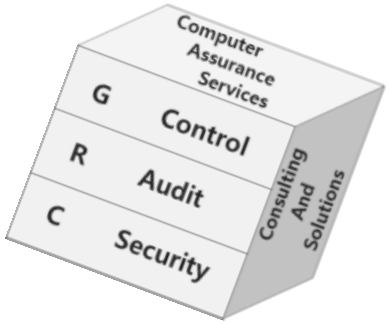
SecurityGRC

보안컴플라이언스 중심의 보안GRC 전자문서 플랫폼 구축 방안

u-Paperless Korea 컨퍼런스
2015. 5. 13

(주)씨에이에스 (C.A.S)
Computer Assurance Services

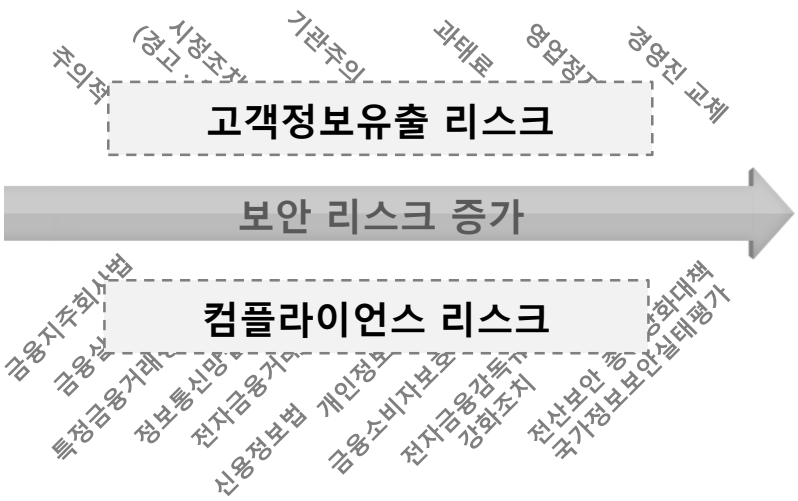


1. SecurityGRC 필요성
2. CAS SecurityGRC 개념도
3. CAS 통합컴플라이언스
4. 통계 및 대시보드
5. 사례를 통한 구축효과

1. SecurityGRC 필요성

고객정보유출 및 컴플라이언스 등의 보안리스크 증가에 따라 CISO관점의 SecurityGRC 통합관리체계가 필요합니다.

카드 3사 협력사 내부 직원유출 **1억건**	캐피탈 불법 대출업자USB 유출 **3만4천건**
카드사 연계 은행 고객 정보 **1500만건**	포스단말기 해킹 **20만건**
14개사 보험 판매대리점 정보유출 **1만3천건**	생명사 외주업체 직원유출 **35만건**



대외이미지 · 신뢰성하락

내외부 협력업무에 대한 보안시급

CISO의 고민

- 보안관점의 리스크의 통합적 관리
- 보안관련 법령(법, 시행령, 규정, 규칙, 규준 등) 준수
- 보안통제 및 내부규정의 효과적인 업데이트
- 감독기관 정기보고 및 점검사항 처리가 용이
- CEO 대상 보안통제에 대한 설명

