

Deloitte.



ExpertHub™

SAP 내부회계 평가 솔루션

DIAS(Deloitte ICFR Automation Solution) for SAP

Risk Advisory Services at Deloitte Anjin
RA-IT&SA

제품 출시 배경

내부회계관리제도 감사 대상

2023년까지 모든 상장사는 외부감사인으로부터 내부회계 관리제도에 대한 감사를 적용 받게 되며, 이에 따라 적용 대상 기업들은 내부회계관리제도에 대한 컨설팅 및 솔루션 도입 등을 통해 자사의 내부회계 통제수준을 강화하여 외부감사에 대비하고 있습니다.

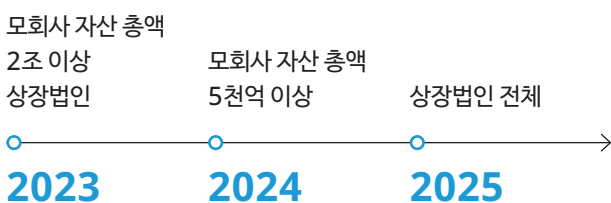


(단위 : 곳) 자료 : 회계업계 추산

연결 내부회계관리제도 감사 도입

2023년부터 단계적으로 연결 내부회계관리제도 감사제도가 시행됨에 따라 연결 자회사를 포함한 연결내부통제 관리가 요구됩니다.

