신 기반시설
- 전자금융 기반시설
- ISMS
- ISMS-P 인증
- ISO/IEC 27001
- 정보보안 관리실태 평가
- CSAP
- PCI DSS



## 취약점 점검업무 표준 프로세스

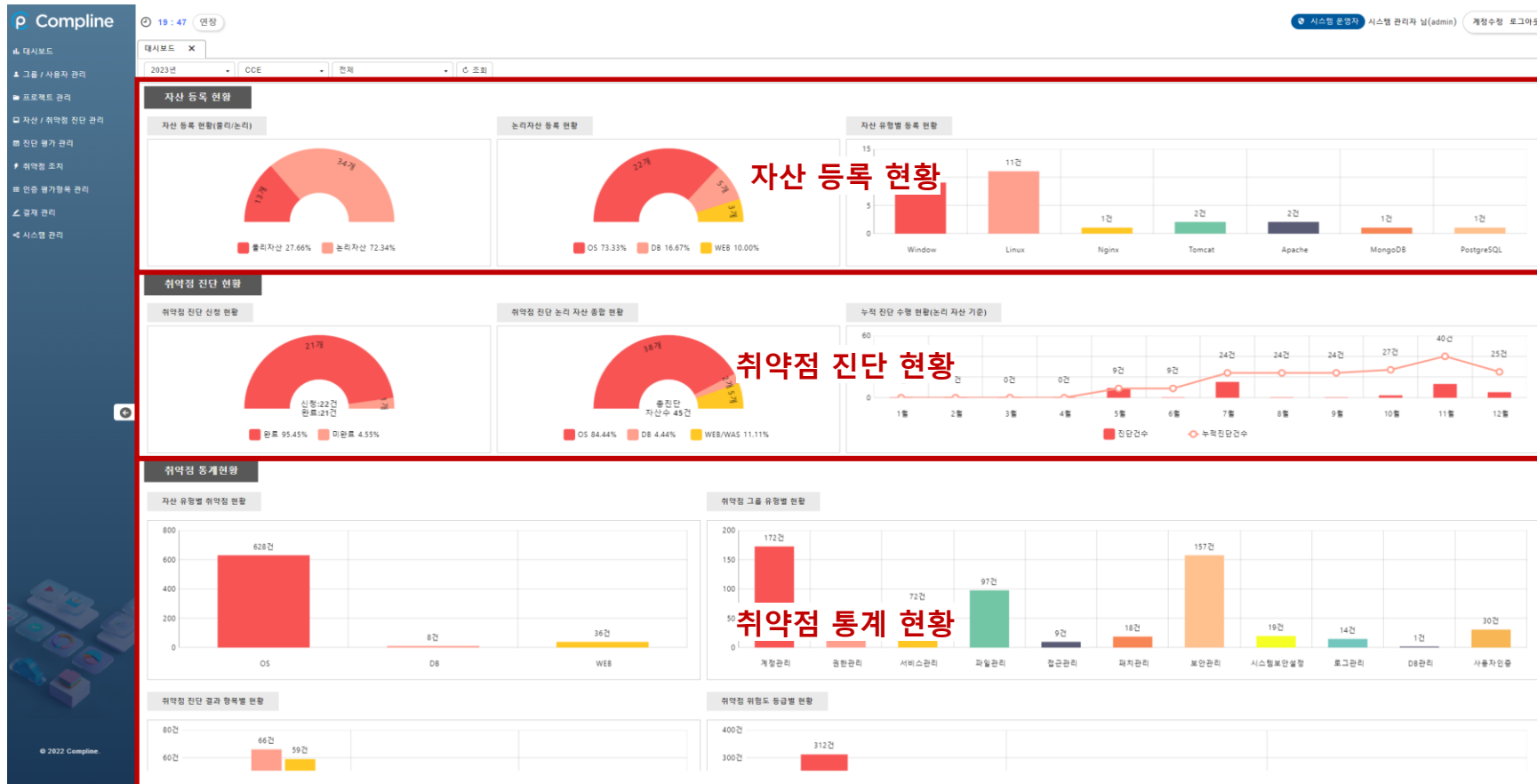


# 정보보안 인증 통합관리 플랫폼 구성 개요



# 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

# 자산관리

## 자산 그룹 별 자산 관리 지원

The screenshot displays the Compline web interface for asset management. It includes a sidebar with 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 central dashboard with donut charts for 'ALL' (OS: 38, WEB: 5, DB: 2, NETWORK: 1), 'OS: 자산현황 조회' (Linux: 29, Windows: 9, Solaris: 1), 'WEB' (Tomcat: 2, Jboss: 1, Apache: 2), and 'NW' (Cisco: 1).
- 자산 그룹 조회 (Asset Group Query):** A table listing assets with columns for Agent status, Hostname, IP, Asset Group, Asset Type, and Asset Category.
- 자산 상세 조회 (Asset Detail Query):** A detailed view for asset GWAPP-1, showing host details, asset group, and evaluation type.

- 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 web interface for asset management. The left sidebar contains navigation menus for '대시보드', '그룹 / 사용자 관리', '프로젝트 관리', '자산 / 취약점 진단 관리', '진단 평가 관리', '취약점 조치', '인증 평가목록 관리', '결과 관리', and '시스템 관리'. The main content area is titled '자산관리' and includes a '평가유형' (Evaluation Type) filter. A table shows asset counts: OS (1), WEB (1), DB (0), NETWORK (0), and 합계 (2). Three donut charts show the distribution: ALL (1), OS (1), and WEB (1). A table below lists assets with columns for Agent 상태, 호스트명, IP, 자산 구분, 자산 유형, 자산 종류, 상세 정보, 서비스명, 진단 옵션, 담당자(정), and 담당자(부). Two assets are listed, both with '완성' status. A red box highlights the '평가유형 별 자산 분류' section in the sidebar and the '자산목록' table.

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