해결 방안

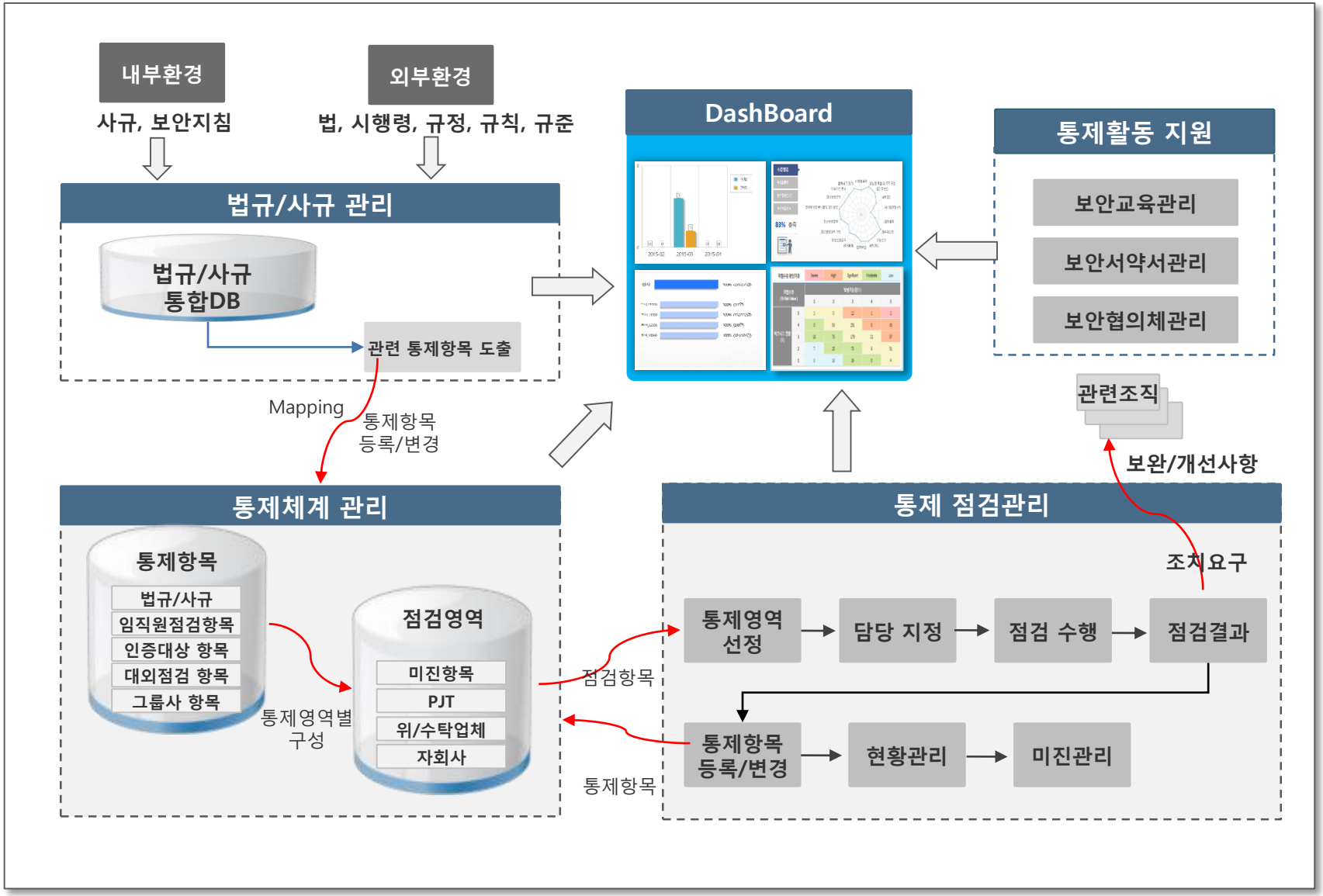
- 보안 Compliance업무의 IT시스템 전환을 통한 업무간소화 및 효율화
- 법규/사규 제·개정 관리를 통한 법규 최신화 유지 및 관련통제 누수부문 억제
- 보안 Compliance 정보의 통합으로 필요정보 적기 활용 및 일관된 정보 공유
- 표준 프로세스에 기반한 통제체계관리

SecurityGRC 통합관리체계 필요

2. CAS SecurityGRC 개념도

전체적인 시스템구성도는 컴플라이언스정보로부터 수준진단 프로젝트를 생성하고, 수준진단을 진행하고 증적을 관리하는 기능과 일반적인 보안활동 업무와 시스템관리 기능으로 구성됩니다.