연결 내부 회계관리제도 감사 시기



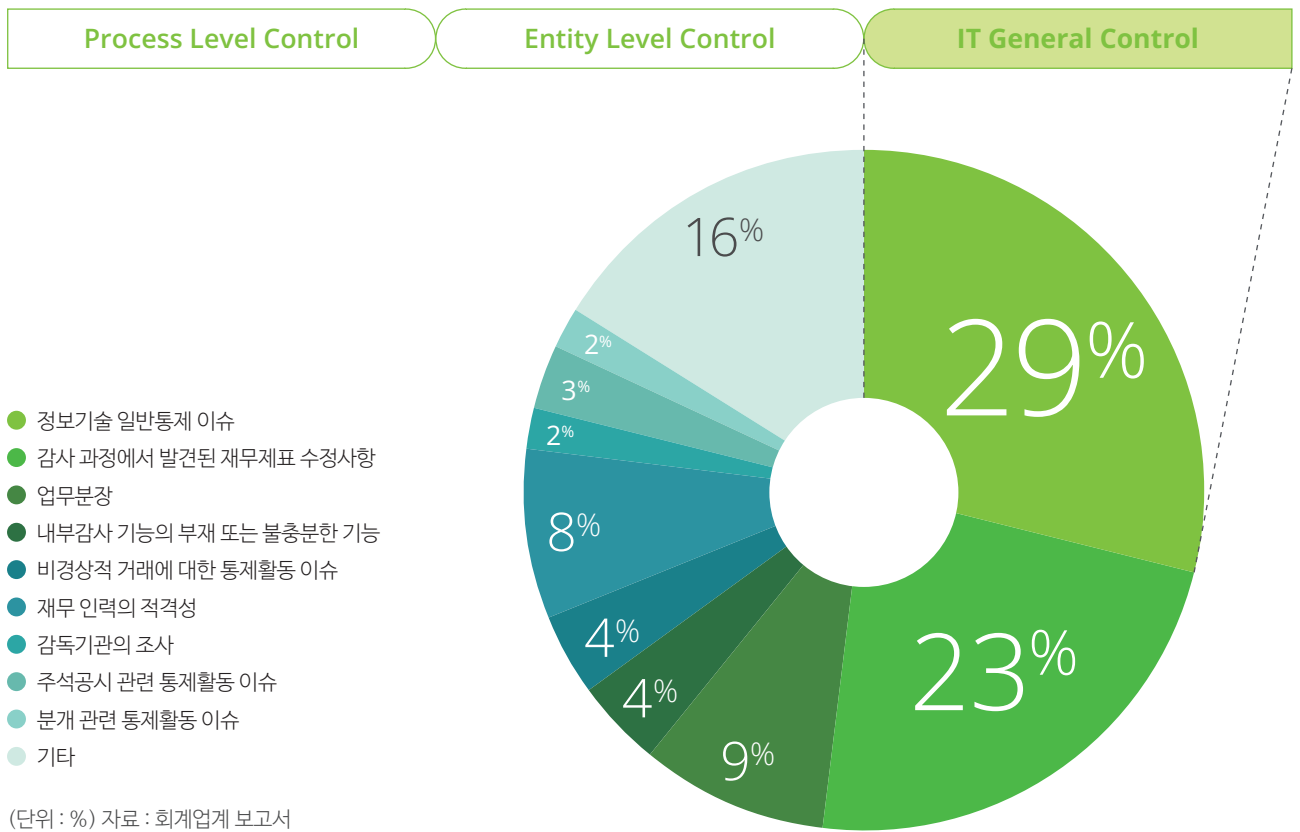
주요 고려사항

- 모회사 감사 책임 확대
- 자회사 내부회계관리제도 구축 및 운영 확대
- 내부회계관리제도 감사 비적정 의견 가능성 증대

내부회계관리제도 감사 상 이슈 및 고려사항

자산 총액 2조 이상 상장기업 대상으로 시행된 내부회계관리제도 감사상 발견된 미비점으로 IT 통제 이슈가 다수 발견되었으며, 재무보고 프로세스상 절대적으로 높아진 IT 의존도를 고려하여 IT 통제 대응이 향후 내부회계관리제도 감사 대응상 주요 과제로 예상됩니다. 이에, 회사는 요구되는 법 제도의 대응을 비롯하여 내부회계관리제도를 위한 컨설팅 및 솔루션 도입을 고려하고 있으나 추가되는 비용, 업무의 부담 등 많은 고려사항에 직면해 있습니다.

자산 총액 2조 이상 내부회계관리제도 감사 미비점 유형



법 제도 대응

- 외부 감사 법률 전면 개정
- 내부회계관리제도 감사 기준 제정

시스템 운영 효율성 제고

- 최신 기술 적용을 통한 프로세스 확장성 및 유연성 확보
- 사용자 요구사항 반영을 통한 업무 효율성 제고

현업 부서 업무 부담 경감

- 업무시스템 간 상호 연계 및 내부통제 절차의 표준화
- 자동화 및 최적화를 통해 내부통제 관련 업무 부담 경감

Why DIAS?

DIAS를 통한 SAP 통제 Best Practice 내재화

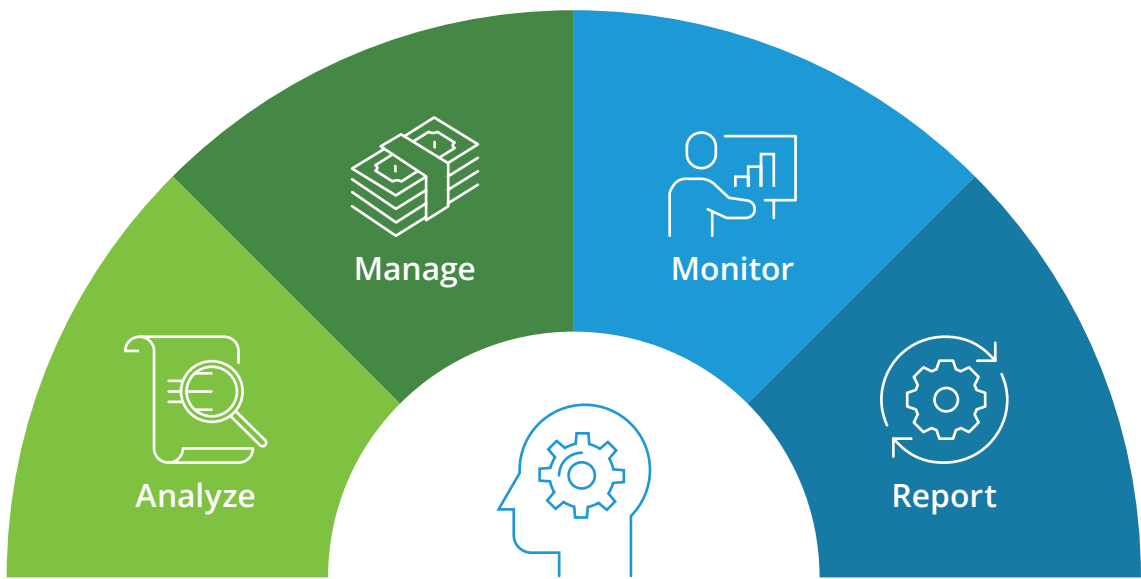
내부통제 효율성 증대는 물론 컴플라이언스 선제적 대응, 비용 절감과 통제활동 신뢰성을 제고합니다.



