Compline

정보보호 인증 통합 플랫폼

Compline 제품 소개서

2023.04

int bridge 인트브릿지

취약점은 있지만 취약점 통합 관리는?

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

진단 프로젝트 생성

- 진단대상 프로젝트 생성
- 진단일정등록
- 기 등록 진단내역 추가

신규 진단 계획 등록

- 진단유형 선택
- 진단대상 선정
- 점검방법 확인
  - 수동점검
  - 예약점검
  - 즉시점검

진단 계획 결재 및 진단

- 결재 요청내역 확인
- 요청내역 승인, 반려
- 결재 요청내역 확인
- 요청내역 승인, 반려

진단결과 확인 및 조치 요청

- 프로젝트 진단상태 확인
- 진단결과 취약점 현황 확인
- 진단 종합보고서 확인
- 조치요청(담당자 통보)

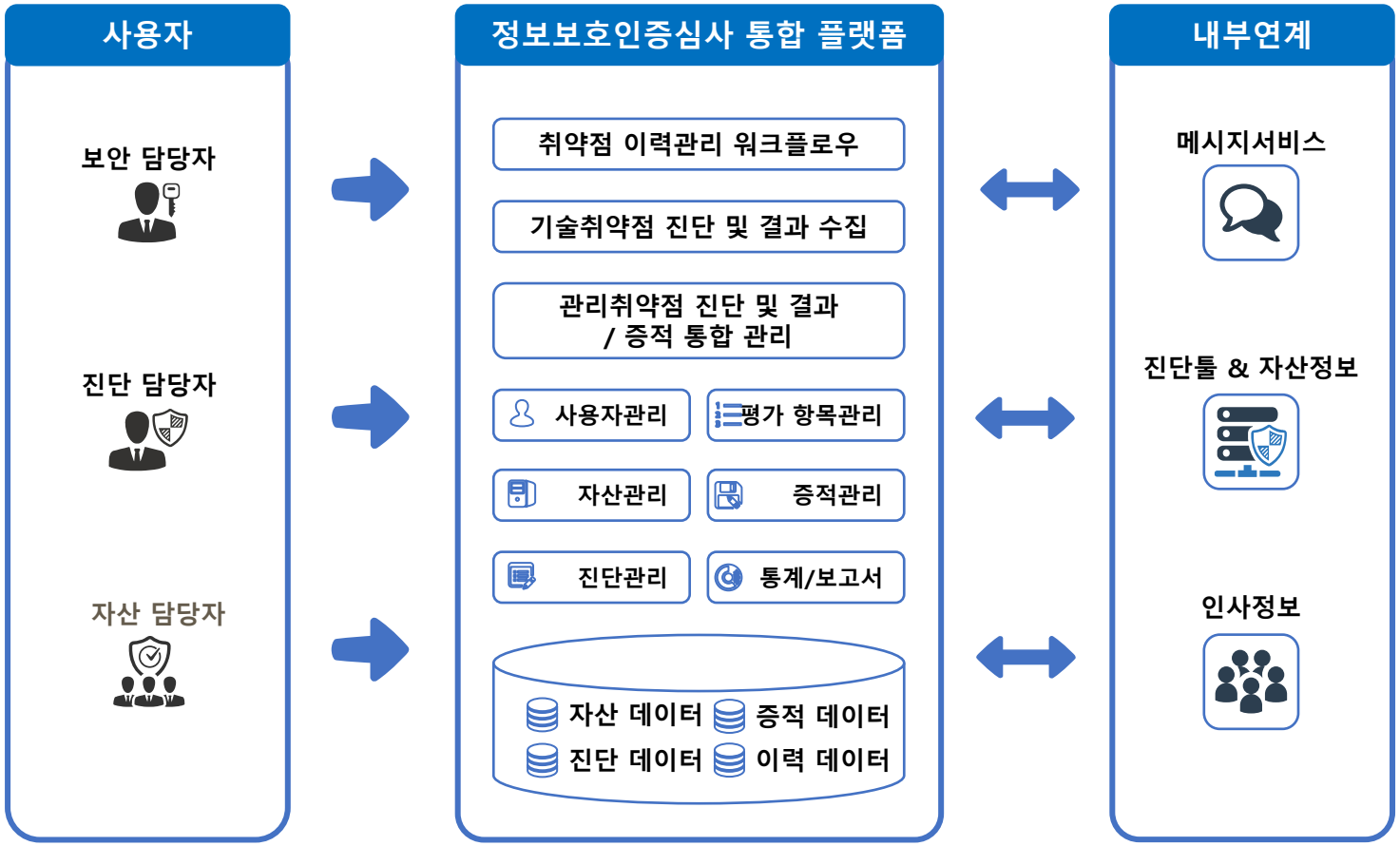
취약점 조치 및 이행 점검

- 취약점 조치항목 확인
- 조치활동 별 요청
  - 조치계획 수립
  - 위험 수용
  - 예외 처리
  - 이행점검

보고서 확인

- 보고서 자동 작성
- 진단 내용 엑셀 다운로드
- 추가 보고서 확인

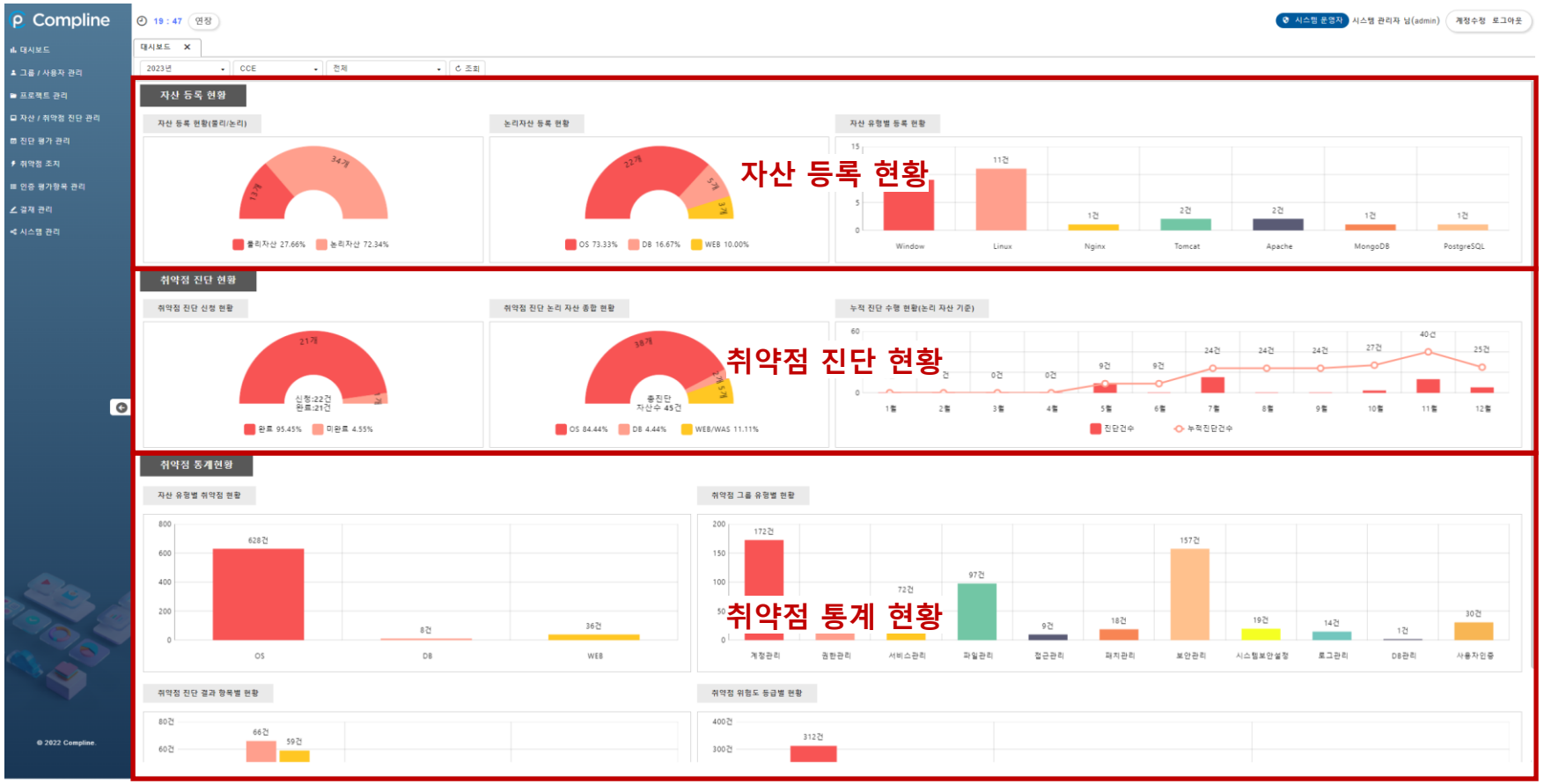
정보보안 인증 통합관리 플랫폼 구성 개요



구분	내용
사용자	**보안담당자** - 취약점 진단 정책 관리 - 진단평가 결과 검토 및 조치대상 식별 - 통계/보고서 검토 **진단/평가 담당자** - 기술취약점 진단 계획수립 - 컴플라이언스 평가 및 증적검토 **자산 담당자** - 조치대상 취약점 확인 및 조치계획 수립 - 취약점 조치 수행
Compline	취약점 진단 및 조치 워크플로우 제공 사용자/자산/**진단결과 통합관리** 제공 **컴플라이언스 항목 관리 및 진단평가** 컴플라이언스 항목 별 **증적 통합 관리** 자동 보고서 및 산출물 생성
내부연계	워크플로우 단계 별 **내부 메시지 서비스 연동** 사용자 **인사정보 동기화 및 SSO인증** 연동 **자산정보 동기화** 및 기술취약점 진단 툴 연동 및 **진단 결과 데이터 통합**