2. CAS SecurityGRC 개념도



3. CAS Unified Compliance Framework : 통합컴플라이언스

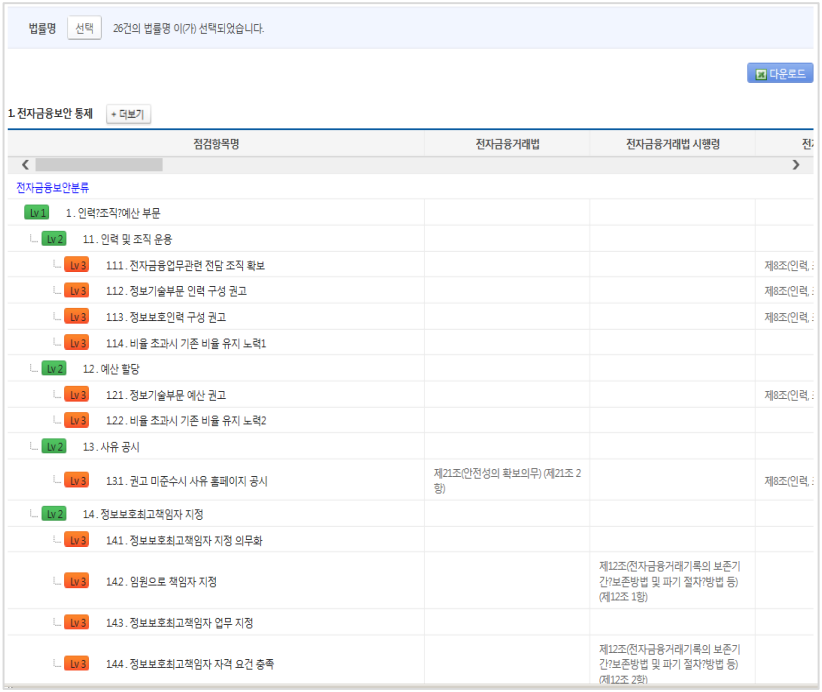
국내외 법규정 및 인증, 표준 등으로부터, 통합된 보안통제를 관리 점검할 수 있는 UCF기반의 통합컴플라이언스를 제공하여, 정보보안 관련 모든 법규 준수 및 대응 세부절차를 마련합니다.

국내

- 전자금융거래법 및 전자금융감독규정
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보보호법
- 신용정보의 이용 및 보호에 관한 법률
- 국가정보원 보안실태점검
- 행정자치부 개인정보 안전성 확보조치 기준고시
- ISMS, PIPL, ISO27001 등의 인증
  최초심사 및 유지관리 심사

국외

- Sarbanes-Oxley Act (SOX)
- Basel II
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- HIPAA
- CMS
- FERC Security Program
- NERC Critical Infrastructure Protection (CIP)
- FFIEC
- NIST
- Cobit
- ISO 27001, 27002
- BS10012