The screenshot displays the 'Compline' web application interface. The main area shows a table titled '인프라 취약점 진단 목록' (Infrastructure Vulnerability Assessment List) with columns for No, 진단유형 (Assessment Type), 진단신청명 (Assessment Name), 자산현황 (Asset Status), 진행상태 (Progress Status), 진단결과 (Assessment Result), 진단예약일시 (Assessment Reservation Time), 진단시작시간 (Assessment Start Time), 결과수집일시 (Result Collection Time), 신청자 (Applicant), and 신청일 (Application Date). The table lists 14 items, all of type '인프라' (Infrastructure).

An overlay window titled '진단 계획 세부 정보' (Assessment Plan Details) is shown, providing information for a selected plan. It includes sections for '진단 정보' (Assessment Info), '신청자 정보' (Applicant Info), and '승인자 정보' (Approver Info). The '진단 정보' section includes details like '진단 유형' (Server/Infra(CCE)), '진단 구분' (Pre-assessment), '진단 템플릿' (Pentest-Tool/Tool-based), '진단 예정일' (2023-03-31 10:00), and '진단 신청명' (2023년 03월 마지막주 인프라 정기점검).

The '신청자 정보' section shows the applicant as '시스템 관리자' (System Administrator) with a personal information protection notice. The '승인자 정보' section shows the approver as '재지수' (Jaejisoo) with a personal information protection notice and a statement that the user is authorized for regular infrastructure maintenance checks.

- 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

# 모의해킹 진단 결과 통합

## 모의해킹 결과 직접 작성 및 등록

- 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 조치 가이드 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**

등록 가능 여부	자산명	URL	자산 구분	자산 유형	자산
가능	홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹

- 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 결과보고서를 활용하여 일괄 등록 양식으로 기능 제공

# 기술 취약점 진단 이력관리

## 취약점 데이터 통합에 따른 조치이력관리 워크플로우 제공

The screenshot displays the 'Compline' dashboard with a sidebar on the left containing navigation options like '대시보드', '그룹 / 사용자 관리', '프로젝트 관리', '자산 / 취약점 진단 관리', '자산 관리', '취약점 진단 일정표', '취약점 진단 계획', '진단 평가 관리', '취약점 조치', '인증 평가항목 관리', '결과 관리', and '시스템 관리'. The main content area is titled '진단결과' and includes several summary cards and a detailed table.