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

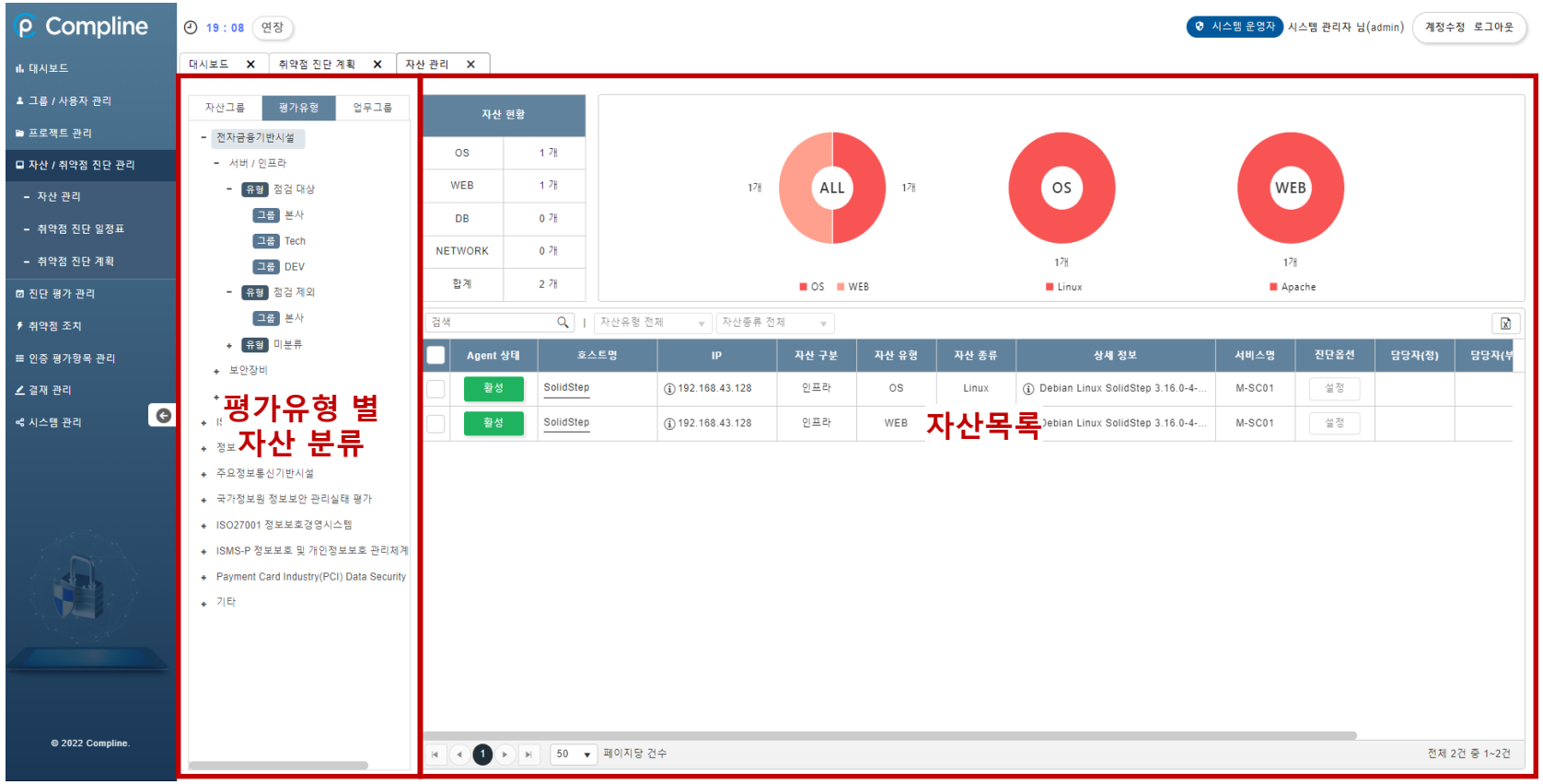
자산관리

자산 그룹 별 자산 관리 지원

- 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

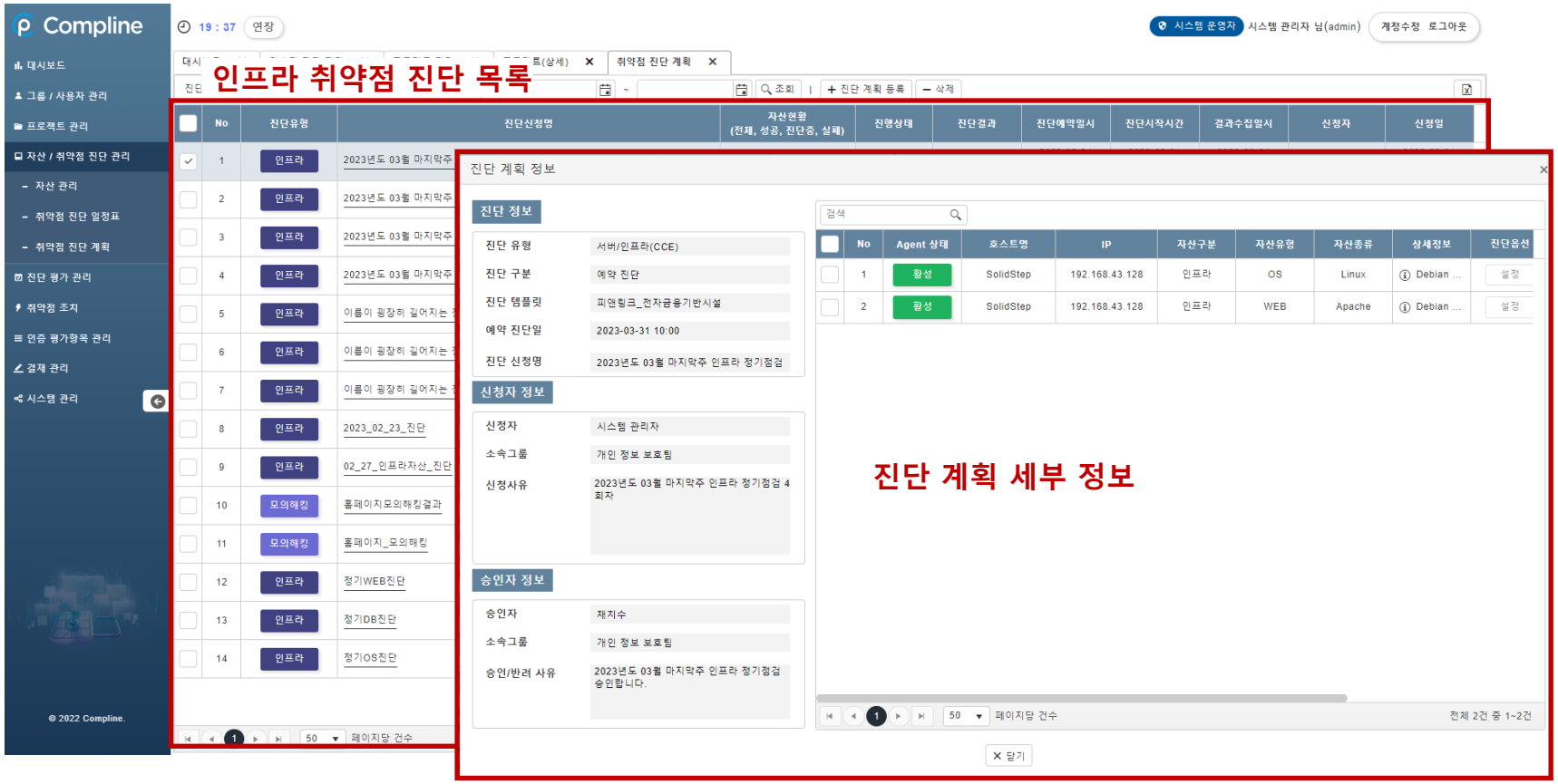
평가유형 별 자산 관리 지원



- 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

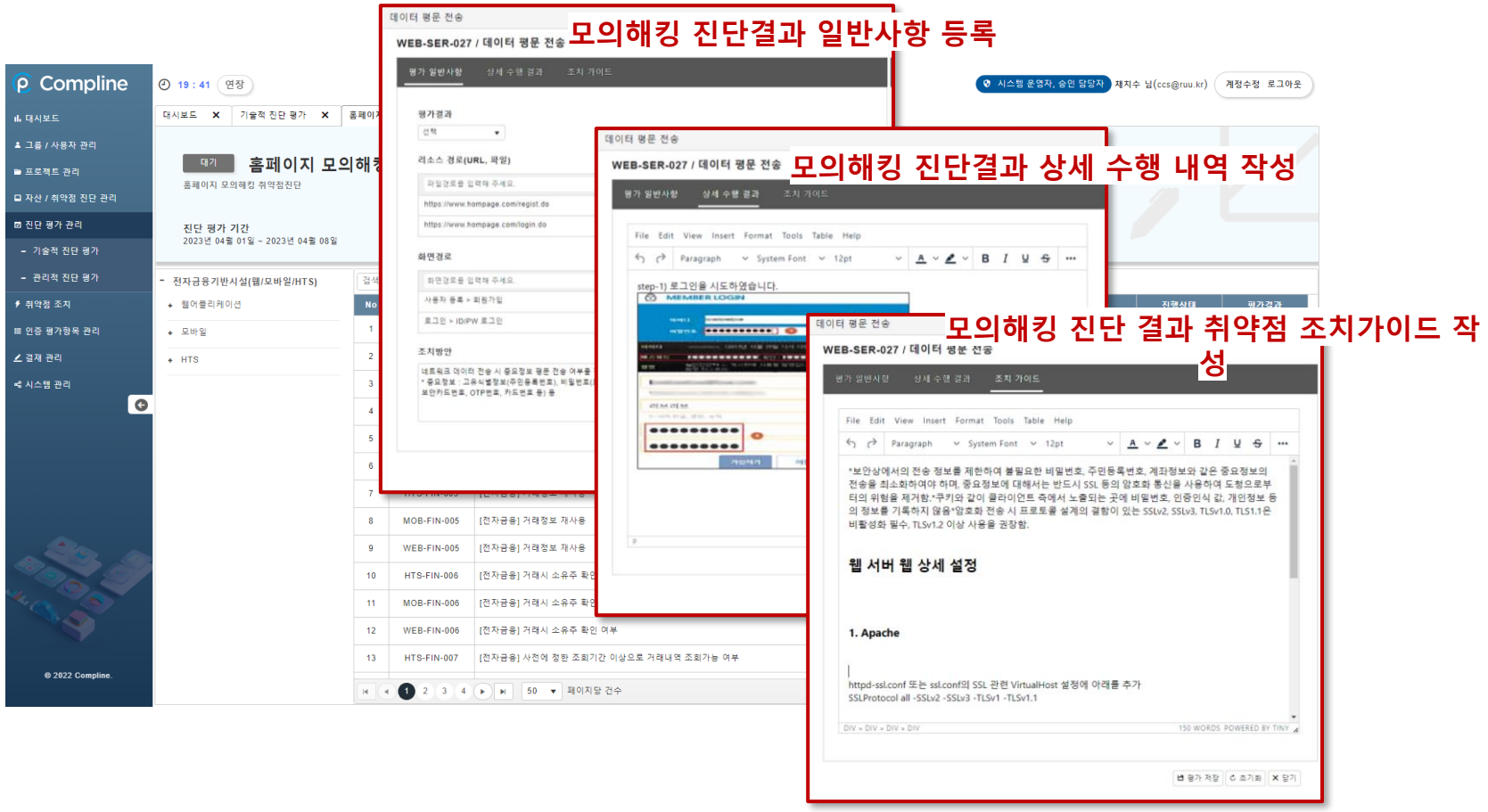