제품 개요

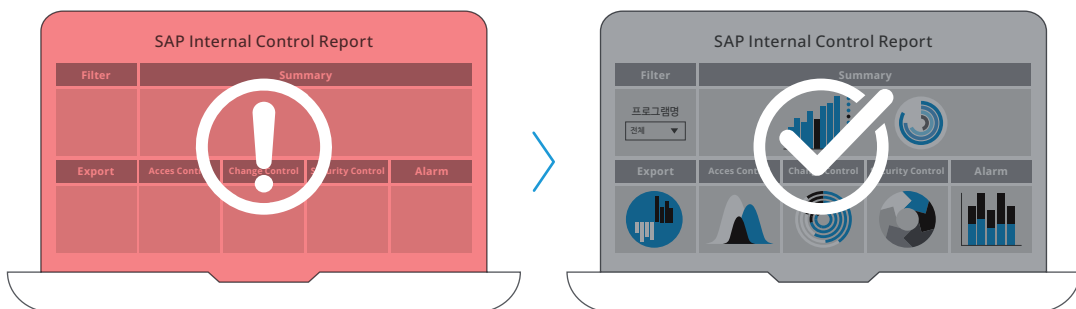
내부회계관리제도 대응을 위한 최적의 SAP 내부회계 지원 솔루션

사용자 친화적인 시스템 구성으로 전문인력의 도움 없이 SAP에 요구되는 내부통제에 대한 분석, 관리 및 모니터링 기능을 지원하며, 감사 대응에 필요한 계정 및 권한 설정 관리와 로그를 수집하여 분석된 보고서를 제공합니다.



Transform your IT General Control

- 계정 관리
- 권한 관리
- 로그 관리
- 설정 관리



제품 구조

IT General Controls 관리

내부회계관리제도 모범규준에서 다루는 IT일반통제(IT General Control)의 관리영역인 접근보안, 변경관리, 컴퓨터 운영이라는 3가지 카테고리를 기본 베이스로 SAP ERP의 특화된 기능을 매핑시켜 내부회계관리제도 대응 시 통제누락이 없도록 구현하였습니다.



컴퓨터 운영

- 배치작업 권한보유자 및 실패내역 조회 (SM36/SM37)
- IDOC 권한보유자 및 실패내역 조회
- 클라이언트 설정(SCC4) 및 시스템 변경 옵션 조회(SE06)
- 통제별 권한보유적정자 관리(기준정보)
- 배치작업 기준정보 관리
- 패스워드 파라미터 기준정보 관리



변경관리

- CTS IMPORT 이력 조회
- SE16을 통한 데이터 변경이력 조회
- 테이블 유지보수 뷰를 통한 데이터 변경 이력 조회
- Debug를 통한 데이터 변경이력 조회
- 회계전표 변경이력 조회