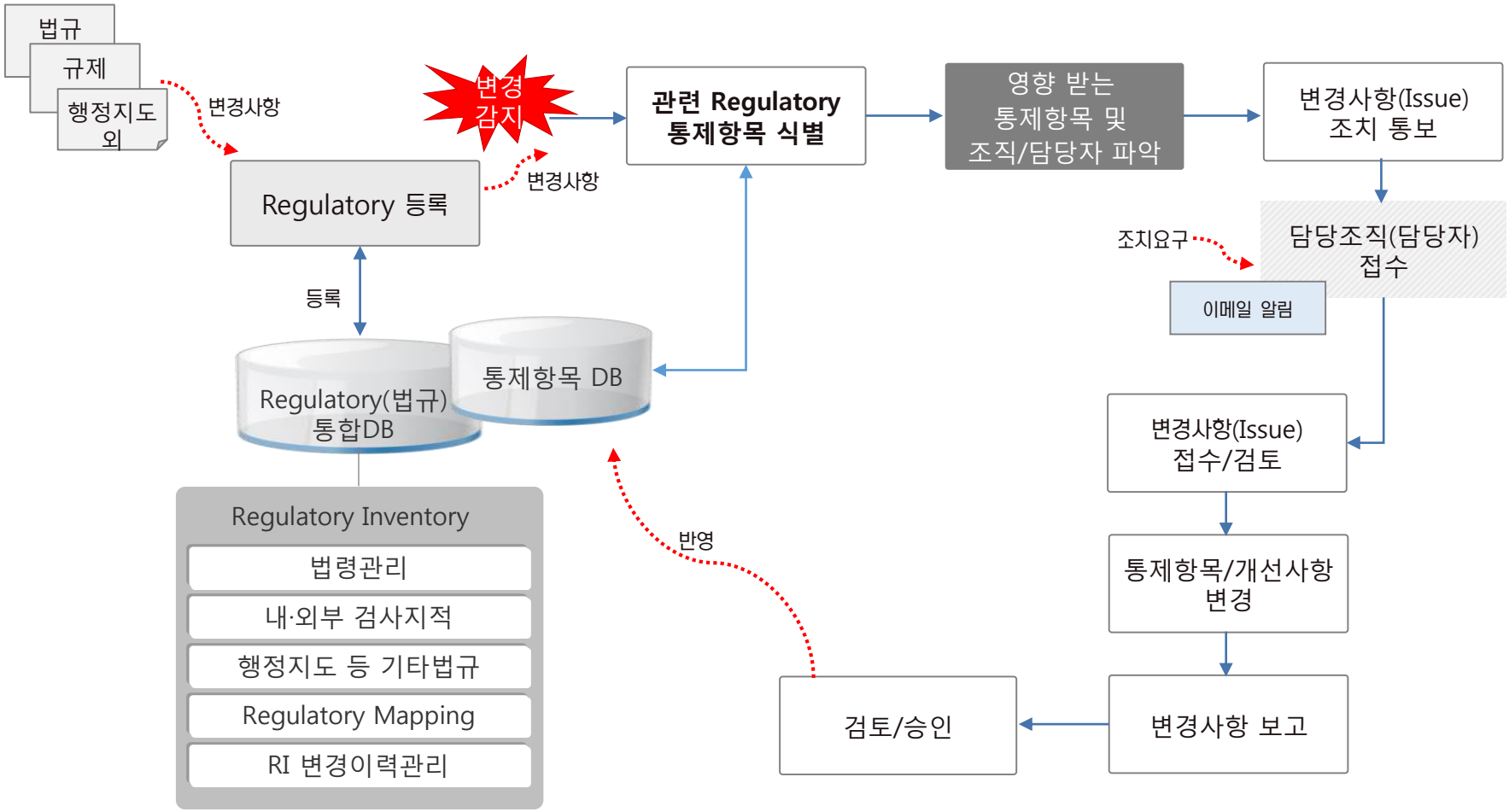


CAS UCF

- **통제항목의 지속적인 변경관리**
- **점검항목의 통합관리 및 중복점검 방지**
- **유연한 Compliance 관리기준 제공**
- **사례산출물 제공을 통한 업무효율성 증대**
- **법규의 Cross Check 기능**

3. CAS Unified Compliance Framework : 변경관리

법규/규제 등 Regulatory 변경에 따른 통제항목의 영향도를 파악하여 영향 받는 통제항목과 대상조직을 식별하여 제시함으로써 통제항목 변경 및 개선사항을 수월하게 반영함에 따라 비용 및 시간이 절감됩니다.



3. CAS Unified Compliance Framework : 보안점검 및 인증

통합보안점검 및 인증 활동을 위해서 참조, 모범산출물과 침해요인 및 개선방안이 제시됨으로써 비용 및 시간이 절감됩니다.