**진단결과 통계 정보제공(모의해킹 예시)**

항목	내용	진단 자산 목록	취약점 위험도 등급별 현황	총 취약점 개수	취약점 진단결과 항목별 현황
그룹명	개인 정보 보호팀			총 집계 67개	
진단신청자	재지수			취약 100.00%	
진단신청명	홈페이지의모의해킹결과				

**항목 별 모의해킹 취약점 내역(모의해킹 예시)**

No	상세보기	위험도	인단결과	조치상태	조치 예정 일자	자산명	URL	자산구분	자산유형	종류	영속코드	영
1	상세보기	높음	취약	이행점검 승인완료		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-FIN-017	전자금융 사용자 입
2	상세보기	다소높음	취약	이행점검 승인완료		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-027	데이터 전송
3	상세보기	다소높음	취약	이행점검 승인완료		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-027	데이터 전송
4	상세보기	다소높음	취약	예외처리 승인완료		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-029	디렉토리 목록 노출
5	상세보기	다소높음	취약	조치완료		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-040	불필요한 파일 노출 여
6	상세보기	다소높음	취약	미조치		홈페이지	https://www.homepage.com	어플리케이션	웹	일반 웹	WEB-SER-041	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 system interface with several overlapping windows. The main window shows a table of assessment results. Overlaid windows include:

- 진단 이력 (Assessment History):** A table with columns for sequence number, assessment category, result, and completion date.
- 취약점 정보 (Vulnerability Information):** A window showing details for a specific vulnerability, including its ID, severity, and remediation status.
- 취약점 상세내역 (Vulnerability Details):** A window providing a step-by-step guide for remediation, such as updating software or configuring security settings.
- 조치 이력 (Remediation History):** A table listing remediation actions, including the user who performed them, the date, and the specific remediation details.

Red boxes highlight these key areas, and a red text box in the center reads: **진단이력 조회 (모의해킹 예시)** (Assessment History Search (Penetration Test Example)).

- 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 항목 관리 및 진단 평가 가능**

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

# 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 'IT자회사'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 임직원 정보보안 관련법규 준수여부 점검결과에 대한 임원(정보보호 최고경영자)보고 여부	On		2022년 08월 17일
FISM-012	정보보호 관련 사항을 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

**항목 카테고리**

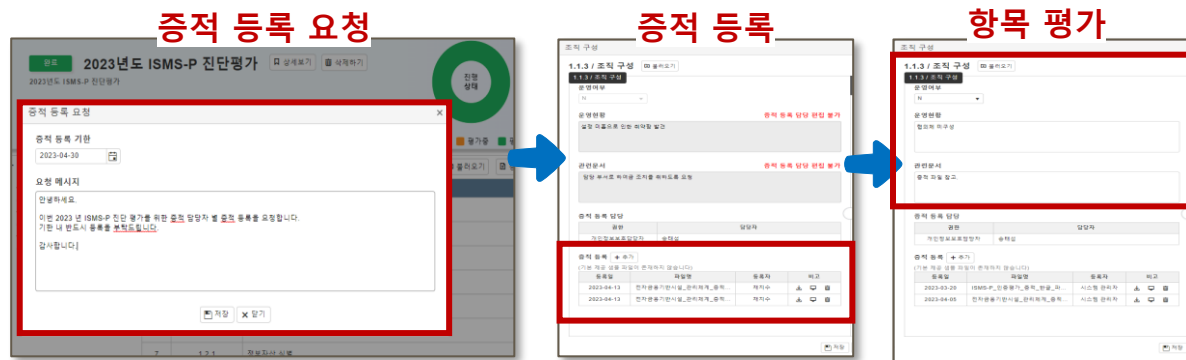
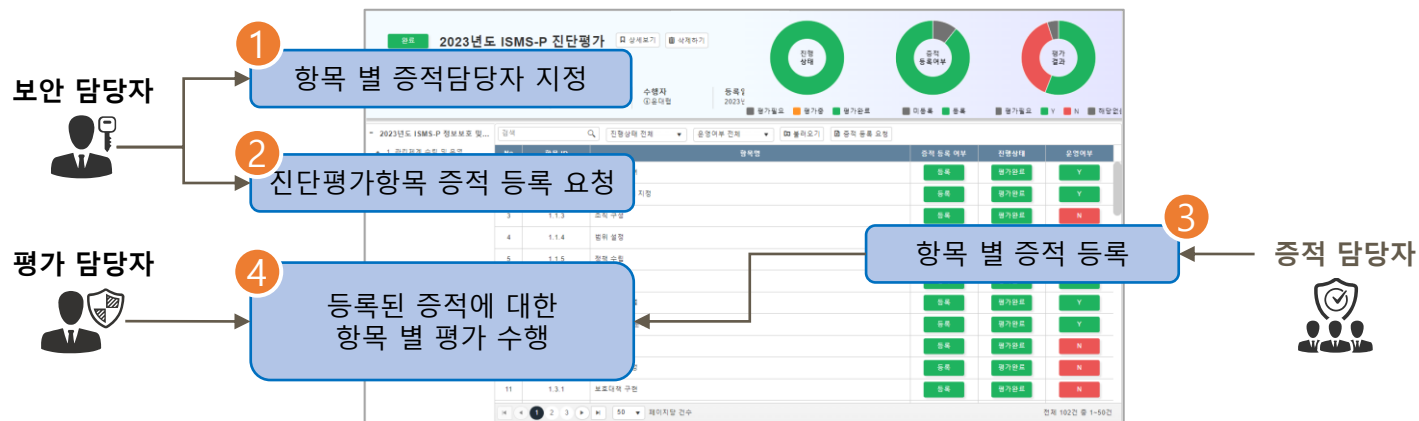
- 항상적보안
- 관리적보안
- 물리적보안
- 기술적보안