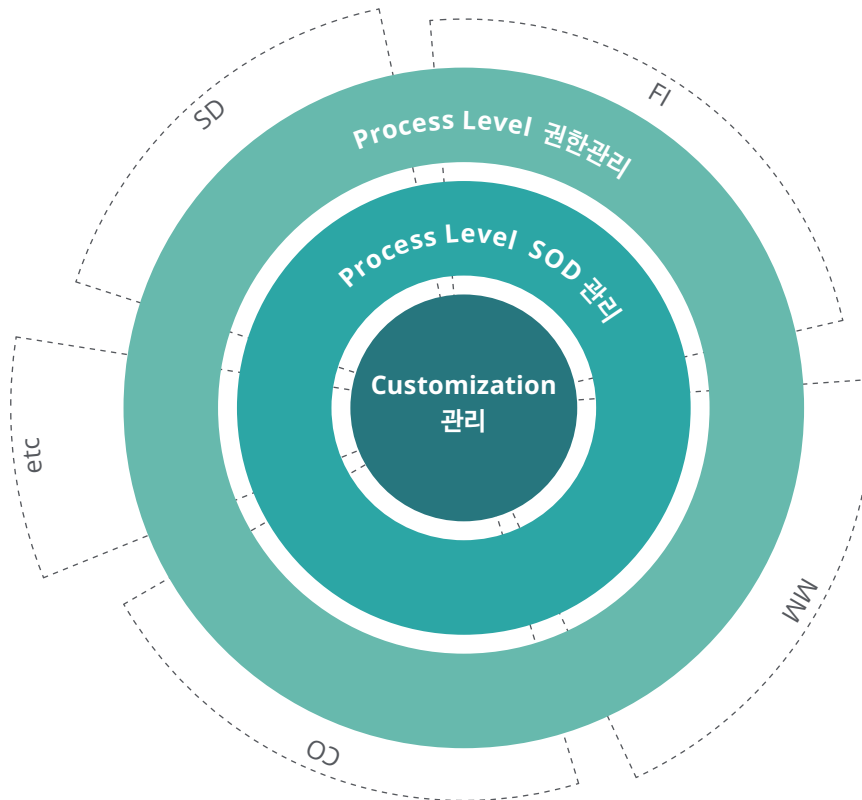


접근보안

- Role/Profile 권한보유자 관리 (SU01/PFCG)
- 패스워드 파라미터 관리
- SAP_ALL / SAP_NEW 권한보유자 관리
- SAP Default ID 관리
- 테이블 유지보수 뷰(SM30) 권한보유자 관리
- 프로그램 직접 실행 권한보유자 관리(SA38)
- Debug 권한보유자 관리
- Role 결합 리스크 시뮬레이션

프로세스 레벨 Restricted Access 및 Segregation of Duties 관리

SOD(Segregation Of Duties, 업무분장)에 근거하여 비즈니스 업무목적상 상충되는 권한을 동시에 보유할 수 없도록 사전 시뮬레이션 프로그램을 통해 권한을 제어하고, 비즈니스별 주요 권한을 보유한 사용자 추출 및 부적절한 권한보유자의 트랙잭션을 추적하여 비즈니스 사고와 재무데이터 왜곡의 영향도를 빠르게 파악할 수 있습니다.



Process Level SOD 관리

- 회계, 구매, 자금 등 주요 프로세스에 대해 업무 목적상 상충되는 비즈니스 권한을 시나리오화하여 기준정보로 관리
- 사용자에게 비즈니스 권한을 부여하기 전 사전에 정의된 SOD 기준정보를 체크하여 권한부여 시 업무분장 위배 여부를 즉각 파악 가능

Process Level 권한관리

- FI, MM, SD 등 코어모듈과 관련한 주요 비즈니스 권한을 보유한 사용자를 식별하고 해당 사용자가 보유한 Role을 List up 하여 부적절한 Role 보유 케이스를 교정할 수 있도록 기회제공
- 비즈니스 권한을 직무상 부적절하게 보유한 사용자가 처리한 트랜잭션 이력을 실시간으로 조회하여 비즈니스 사고 및 재무데이터 왜곡의 영향도를 즉각 파악 가능

Customization 관리

사용 중인 모듈상 회사의 커스터마이징된 프로세스(e.g.CBO)에 따라 업무 진행. 해당 프로세스에 대해서도 권한 또는 업무 분장 위배 여부 등에 대한 검토가 필요한 경우, 회사의 상황에 맞는 별도의 개발이 가능하며, SAP의 스탠다드 기능과 동일하게 모니터링 가능

매니지먼트 Navigator 제공

DIAS Navigator를 통해 ITGC 및 PLC 영역에 대한 단위 프로그램들을 ‘하나의 화면’에서 통합적으로 관리할 수 있습니다. 이를 통해 T-code, 테이블, SUIM 등 다양한 경로를 통해 파편적인 데이터를 취합 및 가공해야 했던 기존의 비효율적인 업무방식을 비약적으로 변화시킬 수 있으며 관리자는 빠르고 정확하게 수집된 데이터에 대하여 분석 및 조치를 취하는 ‘핵심 업무’에만 집중할 수 있습니다.

The screenshot shows the DIAS Navigator interface. At the top, there is a navigation bar with the SAP logo and the text 'DIAS Navigator'. Below this is a search bar and a dropdown menu with options like 'Background로 실행', 'Cancel', and 'More'. A welcome message reads: ': Welcome to DIAS(Deloitte ICFR Automation Solution)'. Below the welcome message is a menu bar with options: '계정 관리', '권한 관리', '로그 관리', '시스템 설정 관리', and '유지보수뷰'. The main area contains a table with the following columns: '프로그램 ...', '프로그램명', '프로그램 설명', '프로그램 실행', '리포트다운로드', and 'Background 실행'. The table lists various programs such as '테이블 유지보수뷰(SM30, SM31) 권한보유자 조회', '자산 프로세스 : 직무분리 위배 시물레이션', '매출 프로세스 : 직무분리 위배 시물레이션', '구매 프로세스 : 직무분리 위배 시물레이션', '경비 프로세스 : 직무분리 위배 시물레이션', '개발권한 보유자 조회', 'SAP_ALL 및 SAP_NEW 권한보유자 조회', 'Role & 사용자 유지보수 권한보유자 조회', and several activity-based programs like '[영업] 주요 비즈니스 Activity 권한보유자 조회'.