취약점 진단 계획 등록 및 진단 요청(진단 툴 연동)



- 인프라 취약점 진단 목록
  - 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

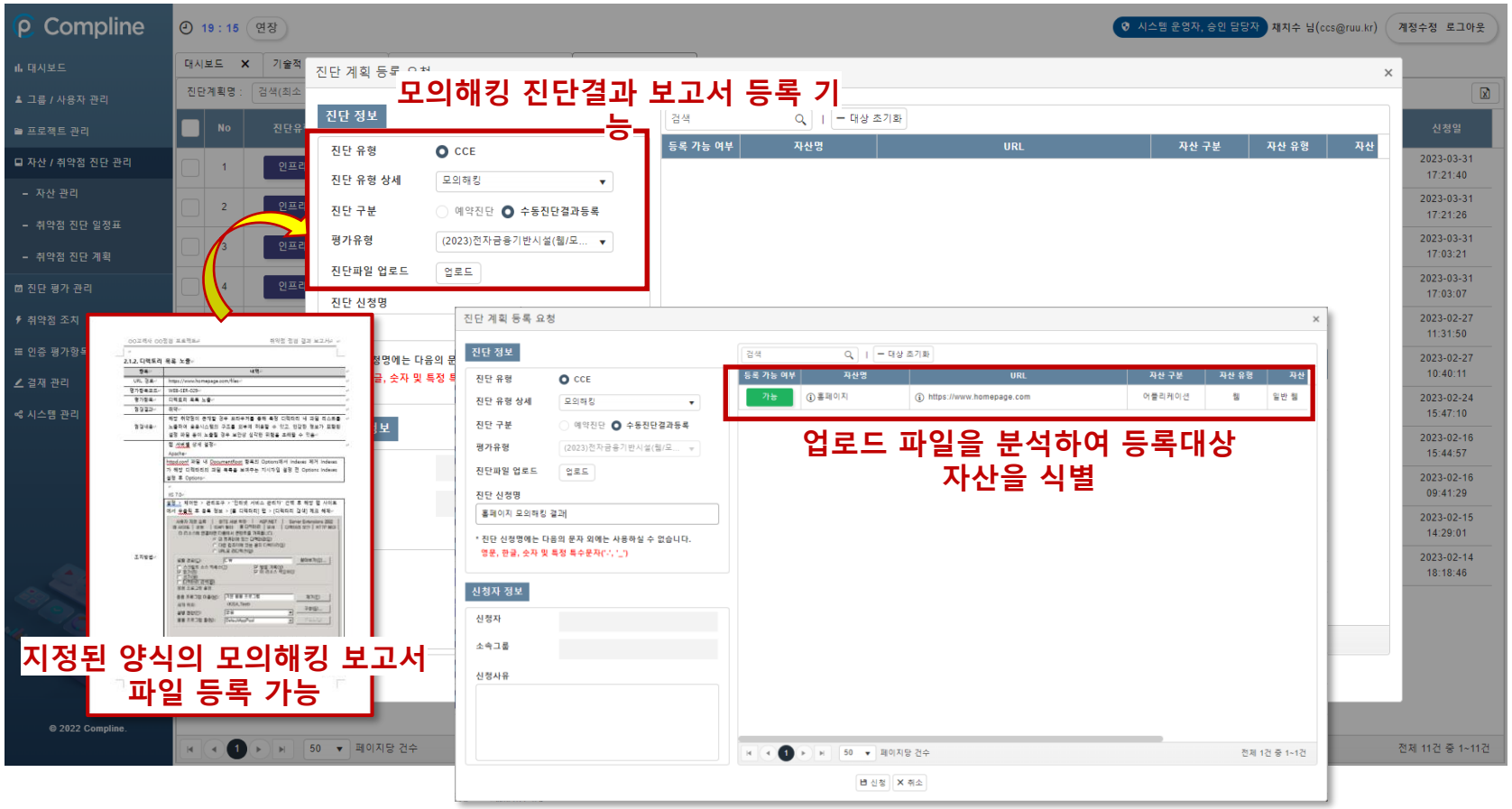
모의해킹 결과 직접 작성 및 등록



- 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 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 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