**세부 항목 정보 관리**

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



# 컴플라이언스 진단 평가

## 인증심사 진단 평가 세부 조회 및 증거 파일 등록

Compline 18:54 연장 시스템 운영자 시스템 관리자 님(admin) 계정수정 로그아웃

기술적 진단 평가 관리

완료 정기 보안장비 취약점 진단평가 인증심사 진단 수행

진단 평가 기간: 2023년 02월 01일 ~ 2023년 02월 17일 담당자: 시스템 관리자

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

원격 로그 서버 사용

ISS-002 / 원격 로그 서버 사용

평가결과: 취약

평가의견: 로그서버와 연결되어 있지 않음

조치방안: 로그서버와 연결구성이 필요

증거 등록 + 추가

(기본 제공 샘플 파일이 존재하지 않습니다)

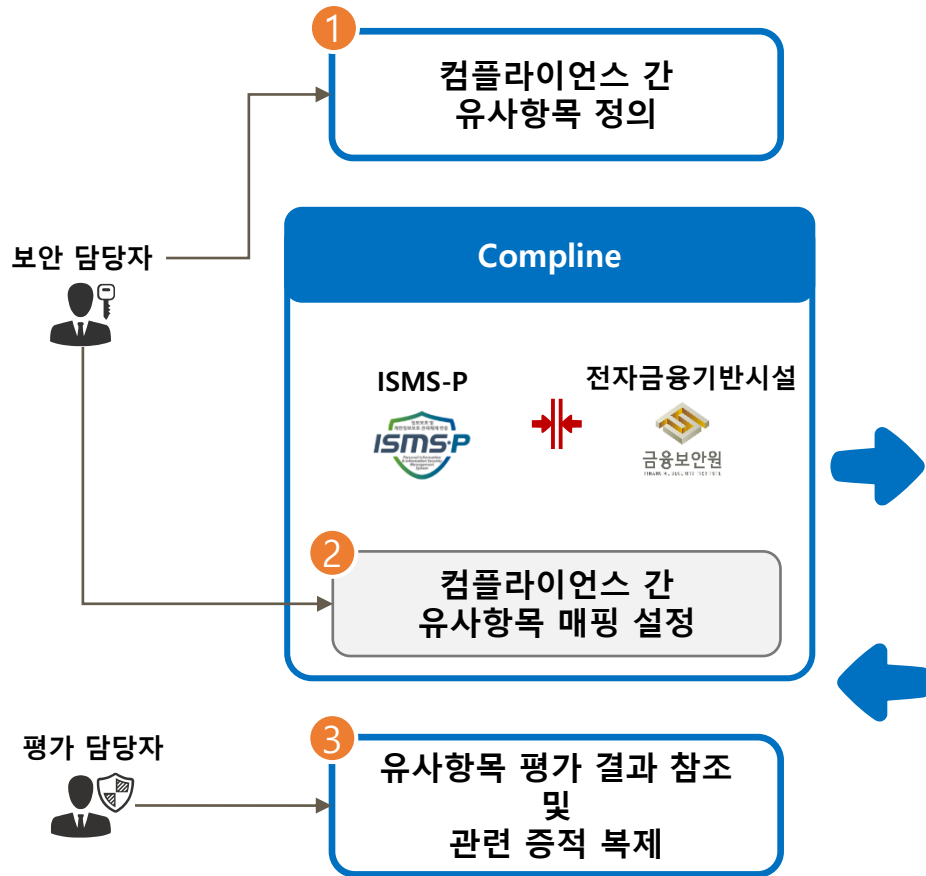
등록일	파일명	증거 파일 등록
2023-02-14	2266593E	증거 파일 등록
2023-02-14	컴플라이언스_모의해킹결과보고서_샘플_데이터.docx	증거 파일 등록
2023-02-14	원격로그서버설정확인.pdf	증거 파일 등록