1 프로그램 분류 선택을 통해
통계영역별 프로그램들을 빠르게
List up 할 수 있습니다.

2 프로그램 실행버튼 클릭 한번으로
빠르게 해당 프로그램으로
이동합니다.

3 Background(배치작업)
실행을 통해 데이터를 저장하여
향후 로그데이터로 활용할 수
있습니다.

특장점 및 기대효과

DIAS 주요 장점

DIAS는 SAP의 CBO¹⁾로 PLC 영역의 다양한 비즈니스 관련 업무권한과 ITGC 영역의 시스템적 Role 관리가 동시에 효과적으로 통제될 수 있도록 PLC 권한관리 기능을 지원합니다.

Analyze 시스템상 발생 가능한 주요 리스크 분석

User Name	사용자명	사용자부서명	보유한 Profile	권한보유적정여부
HSYANG	양효식	인프라운영팀	SAP_ALL	●
MHJEONG	정민호	재무회계팀	SAP_ALL	●
MKKIM	김명관	IT운영팀	SAP_ALL	●
MYCHO	조민연	IT운영팀	SAP_ALL	●

User	사용자	사용자명	Role	Role 구분	권한오브젝트명	필드값
MKKIM	김명관	IT운영팀	ZCO_MT_ROLE	부여예정 Role	S_DEVELOP OBJTYPE	DEBUG
			ZFI_TAX_ROLE	부여예정 Role	S_DEVELOP ACTVT	03
				기본보유 Role	S_DEVELOP ACTVT	02
				기본보유 Role	S_DEVELOP OBJTYPE	DEBUG

직관적인 직무적정성 분석 | 권한 관리

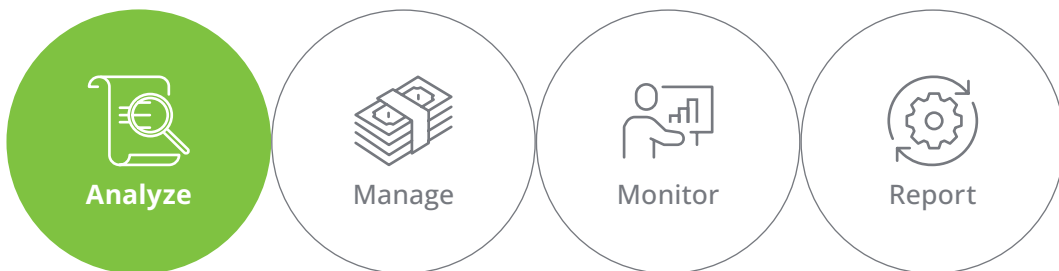
SAP 주요 권한 보유 현황과 사용자의 직무를 분석하여 발생 가능한 리스크를 직관적으로 확인

기준정보 활용을 통한 직무적정성 '자동' 확인을 통해 수작업 및 불필요한 커뮤니케이션으로 인한 업무 loss 감소

상충되는 권한의 사전 방지 | 권한 관리

SAP 주요 권한의 시뮬레이션을 통한 직무 상충 리스크 예측

Role 부여 전 사전 시뮬레이션 작업을 통해 권한이슈를 조기 식별하여 권한이슈 발생 후의 업무 loss 가능성 감소



1) Customer Bolt On (SAP Standard 프로그램이 아닌 ABAP 프로그래밍을 통해 자체적으로 개발한 단위프로그램)

Manage 시스템 주요 보안 설정 및 사용자 접근 관리

DIAS는 내부회계관리제도와 관련된 SAP의 각종 설정을 관리할 수 있는 기능을 제공하고 있으며 부적절한 설정값에 대한 적절한 관리 방향을 제시합니다.