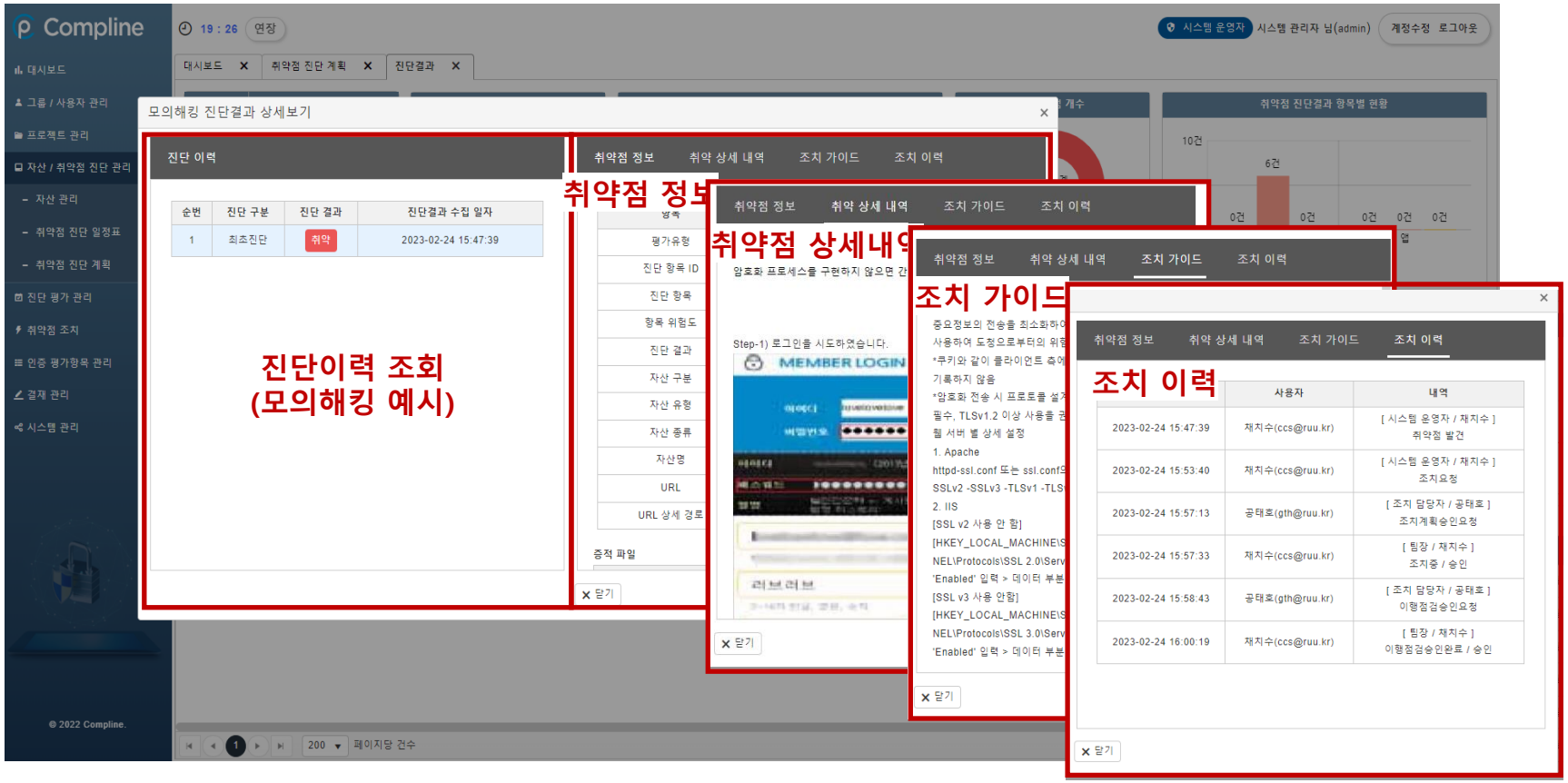
기술 취약점 진단 이력관리

취약점 데이터 통합에 따른 조치이력관리 워크플로우 제공

- 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



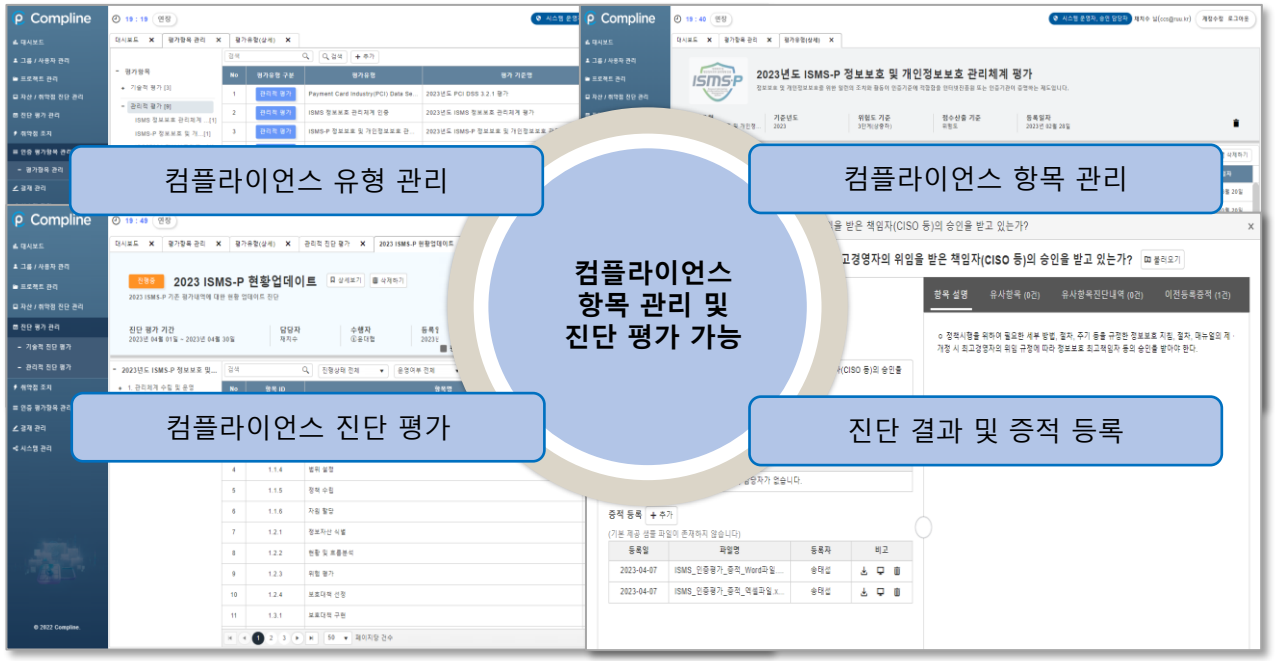
- 취약점 진단이력 조회
  - 진단결과 조회
  - 진단결과 수집 일자 조회
  - 취약점 개수 확인
  - 취약점 진단결과 항목 별 조회
- 취약점 진단 정보 상세
  - 취약점 정보 조회
  - 취약점 상세내역 조회
  - 조치 가이드 조회
  - 조치이력 조회

정보보호 컴플라이언스 진단 평가 통합

컴플라이언스 평가 관리

[주요 인증/심사 및 컴플라이언스 진단 평가 제공]

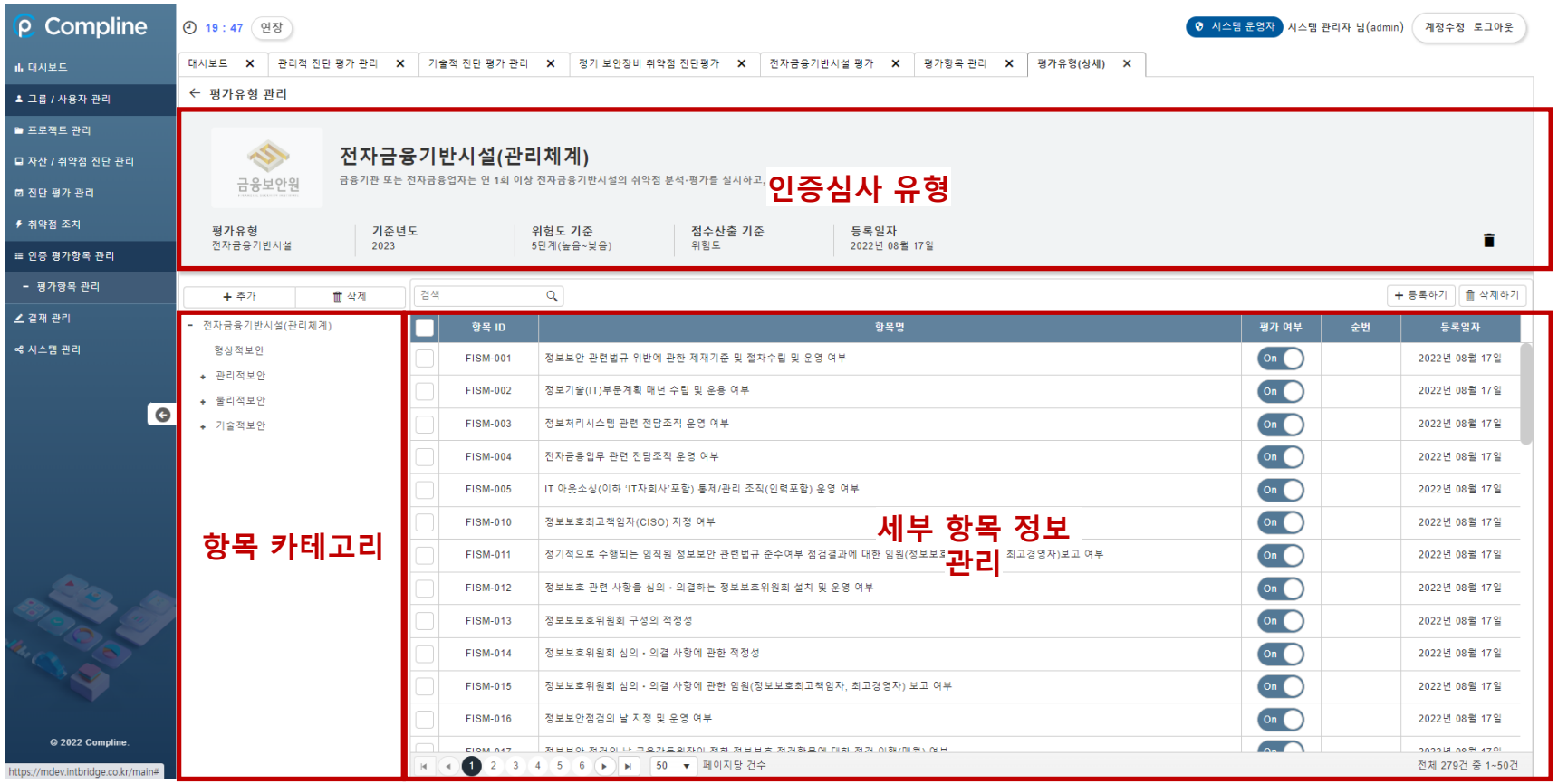
전자금융기반시설 금융보안원 | 주요정보통신기반 KISA | ISMS | ISMS-P | ISO27001 | 자체보안성심의