인증심사 및 통합보안점검 활동

- 전자금융거래법 및 전자금융감독규정
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보보호법
- 신용정보의 이용 및 보호에 관한 법률
- ISMS, PIPL, ISO27001 등의 인증 최초심사 및 유지관리 심사
- 국정원 보안실태점검
- 행자부 개인정보보호 수준진단 행자부 개인정보보호 실태점검
- 전사 보안점검활동

침해요인/개선방안

- 점검항목별 침해요인 제시
- 점검항목별 실현가능한 개선 방안 제시

법 규	15종	**법 정 서 식**	691종
지 침	196종	**계획,결과서**	100종
점검영역	23종	**결 제 문 서**	18종
주제정보	30종	**절 차 서**	16종

비용 및 시간 절감

참조산출물

- 증적(법정서식이나 절차서 등)을 작성 시 참조가능한 산출물
- 각종 법정서식, 지침 및 절차서, 증적산출물 등을 제공
- 개인정보 조직도, 영상정보 운영 계획서, 접근권한 신청서 등 400 종 제공

모범산출물

- 다수의 공공/금융 기관에서 적용한 우수 산출물
- 증적자료로 즉시 활용 가능
- 내부관리계획, 개인정보처리 방침, 개인정보 침해사고 대응매뉴얼 등 420 종 제공

3. CAS Unified Compliance Framework : 법규/사규관리

법규의 제·개정 관리 및 필요정보를 적기에 활용하여 법규/사규와 통제항목간 연관관계(Mapping) 및 이력정보를 제공합니다.

법규/사규 관리 Process

제·개정 법규/사규 준비	Upload 대상 법규/사규 파일 확보
Upload용 파일 생성	정해진 양식에 맞게 조문 분리
법규/사규 Upload	조문 파일 DB 업로드
통제항목 매핑	법규/사규와 통제항목간 매핑
변경 통제항목 식별	제·개정에 영향받는 통제항목 도출
법규/사규 조회	각종 법규 조회

특장점

법규/사규 통합 DB 구조

- **각종 법규/사규를 관리할 수 있는 확장성 있는 통합 DB 구조 채택**

연관관계 제공

- **법규/사규와 통제항목간 연관관계 매핑을 통해 Cross Check 가능**

영향 분석

- **대내외 규제변화를 반영한 영향 받는 통제항목 식별하여 변경관리가 가능**

메뉴 기능 요약	법규 업로드	정해진 양식의 엑셀 파일을 업로드하여 법규/사규 통합 DB에 insert
	매핑 및 이력 관리	내재된 기능으로써 법규/사규와 통제간 정해진 매핑 처리와 제 · 개정 이력 관리
	법규 조문 조회	법규 조회 시, 각 조문에 대하여 신설, 삭제, 변경 여부를 확인 가능
	법규 매핑 조회	복수의 법규를 서로 비교할 수 있는 조회 기능
	통제 항목 매핑 조회	영향 받는 통제 항목들에 대한 조회

3. CAS Unified Compliance Framework : 통제체계관리

법규, 사규의 제·개정 또는 신규 발굴된 통제항목 등록 및 변경, 통제영역 관리, 사례산출물 및 동일증적 지정, 법규 및 사규 지정, Compliance 통합관리 및 규제별통제항목을 확인하는 기능이 포함되어 있습니다.

통제체계 관리 Process

관리대상 통제항목 식별	- 법규, 사규, 보안규정 변경 및 신규 통제항목 발굴 - 담당자에게 알림 제공으로 지속적인 변화 관리 기능
통제영역 식별 및 관리	- PJT, 위/수탁, 자회사, 미진사항, 임직원, 인증, 대외점검 등의 통제 영역 식별 및 관리
통제항목 기본 정보 관리	- Compliance 구분, 점검분류, 점검내용, 점검방법, 지침, 요령 등의 정보 관리 - 유연한 통제항목 레벨 지정이 가능
이슈 및 개선방안 관리	- 사후저리에 대한 가이드라인을 제시
사례산출물 매핑	- 모범/참조 산출물을 매핑 - 매핑을 통해 증적자료 생성시 모범/참조산출물을 활용하여 업무효율 증대
법규/사규 매핑	- 통제항목과 연관된 법률을 매핑 - 다양한 법규/사규 간의 Cross Check 기능 제공
동일증적 매핑	- 동일한 증적이 관리되고 있는 통제항목글 간의 연관관계 매핑 - 동일 증적을 통한 중복점검 방지 및 증적산출물 중복 배제
컴플라이언스 통합관리	- Compliance간 유사점검항목 통합관리를 통한 점검항목의 중복을 배제
규제별통제항목 확인	- 다양한 법규/사규 등의 연관관계를 확인 - 다양한 법규/사규 간의 Cross Check 기능 제공