패스워드 파라미터명	감사법인가준	회사정책	(호스트명)JUSSLTCSNW1	미비여부
login/failed_user_auto_unlock	0	1	1	▲
login/fails_to_user_lock	5	1	5	■
login/min_password_diff	1	1	2	■
login/min_password_digits	1	0	1	■
login/min_password_letters	1	1	0	●
login/min_password_lng	8	6	6	▲
login/min_password_specials	1	0	0	▲
login/password_expiration_time	90	80	0	●

Client 번호	Client 명	Changes and Transports for Client-Specific
821	CUA_TEST2	No changes allowed
290	DCAMSS	Changes without automatic recording
066	Early Watch	No changes allowed
501	ERS CA Golden Client	No changes allowed
199	ewewe	Automatic recording of Changes
100	Practitioner Client - SAP	Automatic recording of Changes
500	PS2 Client 250 Sandbox DT	Changes without automatic recording
000	SAP AG	No changes allowed

패스워드 파라미터 관리 | 설정 관리

SAP 패스워드 파라미터 값이 적절한 유효성을 가지고 있는지 실시간 조회를 통해 확인가능

회사만의 기준값 설정을 통해 산업표준 또는 감사 기준과 다른 운영(Operation) 관점의 자체적인 Value 세팅이 가능

보안 설정값 관리 | 설정 관리

SAP 주요 보안 설정 등 주요 이벤트를 기록하고 주요 이벤트에 대한 적절한 대응 방향을 제공

시스템 주요 설정값의 미비 여부에 대한 '자동' 식별을 통해 직관적으로 확인하고 미비사항에 대한 권고조치 가이드 제공



Monitor 시스템상 발생한 주요 활동의 쉽고 빠른 조회

DIAS를 통해 재무보고의 왜곡을 초래할 수 있는 위험을 가진 시스템 환경 설정 변경 및 사용자 액티비티에 대한 로그를 자동으로 수집하고 손쉽게 조회할 수 있습니다.

User ID	사용자명	사용자부서명	사용자타입변경일자	기준사용자	기준사용자타입
ATKUMAR	Atul Kumar		23.02.2022	S	Service User
CHERRY	cherry koul		07.03.2022	B	System User
INSK01			22.02.2022	A	Dialog User
			22.02.2022	S	Service User
			22.02.2022	B	System User
LCALCADA	Leonardo Calcada		18.02.2022	A	Dialog User
			18.02.2022	S	Service User
PVILAS	Pedro Macedo Vilas	ERS - IT AUDIT	03.02.2022	S	Service User
			03.02.2022	C	Communicatio

Debug 수행	User	사용자명	사용자부...	Message ID	Debug를 통한 데이터변경내역
29.05.2022	MKKIM	김명관	IT운영팀	A19	Field contents changed: CODE -
	MKKIM	김명관	IT운영팀	A14	> in program LSETBF01 , line 00
	MKKIM	김명관	IT운영팀	A19	Field contents changed: FIELD_
	MKKIM	김명관	IT운영팀	A14	> in program CL_DSH_DDIC_AS
	MKKIM	김명관	IT운영팀	A19	Field contents changed: R_CAC
	MKKIM	김명관	IT운영팀	A14	> in program CL_DSH_DDIC_AS
	MKKIM	김명관	IT운영팀	A19	Field contents changed: R_TIME
	MKKIM	김명관	IT운영팀	A14	> in program CL_DSH_DDIC_AS

설정 변경 이력 검토 | 로그 관리

사용자 타입 변경, 시스템 설정변경 등 트랜잭션과 시스템 운영에 영향을 미칠 수 있는 주요 이벤트에 대한 상세 로그와 권고 가이드 제공

사용자 타입 변경 등 자동 모니터링 결과를 통해 사용자가 취해야 하는 후속조치를 권고가이드로 제시

감사 로그의 자동 적재 | 로그 관리

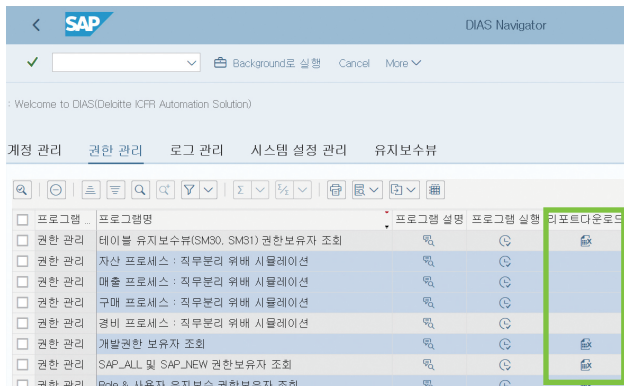
담당자가 놓치기 쉬운 변경 내역 등의 감사로그를 자동으로 수집하여 완전성 있는 데이터 제공

Debug를 통한 데이터 변경 등 주요 로그 정보를 별도의 CBO 테이블에 저장함으로써 향후 서버상의 로그정보 삭제 상황에 대비



Report 내부회계 활동에 대한 효율적인 문서화 지원

DIAS는 SAP에서 추출된 결과에 대한 셀프 분석 및 관리가 가능하도록 엑셀 형태의 보고서를 제공하여 내부회계관리제도의 효율적인 내재화를 지원합니다.