기능구분	기능 상세
컴플라이언스 항목 관리	· 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	· 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 증적 파일 등록 · 업로드 증적에 대한 미리보기 기능 지원
컴플라이언스 취약점 조치	· 취약점 별 조치담당자 지정 및 조치요청 · 조치에 따른 이행 점검 프로세스 제공
보고서 자동생성	· 컴플라이언스 별 진단평가 결과 보고서 자동 생성 · 컴플라이언스 별 진단결과 증적 일괄 다운로드

정보보호 컴플라이언스 진단 평가 통합

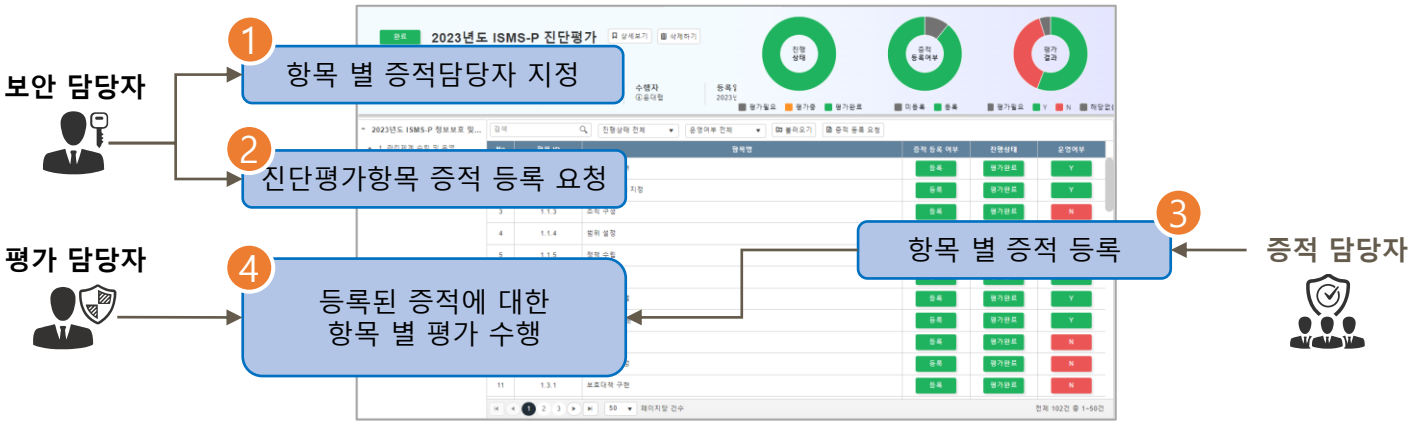
인증심사 평가(컴플라이언스) 항목 관리



- 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 증적 통합 관리

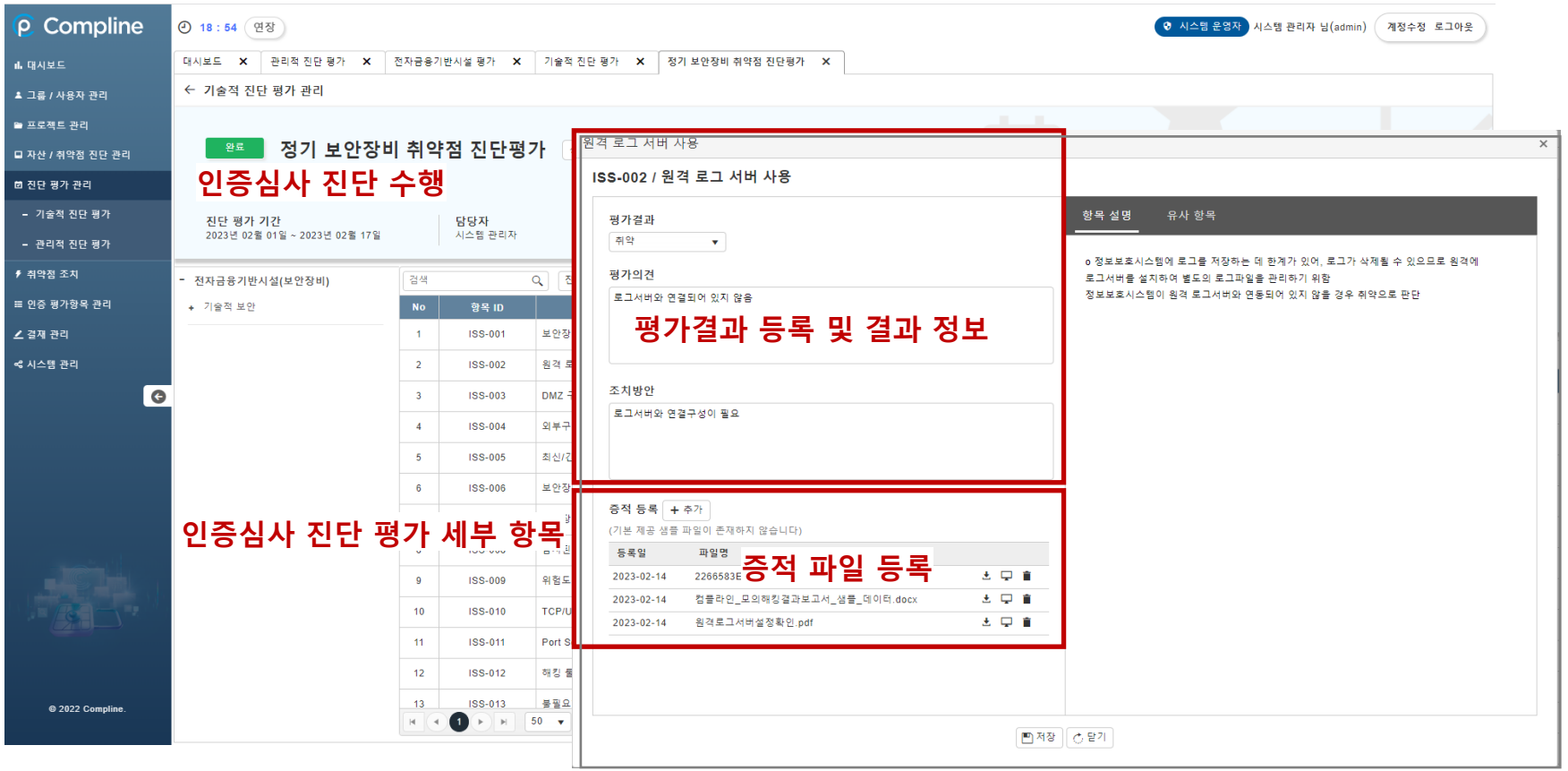
인증/심사 평가 항목 별 증적 담당자 지정 및 증적 등록 요청



기능구분	기능 상세
컴플라이언스 항목 관리	· 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	· 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 증적 파일 등록 · 업로드 증적에 대한 미리보기 기능 지원
컴플라이언스 취약점 조치	· 취약점 별 조치담당자 지정 및 조치요청 · 조치에 따른 이행 점검 프로세스 제공
보고서 자동생성	· 컴플라이언스 별 진단평가 결과 보고서 자동 생성 · 컴플라이언스 별 진단결과 증적 일괄 다운로드