특장점

- 통제항목의 지속적인 변경관리
- 점검항목의 통합관리 및 중복점검 방지
- 유연한 Compliance 관리기준 제공
- 사례산출물 제공을 통한 업무효율성 증대
- 법규의 Cross Check 기능

메뉴 기능 요약 (통제관리)	통제영역분류	대규모 PJT, 위/수탁, 자회사, 미진사항, 임직원, 인증, 대외점검 등의 통제영역 분류를 관리하는 기능으로, 통제항목관리 및 통제점검관리에서 활용된다.
	통제항목관리	식별된 통제항목을 등록/수정하며, 기본 정보와 이슈 및 개선방안, 사례산출물, 법규/사규 등의 정보를 매핑한다.
	동일증적관리	동일한 증적이 관리되고 있는 통제항목들을 식별하여 연관관계를 관리하여 중복을 배제한다.
	컴플라이언스통합관리	Compliance간 유사점검항목 통합관리를 통한 점검항목의 중복을 배제한다.
	규제별통제항목조회	다양한 법규/사규 등의 연간관계를 확인하여 Cross Check가 가능하도록 한다.

3. CAS Unified Compliance Framework : 통제점검관리

법규, 사규, 대외/협력기관 Compliance에 대한 통제 항목에 대하여 수준진단 ,미진관리에 대한 사후관리를 지원하며, 법적 대응을 위한 자가통제 체크리스트에 의한 점검을 지원합니다.

통제 관리 Process

P	통제영역 선정	,PJT,위/수탁,자회사,미진사항 등 , 통제 영역 선정
	담당지정	통제대상에 이행요청, 알림 계획관리에 의한 통보
D	담당자 점검시행	통제담당 통제 진단 , 증적 자료 등록
C	현황관리	평가진척도 확인 , 검검 재 요청, 진행율 확인
A	미진관리	목표대비 통제 미진관리, 조치대상선별,사후관리,이슈관리
	결과조회	진단결과 조회

"PDCA Cycle"
Compliance 통제 점검 체계 구성

특장점

" 표준화된 통제 영역 적용"

- 법적 대응을 위한 통제점검 체계 적용
- 법규,사규 ,PCI-DSS 인증 등 점검 항목 적용
- 개인정보보호 등 Cross Check 된 규제법 관리
- 협업기관,미진사항의 표준체크리스트 점검 관리

" 통제 점검 관리의 체계화 "

- 진행진단평가 시 점검영역별, 주제별 진행 기능
- 담당자별 일정에 대한 알림 기능 제공
- 통제항목별 점검기준, 점검방법, 평가 가이드
- 전체 /담당자별 진척률 산정
- 통제항목 목표설정에 의한 GAP 분석 제공

메뉴 기능 요약 (통제관리)	통제점검 등록	통제 점검을 위한 하나의 수준진단 프로젝트를 생성하는 기능으로, 프로세스 및 점검항목을 선택하고 담당자와 일정을 지정함
	진행현황 [프로세스 別]	통제 점검 수행 시 프로세스별 진행현황을 확인하고, 진단평가를 수행함
	진행현황 [주제 別]	통제 점검 수행 시 주제별로 진행현황을 확인하고, 진단평가를 수행함
	사후관리	점검항목에 대한 진단평가 시 조치예정 또는 예외처리 항목에 대해서 수준진단이 종료된 후에도 사후관리를 통해 조치함
	결과조회	수준진단이 종료된 프로젝트의 목록 및 상세 진단평가 정보를 조회함