인증심사 진단 평가 세부 항목

- 진단 평가 수행
  - 평가기간 확인
  - 담당자/수행자 확인
  - 등록일자 확인
- 진단 평가 세부 항목 제공
  - 세부항목 확인
  - 항목 별 진행상태/평가결과 확인
- 항목 별 증거 파일 통합
  - 평가결과/평가의견/조치방안 확인
  - 증거 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**

항목ID	FISM-012
항목명	정보보호 관련 사항 심의·의결하는 정보보호위원회 설치 및 운영 여부

**유사항목 평가 결과 조회**

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

**증적 목록**

등록일	파일명	비고
2022-11-15	FISM-012.txt	다운로드

# 컴플라이언스 진단 평가 결과 조회

## 인증심사 진단평가 결과 및 증거 확인

The screenshot displays the 'Complye' system interface. The main content area is titled '진단 평가 정보' (Audit Evaluation Information) for '전자금융기반시설 평가' (Electronic Financial Infrastructure Evaluation). It shows the evaluation period from 2023.01.01 to 2023.10.26 and the administrator '시스템 관리자'.

A table lists the audit items, with '항목 별 진단 평가 목록' (Item-wise Audit Evaluation List) highlighted. The table includes columns for 'No', '항목 ID', and '항목명'.

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

The detailed view for 'FISM-003 / 정보처리시스템 관련 전담조직 운영 여부' shows the evaluation result, criteria, and evidence. The '증거 등록' (Evidence Registration) section shows a file named 'FISM-003.txt' uploaded on 2022-11-15. The '항목 세부 설명' (Item Detailed Description) provides regulatory references and requirements.

- 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 'Comply' system interface. The top navigation bar includes 'Comply' and user information. The main content area is titled '관리적 진단평가 관리' and contains several summary cards and a detailed table.