컴플라이언스 진단 평가

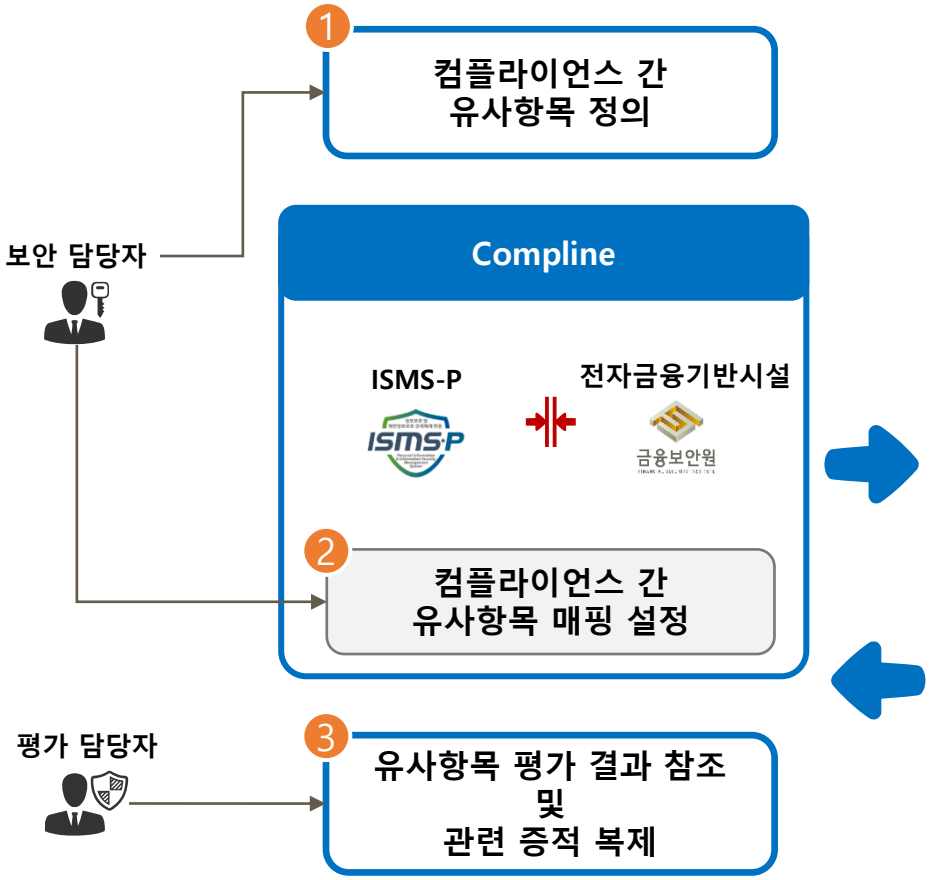
인증심사 진단 평가 세부 조회 및 증적 파일 등록

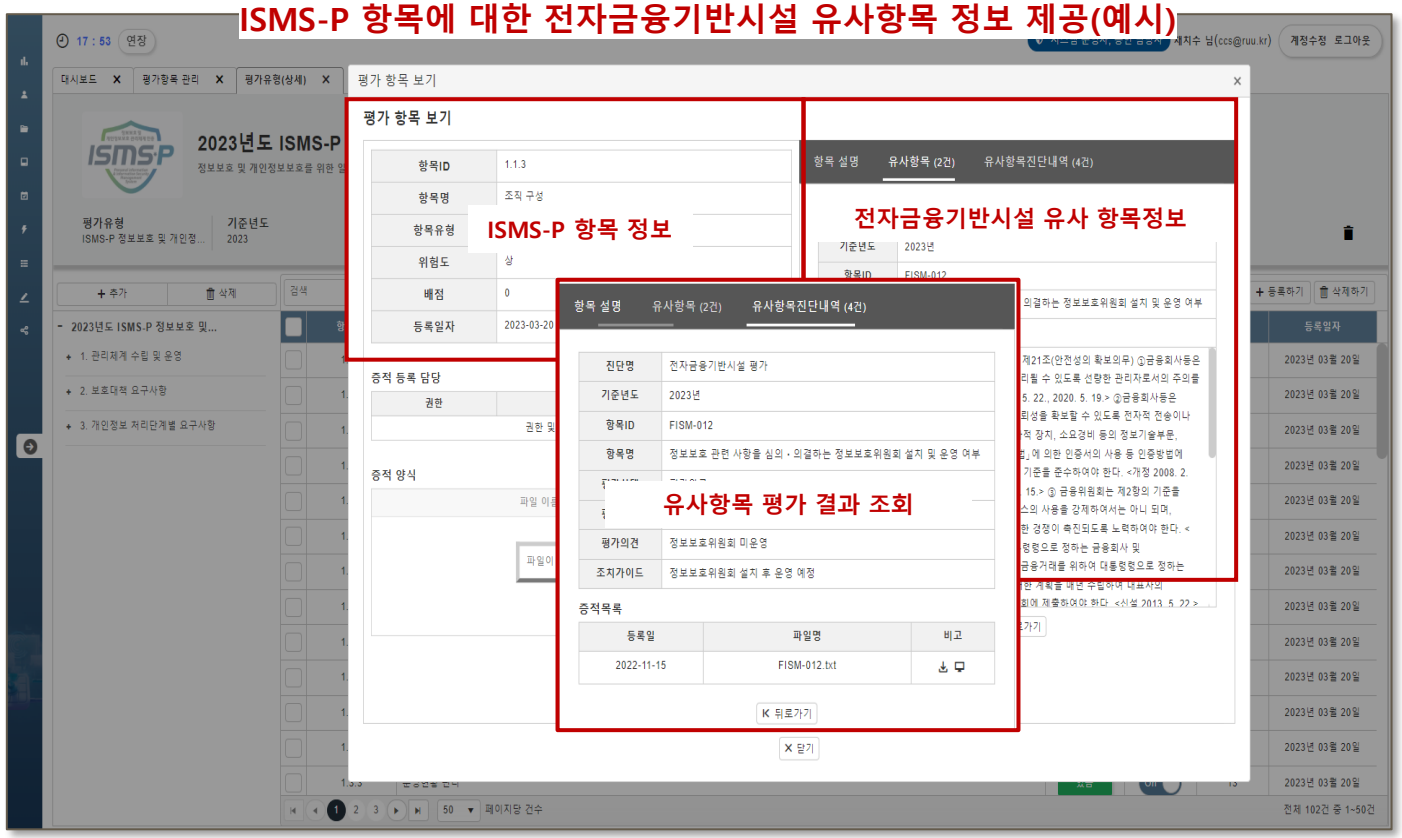


- 진단 평가 수행
  - 평가 기간 확인
  - 담당자/수행자 확인
  - 등록일자 확인
- 진단 평가 세부 항목 제공
  - 세부항목 확인
  - 항목 별 진행상태/평가결과 확인
- 항목 별 증적 파일 통합
  - 평가결과/평가의견/조치방안 확인
  - 증적 파일 등록 확인
  - 항목 별 내용 확인
  - 유사항목 비교