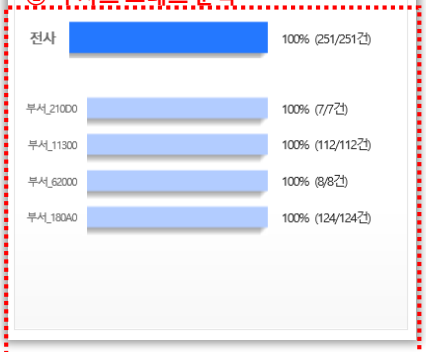
4. 통계 및 대시보드

정보보안 법규 및 인증 관련 컴플라이언스 관리 활동 전반에 관한 진행률 관리 및 통제항목 목표수준 관리 현황에 대한 대시보드를 제공합니다.

예시

보안점검활동 진행률

① 바 차트 그래프 분석



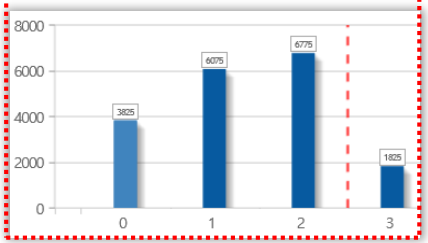
점검항목 통계

② 도표 분석

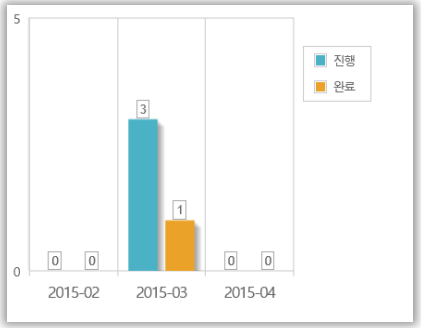
점검년도	회차	점검계획명	점검자산건수	취약점발견 자산건수	발견취약점건수	조치상태별 점검항목건수			
						미조치	조치예정	조치완료	예외처리
2014	3	2014 3회차 점검	30	8	15	3	5	5	2
2014	2	2014 2회차 점검	29	7	17	5	5	5	2
2014	1	2014 1회차 점검	29	9	19	5	10	4	0

번호	수준진단	진단단계	기관분류코드	프로젝트명	수행일자	상태	경과율
6	고객사수준진단	해당없음	금융기관	2015년도 상반기 내부수준진단	2015-03-19 ~ 2015-03-31	프로젝트완료	0%
5	ISMS인증	유지관리	중소기업	'15년 씨에이에스 ISMS 사후심사 대응	2015-03-18 ~ 2015-03-31	프로젝트수행	0%
4	ISMS인증	최초심사	공공기관	테스트	2015-03-18 ~ 2015-03-18	프로젝트수행	5%
3	PIPL인증	최초심사	공공기관	2015년 OO재단 PIPL 인증 컨설팅	2015-03-09 ~ 2015-03-31	프로젝트수행	2%
2	ISMS인증	변경심사	대기업	test1	2015-03-03 ~ 2015-04-01	프로젝트수행	100%
1	ISMS인증	최초심사	금융기관	2015년도 상반기 내부 보안점검	2014-12-01 ~ 2015-09-30	프로젝트수행	100%