목적에 대한 테스트 목적				
프로그램	ASRCR0001			
Purpose	1: Role 생성 및 유지보수에 대하여 접근이 가능한 사용자 테스트 2: 사용자마다 리코드 생성/수정권한을 보유한 사용자 조회, 사용자 잠금/해제, 패스워드 변경 권한보유자 조회			
수행일자	1: 아래 권한을 보유한 사용자리스트를 추출한다. - Role 생성권한 - Role 수정권한 - 사용자리스트의 리코드 생성/수정권한 - 사용자 잠금/해제 - 패스워드 변경 권한보유자 조회 2: 관리자에게 의하여 대상 계정유에 대한 직무 및 역할을 고려한 후 권한보유의 적정성을 평가한다.			
결과에 대한 테스트 옵션				
A	권한이 가진 권한에 사용자리스트를 포함, 권한이 적절성 검증한다. 검토한다.			
B	역할 지정보유권 획득 및 직무기중에서 관리자 사용자보유 권한이 적절성 검증한다. 검토한다.			
C	권한계정의 일부 비즈니스 유효성 상, 통치권에 해당 계정을 제외한 권한이 부여하고 있고 테스트에 대한 출제가 이루어지고 있			
결과 결과기호				
P	비교사항 없음			
X	비교사항 불일치			
-	허용 사항 없음			
(M)	2차 사용자 또는 경우 기호			
권한구분	User ID	사용자명	사용자부서명	S_TIC
Role 생성권한	PULINI	PULINI AGARWAL		X
Role 생성권한		11907		X
Role 생성권한	31BHABAT	Bhabat Bhanu		X
Role 생성권한		442354	Uthav daga	X
Role 생성권한	SSBAP_T2	SSBAP_T2		X
Role 생성권한	SAUDIT	SAUDIT		X
Role 생성권한	SAUDIT	SAUDIT		X
Role 생성권한	BRICKERDELUN	Verdun		X

손쉬운 보고서의 생성 | Navigator

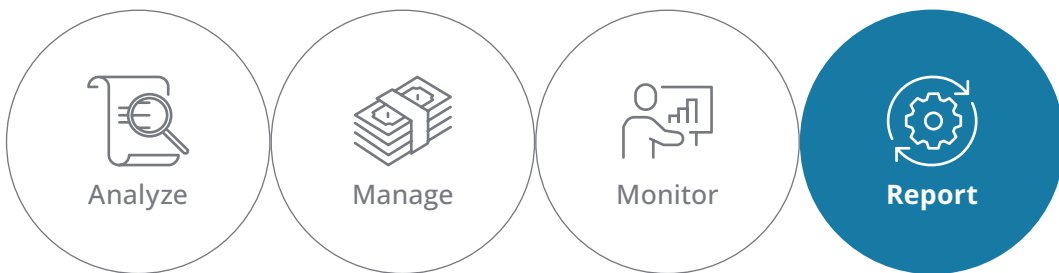
담당자는 Navigator상에서 추출한 통계 결과값을 즉시 보고서 양식으로 시각화하여 분석 가능