컴플라이언스 유사 항목 정보 제공

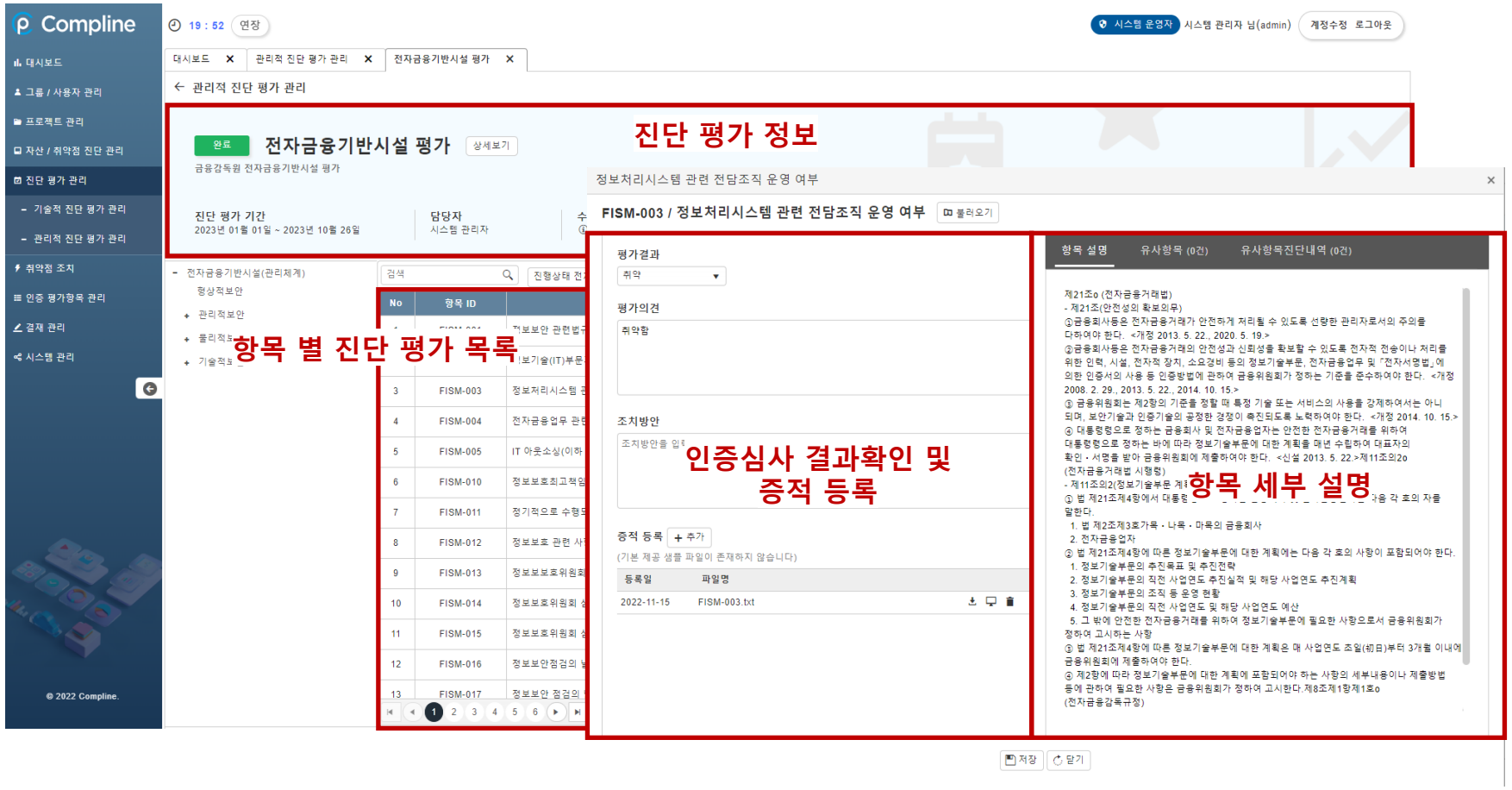
컴플라이언스 평가 유사 항목 매핑을 통한 평가 결과 참조 및 관련 증적 복제





컴플라이언스 진단 평가 결과 조회

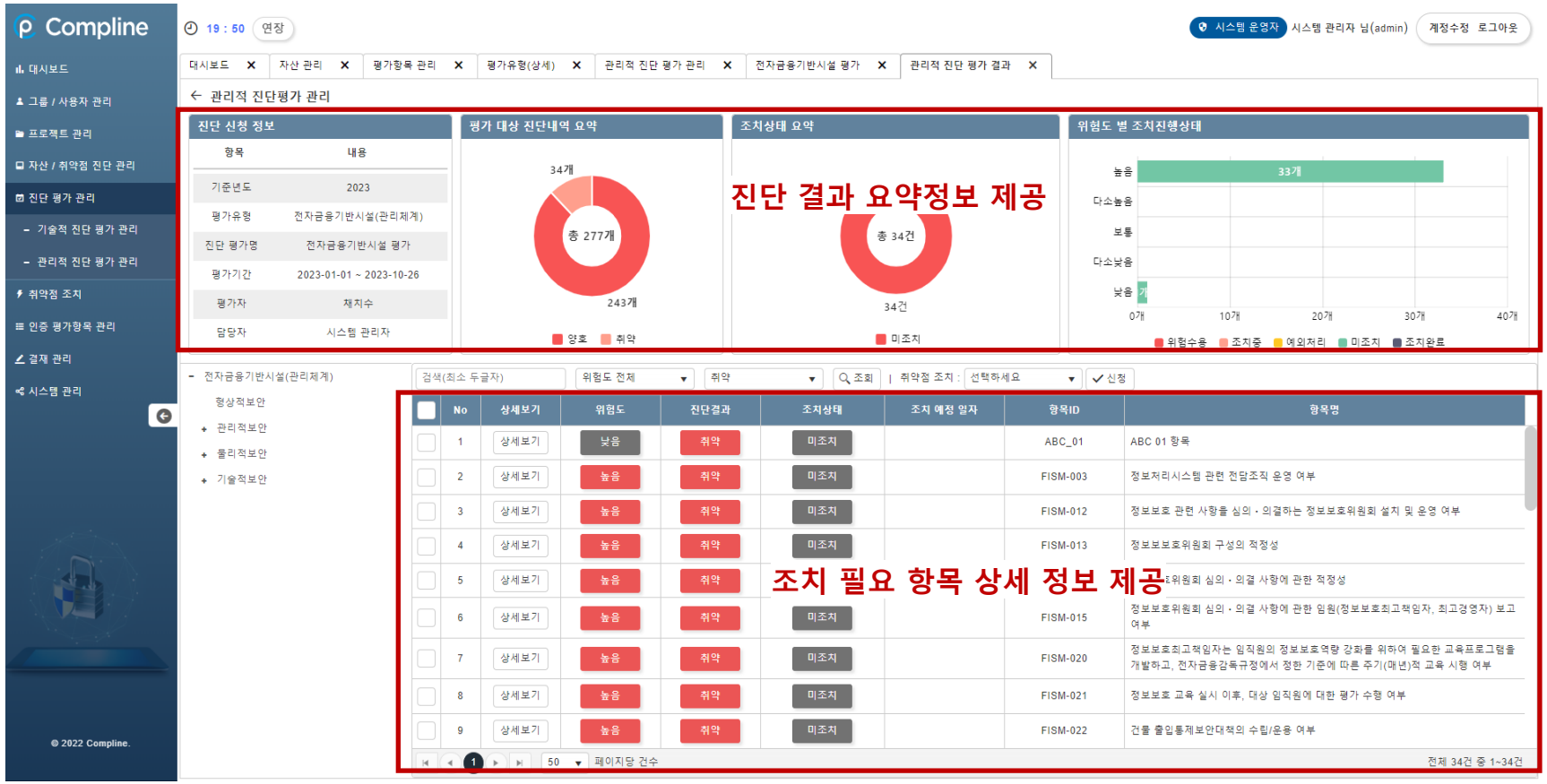
인증심사 진단평가 결과 및 증적 확인



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

컴플라이언스 진단 조치 이력관리(이행점검관리)

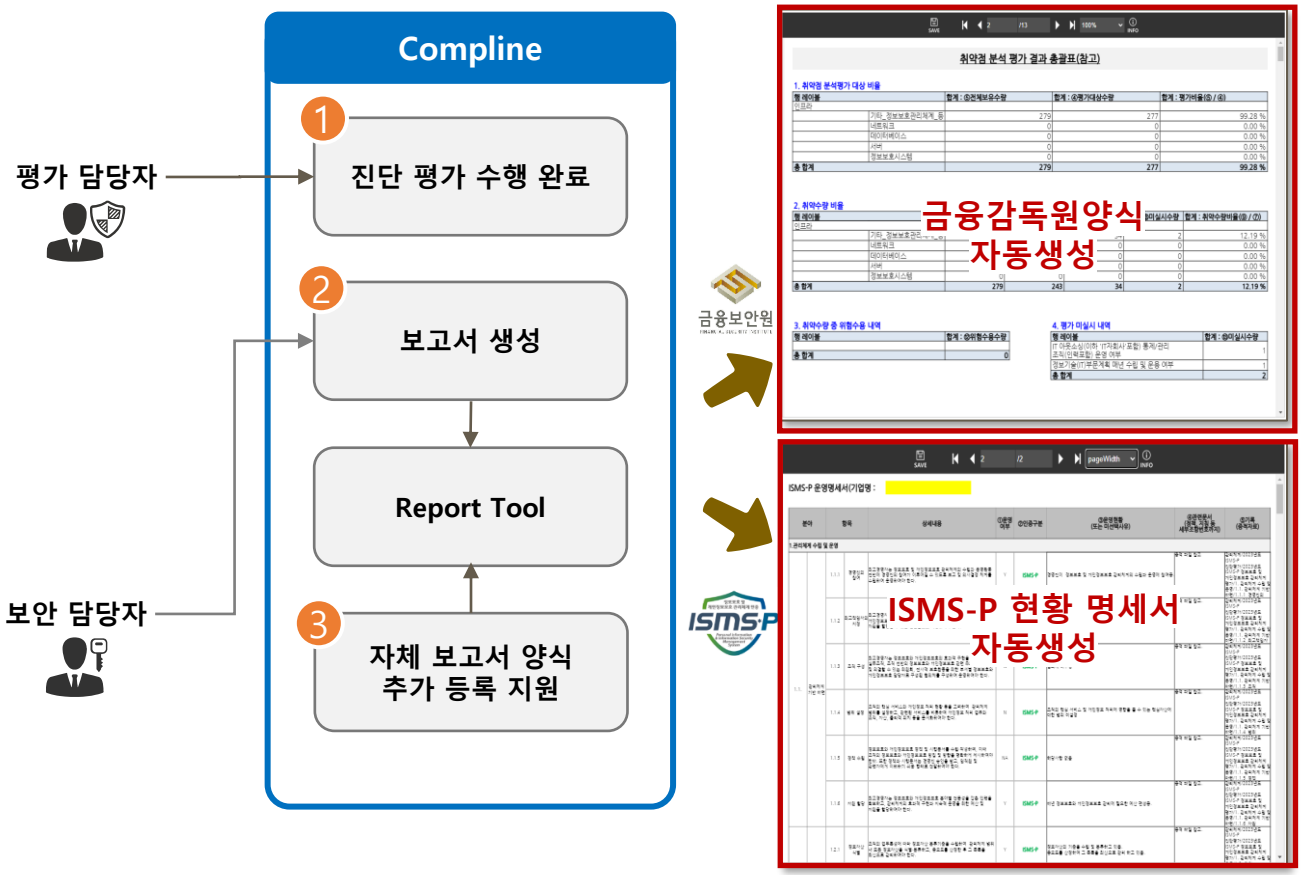
인증심사 진단평가 결과 조치(이행) 필요 항목에 대한 조치 워크플로우 제공



