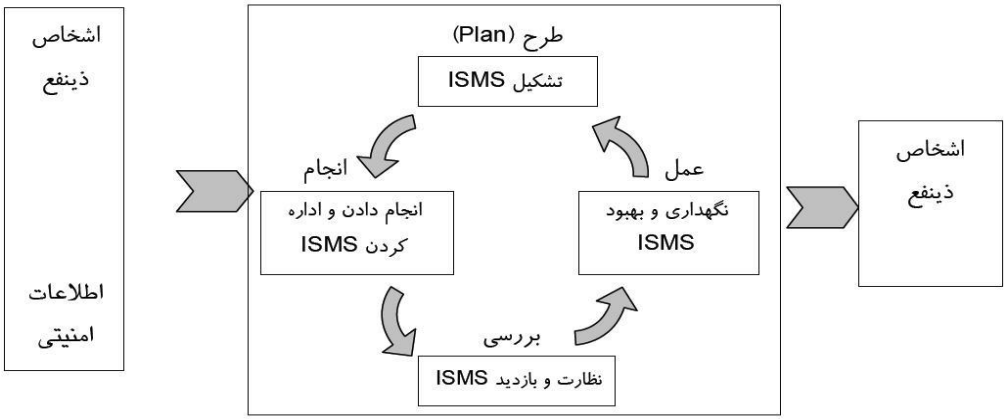
متخصص جوان صنعت نفت	**فرم ایده های خلاقانه**	**تاریخ: ۱۳۹۱/۵/۱۵** **شماره:** **صفحه ۱ از ۳**

عنوان ایده	**تشکیل کارگروه تخصصی امنیت فناوری اطلاعات به منظور استقرار و اداره سیستم مدیریت امنیت اطلاعات ISMS**			
مخاطب ایده	**مخاطب اصلی در وزارت نفت**	وزیر محترم نفت		
	مخاطبان دیگر	مدیران بلند پایه شرکت ملی نفت ایران و شرکت نفت فلات قاره		
پیشنهاد دهنده	**نام و نام خانوادگی**	اشکان جعفری شورباخورلو	**سمت سازمانی**	طرح نظام، نفت فلات قاره، منطقه سیری
			پست الکترونیک	Ajafari35@gmail.com
بیان مسئله و چالش	با توجه به نقش اطلاعات به عنوان کالای با ارزش در تجارت امروز، لزوم حفاظت از آن ضروری به نظر می رسد. برای دستیابی به این هدف هر شرکت بسته به سطح اطلاعات (از نظر ارزش اقتصادی یا امنیتی آن) نیازمند به طراحی سیستم مدیریت امنیت اطلاعات است تا از این طریق بتواند از سرمایه های اطلاعاتی خود حفاظت نماید. بالطبع، شرکتهای دولتی نیز نه تنها از این قاعده مستثنی نیستند، بلکه بیش از سایر شرکتها، نیازمند توجه به مقوله امنیت اطلاعات هستند. در شرکت نفت، اهمیت حفاظت از منابع اطلاعاتی بیش از بنگاههای اقتصادی می باشد. در این شرکت، اطلاعاتی وجود دارد که از جنبه های سیاسی و استراتژیک، دارای اهمیت فوق العاده و بعضاً حیاتی هستند و از اینرو، انتشار یا سوء استفاده از چنین اطلاعاتی، نه تنها از نظر اقتصادی زیان بار خواهد بود، بلکه تبعات منفی سیاسی، اجتماعی و نظامی بسیار وسیعی برای کل کشور بهمراه خواهد داشت. با گسترش شبکه های کامپیوتری و مجهز شدن شرکتها به اینگونه شبکه ها، محافظت مناسب از امنیت اطلاعات موجود در شبکه ها بسیار مهم می باشد. برای این منظور لازم است هر شرکت بر اساس یک متدولوژی مشخص، ضمن تهیه طرح ها و برنامه های امنیتی مورد نیاز ، تشکیلات لازم جهت ایجاد و تداوم امنیت اطلاعات خود را نیز ایجاد نماید.			
شرح پیشنهاد بهبود	یکی از مهم ترین استاندارد های موجود، استاندارد مدیریتی ISO/IEC 17799 می باشد. این استاندارد در حال حاضر بصورت فراگیر در سرتاسر جهان مورد استفاده قرار می گیرد و بسیاری از شرکتهای معتبر تلاش می کنند که ضمن پیاده سازی این استاندارد، از مراکز صدور گواهی تأییدیه مبتنی بر اجرای موفقیت آمیز آنرا نیز کسب نمایند.			

مطابق این استاندارد، امنیت یک فرآیند یکباره نیست، بلکه یک فرآیند مداوم است که بایستی دائماً تکرار گردد.

چرخه امن سازی یا استقرار سیستم مدیریت امنیت اطلاعات ISMS، شامل چهار مرحله Plan-Do-Check-Act (PDCA) بوده و بر اساس استانداردهای مطرح این حوزه مطابق شکل زیر است:



شکل ۱: مدل PDCA بکار گرفته شده مطابق فرآیندهای ISMS

خروجی فاز اول استقرار سیستم مدیریت امنیت اطلاعات یعنی فاز طراحی (Plan)، طرح جامع امنیت اطلاعات می باشد.

این طرح پس از تهیه بررسی و تحلیل شده و به تأیید بخشهای مختلف در صنعت خواهد رسید. سپس در فاز دوم استقرار سیستم مدیریت امنیت اطلاعات یعنی فاز اجرا Do طرح، آماده شده اجرا خواهد گردید. لازم به ذکر است برای تکمیل این چرخه و استمرار آن لازم است پس از اتمام فاز دوم، کلیه موارد و راهکارهایی از طرح جامع امنیت اطلاعات که مربوط به فازهای بررسی Check و عمل Act می باشد، کاملاً و با دقت توسط شرکت بکار گرفته شده و استمرار داشته باشند.

طرح جامع امنیت شبکه:

طرح جامع امنیت شبکه به عنوان مهمترین بخش طرح جامع امنیت اطلاعات و مبتنی بر مدل دفاع از عمق یا دفاع چند لایه می باشد. در این مدل، اقدامات امنیتی در پنج لایه مختلف ارائه می

گردد. این لایه ها از این قرارند:

۱. امنیت پیرامونی شبکه

۲. امنیت داخلی شبکه

۳. امنیت میزبانها

۴. امنیت برنامه های کاربردی

۵. امنیت داده ها

نهایتاً راهکارهای امنیتی بمنظور امن سازی هر لایه شبکه با توجه به مدل امنیت چند لایه، در سه بخش **تجهیزات و ابزارهای امنیتی مورد نیاز، تنظیمات و پیکربندیهای امنیتی و روالها و رویه های امنیتی**، بایستی ارائه شود.