점검항목 수행 건 수



보안통제 진행현황



통제항목 목표수준 관리

특장점

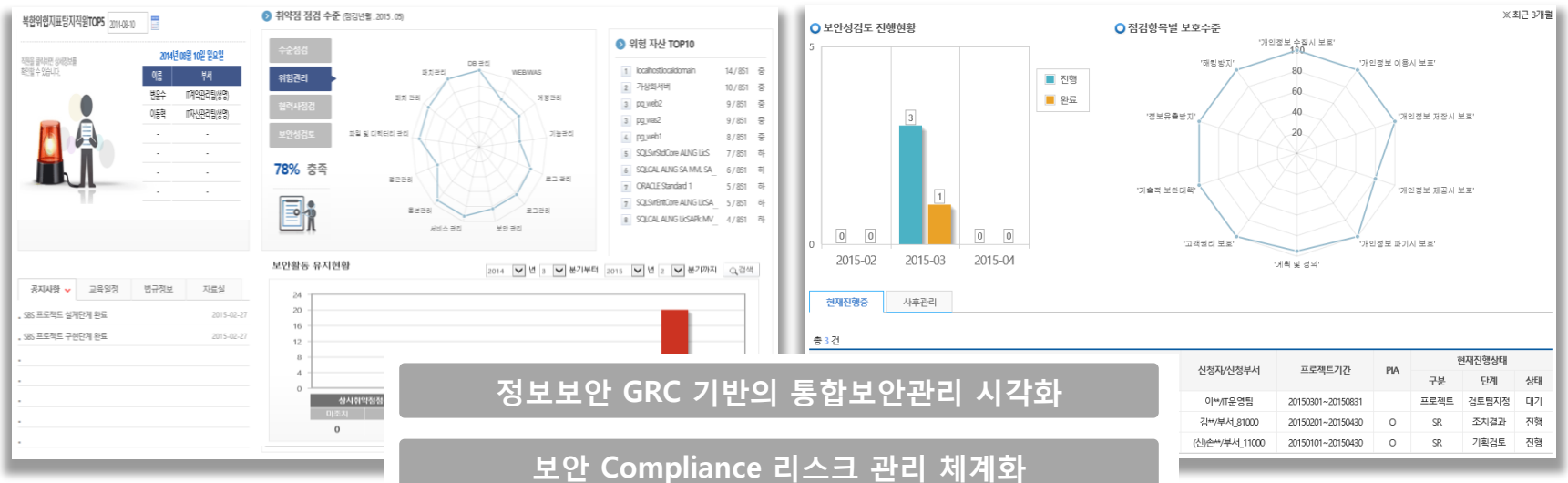
- 다양한 차트를 활용한 분석정보 제공
- 목표대비 진행현황 실적관리 가능
- 그래프 및 도표 다운로드 기능 제공

① **바 차트 그래프 분석**	부서별, 기간별 비교 분석 정보를 제공
② **도표 분석**	보안협의체 계획을 등록하고 협의체를 운영하고 결과를 관리함
③ **레이더 차트 분석**	다차원 점검항목 및 지표를 비교분석 할 수 있는 레이더 차트 제공

5. 사례를 통한 구축효과 – N사

Compliance 관리체계 구축 효과

- 보안 이상징후, 보안활동, 보안 컴플라이언스 관리를 통한 Compliance 리스크 관리 가능
- 정보보안 컴플라이언스 업무활동으로 소송에 대비한 증적 마련
- 보안성심의(PJT, SR), 협력사점검, 임직원 점검, 취약점점검 및 보안서비스 등의 보안 Compliance 업무 효율적 수행
- 직원 상주 유지보수 수행을 통한 지속적인 관리체계 지원

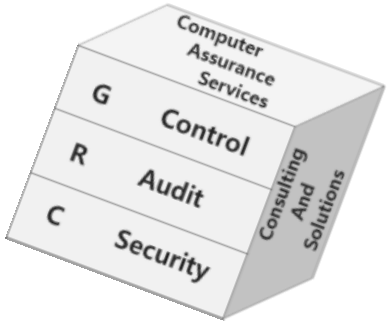


정보보안 GRC 기반의 통합보안관리 시각화

보안 Compliance 리스크 관리 체계화

이상징후 상시모니터링을 통한 효율적인 보안내부통제

개별적 정보보안 업무들의 통합을 통한 시간비용 절감



CAS SecurityGRC 를 통하여 u-Paperless 창조경제를 이뤄나가겠습니다. 감사합니다.

㈜씨에이에스 영업기획팀 차장 CISA 최인규

ikchoi@casit.co.kr

(주)씨에이에스 (C.A.S)
Computer Assurance Services