- 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

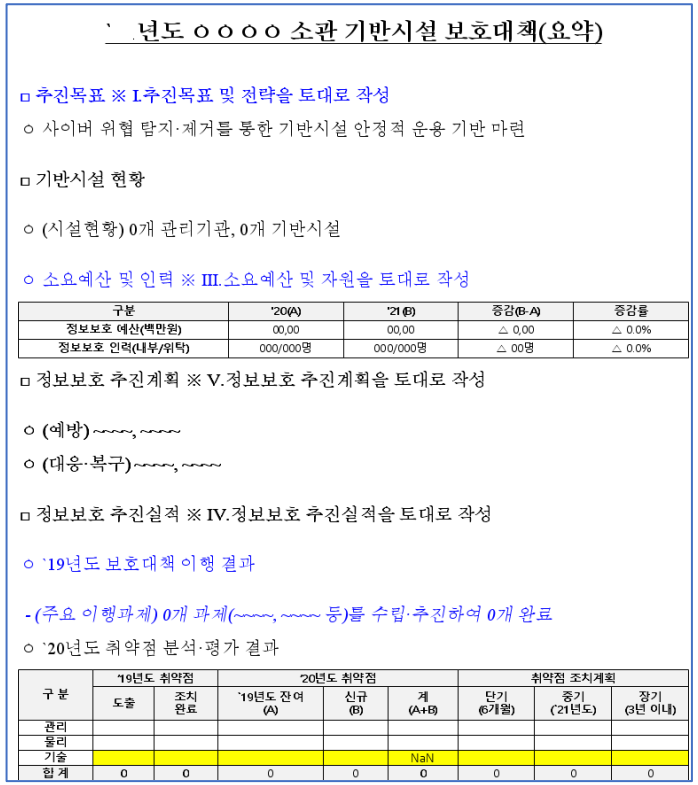
보고서 자동 생성 및 증적 파일 일괄 다운로드



기능구분	기능 상세
컴플라이언스 보고서 및 증적 파일	· 컴플라이언스 별 평가 결과 기반 제출 보고서 자동 생성 지원 · 고객사 보고서 양식을 유지하여 자동 보고서 생성 지원 · 평가 완료 컴플라이언스에 대한 증적 일괄 다운로드 지원
다양한 보고서 파일 포맷 지원	· 자체 내장 리포트툴을 이용하여 보고서 생성 시 미리보기 지원 · 미리보기 보고서를 다양한 파일 포멧으로 저장 가능(word, excel, ppt, pdf 등)
내부 보고서 생성 확장	· 자산, 취약점, 컴플라이언스 평가 정보 등 Complin 솔루션에 저장된 데이터를 기반한 다양한 보고서 생성 커스터마이즈 가능 · 내장된 리포트 툴에 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)



` 년도 ㅇㅇㅇㅇ 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

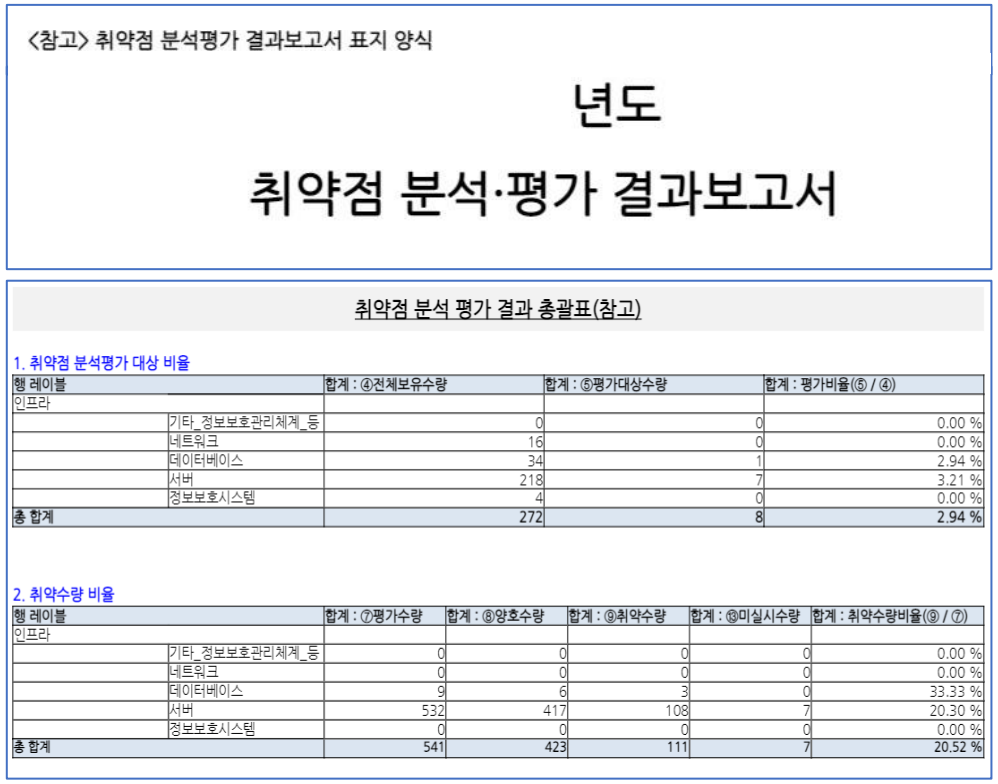
○ `19년도 보호대책 이행 결과

- (주요 이행과제) 0개 과제(~~~~, ~~~~ 등)를 수립·추진하여 0개 완료

○ `20년도 취약점 분석·평가 결과

구 분	'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			
합 계	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)

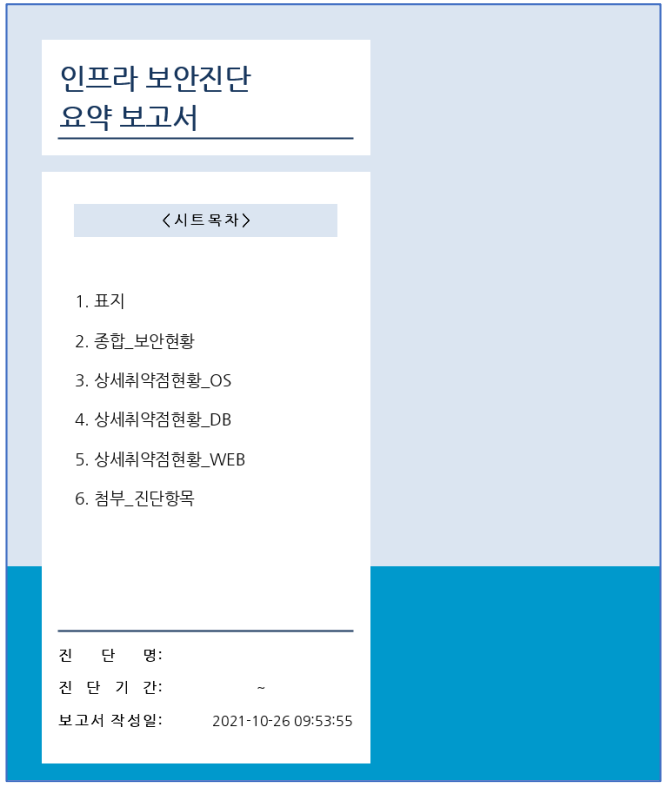
1. 취약점 분석평가 대상 비율

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

<시트목차>

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]

LH 한국토지주택공사

KiSTi 한국과학기술정보연구원
Korea Institute of Science and Technology Information
www.kisti.re.kr

[금융기관]

KB 국민은행

NH투자증권

하나캐피탈

[기업]

SK 하이닉스

int bridge
인트브리지

대표번호 : 02-6407-6001

영업문의 sales@intbridge.co.kr

기술문의 : tech@intbridge.co.kr

서울특별시 영등포구 은행로 29 정우빌딩 716호

감사합니다.