빠른 리포트 출력 기능을 통해 리포트 산출의 번거로움을 제거

반자동 내부회계 증빙

담당자는 반자동 보고서를 즉시 검토하여, 감사 법인별 요구사항에 빠르게 대처 가능

통제의 운영효과성 검토를 위한 표준 리포트 제공



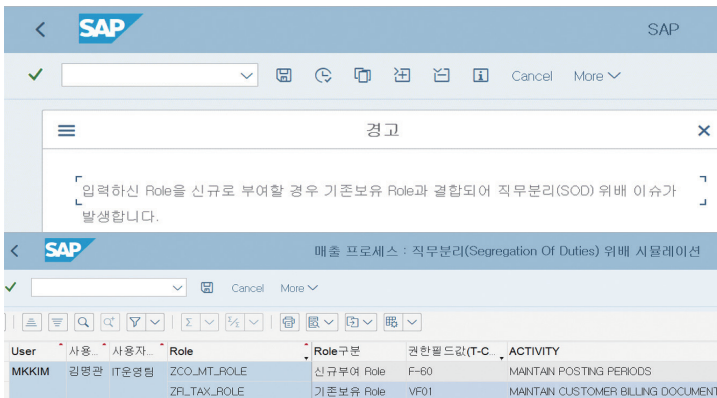
프로세스 레벨 권한관리

PLC 영역과 ITGC영역의 접점 관리

PLC 영역의 다양한 비즈니스 관련 업무권한과 ITGC 영역의 시스템적 Role 관리가 동시에 효과적으로 통제될 수 있도록 PLC 권한관리 기능을 지원합니다.

PLC 영역에 대한 SOD 관리

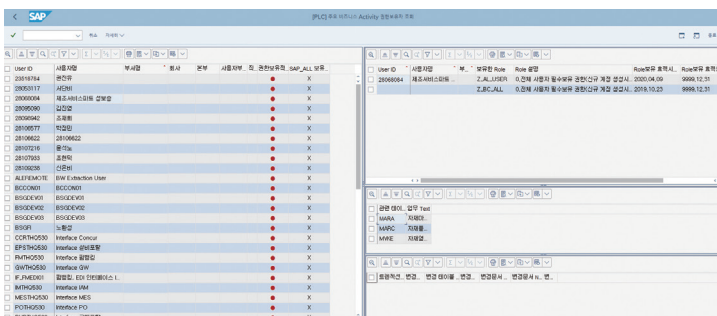
DIAS는 내부회계관리제도의 IT일반통제영역뿐만 아니라 PLC(Process Level Control) 영역의 주요 프로세스와 관련한 권한관리까지 수행할 수 있도록 구현되어 있습니다. 매출 등 주요 비즈니스 Role을 사용자에게 부여하기 전 시뮬레이션 작업을 통해 직무분리(SOD) 이슈를 예방합니다.



사용자에게 신규 권한(Role)을 부여하기 전 부여예정 Role과 기존 보유 Role을 조합하여 관련 Role을 동시에 보유할 경우 발생할 수 있는 직무분리(Segregation Of Duties) 위배 이슈를 사전에 체크
 예) 전기기간(Posting period)에 대한 유지보수 권한과 Customer에 대한 Billing document 처리권한을 동시에 보유할 경우 직무분리 위배임을 알람으로 표시

PLC 영역에 대한 권한검토 및 추적관리

재무회계(FI), 구매(MM), 영업(SD), 생산(PP) 등 SAP의 모듈에 대한 주요 비즈니스 Activity를 기준정보로 구현하고 관련 T-CODE를 매핑하여 직무상 부적절하게 권한을 보유하고 있는 사용자를 적시에 식별하고 사용자가 처리한 트랜잭션 로그를 동시에 확인하여 영향도를 평가할 수 있습니다.



PLC 영역의 주요 비즈니스 Activity에 대한 권한보유자를 추출하여 직무적정성을 자동으로 판단하고 적시에 권한검토 및 조치가 수행될 수 있도록 하며 부적절하게 권한을 보유한 유저가 처리한 트랜잭션 이력을 즉각적으로 확인 가능

2 in 1 서비스

솔루션과 컨설팅의 토탈 솔루션

DIAS는 SAP 내부통제 상의 문제점을 신속히 파악할 수 있도록 관련 정보를 제공하며, 관련 정보에 대한 효과적인 분석 및 활용을 위해 상세 분석 및 대응 방향에 대한 컨설팅을 토탈 솔루션을 제공합니다.



전문가 컨설팅

- 솔루션 도입 시 사전 진단 및 현황 분석을 통한 내부회계관리제도 대응 관점의 컨설팅 제공
- 솔루션 사용 및 효과적인 활용에 대한 내재화 측면의 전문가 컨설팅 제공

최적화 솔루션

- 회사 SAP 환경과 비즈니스 프로세스에 최적화된 솔루션 설정 및 적용
- SAP 내부회계관리제도 IT 관점의 다양한 분석 기능 및 엑셀기반의 보고서 제공

For More Information, Please Contact

조민연 파트너

Tel. 010-6361-2728

E-mail. minycho@deloitte.com

정민호 이사

Tel. 010-4783-9074

E-mail. minhjeong@deloitte.com

양효식 이사

Tel. 010-3909-3411

E-mail. hyoyang@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.