**진단 결과 요약정보 제공**

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

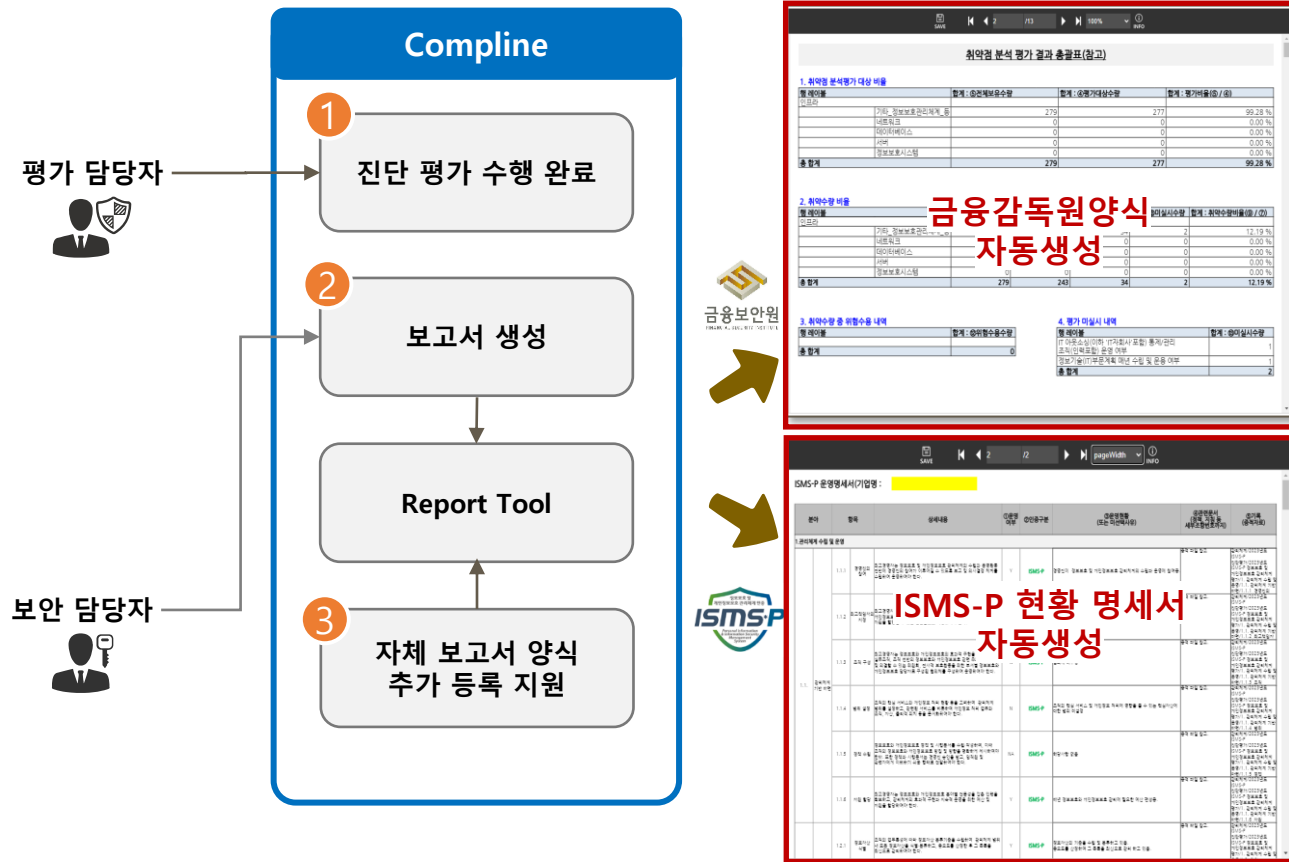
**조치 필요 항목 상세 정보 제공**

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	정보저리시스템 관련 전담조직 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 적정성
6	상세보기	높음	취약	미조치		FISM-015	정보보호위원회 심의·의결 사항에 관한 임원(정보보호최고책임자, 최고경영자) 보고 여부
7	상세보기	높음	취약	미조치		FISM-020	정보보호최고책임자는 임직원의 정보보호역할 강화를 위하여 필요한 교육프로그램을 개발하고, 전자금융감독규정에서 정한 기준에 따른 주기(매년)적 교육 시행 여부
8	상세보기	높음	취약	미조치		FISM-021	정보보호 교육 실시 이후, 대상 임직원에 대한 평가 수월 여부
9	상세보기	높음	취약	미조치		FISM-022	간통 줄임통계보안대책의 수립/운영 여부

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

# 다양한 보고서 양식 출력 지원

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

2019년도 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

[주요정보통신기반시설 양식]

<참고> 취약점 분석평가 결과보고서 표지 양식

### 년도 취약점 분석·평가 결과보고서

취약점 분석 평가 결과 총괄표(참고)

1. 취약점 분석평가 대상 비율

행 레이블	합계 : ④전체보유수량	합계 : ⑤평가대상수량	합계 : 평가비율(⑤ / ④)
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

행 레이블	합계 : ⑦평가수량	합계 : ⑧양호수량	합계 : ⑨취약수량	합계 : ⑩미실시수량	합계 : 취약수량비율(⑨ / ⑦)
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 %

[금융위원회 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: ~~~~~

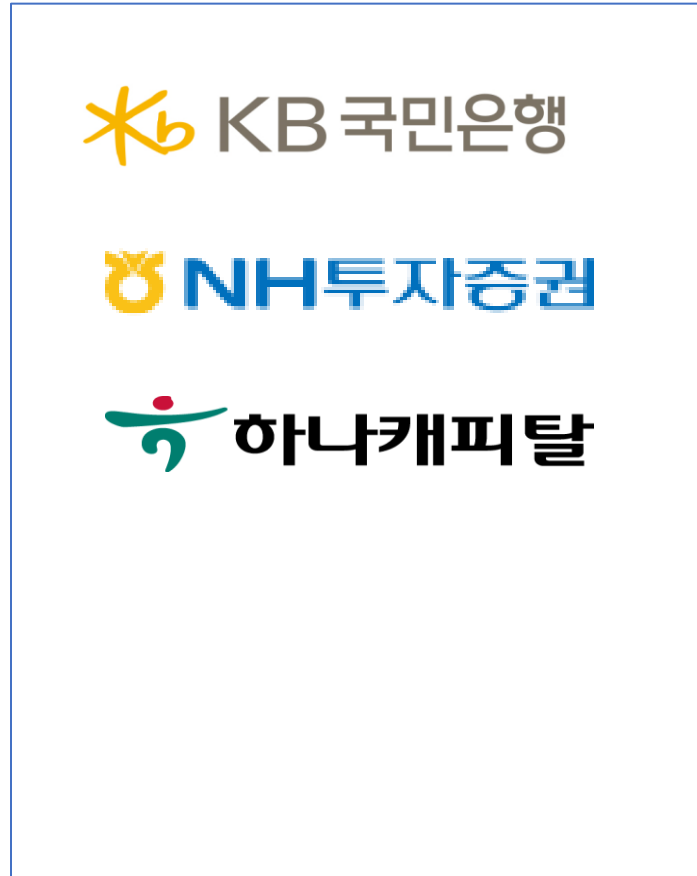
보고서 작성일: 2021-10-26 09:53:55

[컴플라인 양식]

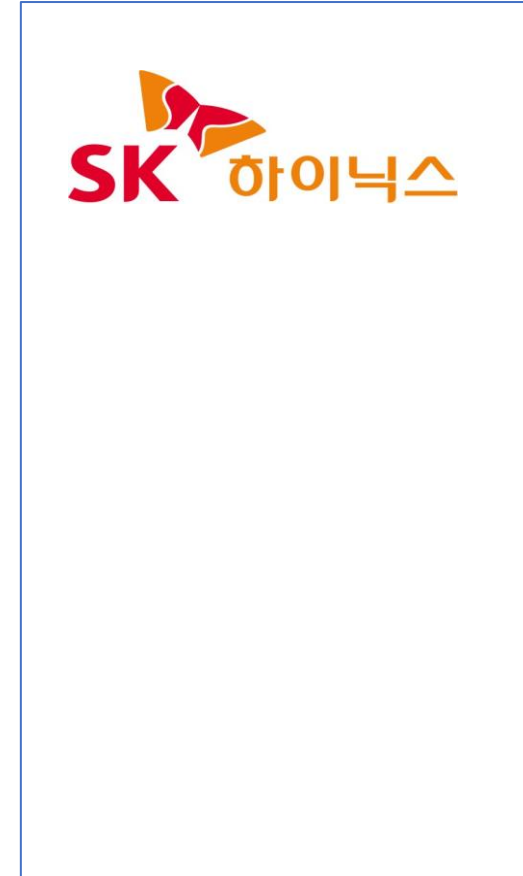
# Reference 레퍼런스



[공공기관]



[금융기관]



[기업]



대표번호 : 02-6407-6001



영업문의 [sales@intbridge.co.kr](mailto:sales@intbridge.co.kr)



기술문의 : [tech@intbridge.co.kr](mailto:tech@intbridge.co.kr)



서울특별시 영등포구 은행로 29 정우빌딩 716호

# 감사합니다.