

# ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

۱۶ شهریور ۱۳۹۹





# ارائه نیازهای فناورانه

۱ - شرکت کاشف

## چشم انداز

کاشف در افق ۱۴۰۱ شرکتی است مورد اعتماد، کارآمد و دانش محور با نقشی سازنده، ارزش افزا و اطمینان بخش در ارتقای امنیت و تابآوری زیست بوم تولید و تبادل اطلاعات بانکی

## مأموریت

پایش موثر، جهت دهی و ارزشیابی هوشمند امنیت فضای تولید و تبادل اطلاعات بانکی با اتکا به نیروی انسانی متخصص و متعهد، فناوری های نوین، پژوهش و نوآوری

## اهداف کلان

**پیشگیری** ارتقای توانمندی نظام بانکی در پیشگیری از رخدادهای امنیت اطلاعات  
**نظارت و ارزیابی** افزایش توان نظارتی شرکت کاشف و نظارت پذیری در نظام بانکی  
**شناسایی و پاسخگویی** ارتقای قابلیت شناسایی و پاسخگویی هماهنگ به تهدیدها و رخدادهای امنیت اطلاعات  
**فرهنگ سازی** رشد آگاهی عمومی و اعتلای شایستگی های تخصصی در حوزه امنیت اطلاعات بانکی  
**تعالی سازمانی** توسعه قابلیت های سازمانی

## راهبردهای اصلی - استراتژی ها

- جلب مشارکت، برقراری تعاملات هدفمند و به اشتراک گذاری اطلاعات با ذی نفعان نظام بانکی
- تمرکز بر رویکرد مدیریت مخاطرات امنیت اطلاعات بانکی
- تمرکز بر شناسایی حوادث و تهدیدها و ایجاد هماهنگی و همکاری عملیاتی در رسیدگی به آنها
- نهادینه سازی امنیت به عنوان مزیت رقابتی در نظام بانکی
- توانمندسازی نیروهای انسانی فعال در نظام بانکی
- فرهنگ سازی عمومی در به کارگیری امن خدمات بانکی
- برون سپاری خدمات و مشارکت با شرکتهای دانش بنیان و مراکز علمی و پژوهشی
- توسعه خدمات در جهت رشد و تنوع منابع

# برنامه راهبردی شرکت مدیریت امن الکترونیکی کاشف

در افق میان مدت ۱۳۹۹ الی ۱۴۰۱

# فهرست

## □ تدوین الزامات

- الزامات و راهنمای امن سازی واسط‌های نرم افزاری بانکی
- الزامات و راهنمای توسعه امن سامانه‌های اطلاعاتی
- الزامات و راهنمای مدیریت رویداد و رویداد نگاشت
- مقررات ناظر بر راهکارهای مبتنی بر زنجیره بلوک در نظام بانکی
- مقررات ناظر بر به اشتراک گذاری اطلاعات تهدیدات سایبری و تقلب های بانکی
- تنظیم مقررات ناظر بر به اشتراک گذاری اطلاعات تهدیدات سایبری و تقلب های بانکی

# فهرست

## پژوهش

- طراحی و تدوین چارچوب مدیریت مقابله با تقلب‌های بانکی
- تجزیه و تحلیل سریع و دقیق محیط انتشار پیام
- شناسایی مشتریان از راه دور
- نظام تولید، تبادل، ذخیره سازی و استفاده امن از گواهینامه های دیجیتال در ابزارهای همراه

# فهرست

## □ سامانه‌های اطلاعاتی

- سامانه تشخیص هوشمند ابزارهای خودکار
- سامانه شناسایی هوشمند حملات فیشینگ
- سامانه اشتراک‌گذاری و تحلیل اطلاعات امنیتی
- سامانه شناسایی هوشمند افشای اطلاعات حساس بانکی و رسیدگی به آن‌ها
- سامانه شناسایی هوشمند سوءاستفاده از ابزارهای بانکی و پرداخت در کسب و کارهای غیرمجاز/مجرمانه و مقابله با آن‌ها
- سامانه مدیریت حقوق اطلاعات



تنظیم الزامات و راهنمای امن سازی واسط‌های نرم  
افزاری بانکی



# شرح نیاز فناورانه

API مخفف Application Programming Interface رابط‌هایی نرم‌افزاری هستند که ارتباط بین نرم‌افزارهای مختلف یا بخش‌های مختلف از یک نرم‌افزار را پیاده‌سازی می‌کنند. نیاز اصلی در این بخش تدوین الزامات امنیتی مرتبط با واسط‌های نرم‌افزاری بانکی است.

- بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر
- بررسی به‌روش‌ها و استانداردها
- بررسی نیازمندی‌های داخلی
- تدوین الزامات امن‌سازی واسط‌های نرم‌افزاری
- تنظیم مقررات ناظر بر فعالیت بازیگران
- تدوین راهنمای اجرای الزامات



# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

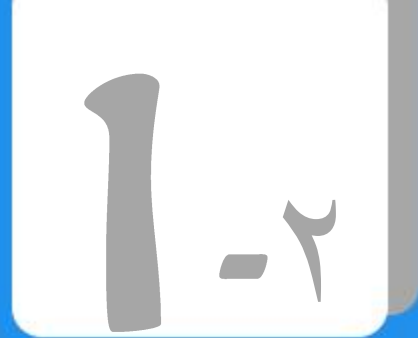
فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- بررسی استانداردها/ به‌روش‌ها
- بررسی تجارب تنظیم‌گری
- تنظیم فرهنگ‌واژگان
- تدوین الزامات و گزارشات
- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما



تنظیم الزامات و راهنمای توسعه امن سامانه‌های  
اطلاعاتی



# شرح نیاز فناورانه

الزامات امنیتی مورد نیاز برای توسعه امن نرم افزارها در تمامی مراحل چرخه عمر توسعه نرم افزار شامل تحلیل نیازمندی ها، طراحی، توسعه و آزمون، پیاده سازی، مستند سازی و ارزشیابی نرم افزار

- بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر

- بررسی به روشها و استانداردها

- بررسی نیازمندیهای داخلی

- تدوین الزامات توسعه امن نرم افزارهای بانکی

- تنظیم مقررات ناظر بر بازیگران

- تدوین راهنمای اجرای الزامات

# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

بررسی استانداردها/ به‌روش‌ها

- بررسی تجارب تنظیم‌گری

- تنظیم فرهنگ‌واژگان

- تدوین الزامات و گزارشات

- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما





تنظیم الزامات و راهنمای مدیریت رویداد و رویداد  
نگاشت



# شرح نیاز فناورانه

الزامات امنیتی مورد نیاز برای مدیریت رویدادها و رویدادنگاشت ها  
(Event & Log Management)

- بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر

- بررسی به روشها و استانداردها

- بررسی نیازمندیهای داخلی

- تدوین الزامات مدیریت رویداد و رویداد نگاشت ها

- تنظیم مقررات ناظر بر بازیگران

- تدوین راهنمای اجرای الزامات

# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

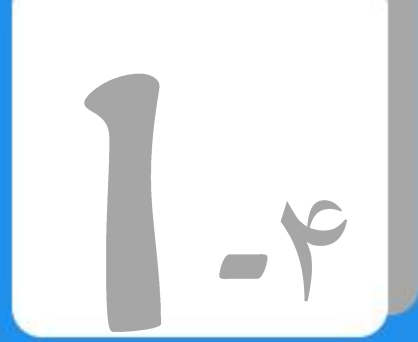
فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- بررسی استانداردها/ به‌روش‌ها
- بررسی تجارب تنظیم‌گری
- تنظیم فرهنگ‌واژگان
- تدوین الزامات و گزارشات
- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما



تنظیم مقررات ناظر بر راهکارهای  
مبتنی بر زنجیره بلوک در نظام بانکی



# شرح نیاز فناورانه

تنظیم مقررات ناظر بر راهکارهای مبتنی بر زنجیره بلوک مورد استفاده در  
نظام بانکی

بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر

بررسی به روشها و استانداردها

بررسی نیازمندیهای داخلی

تنظیم مقررات ناظر بر زنجیره بلوک

تدوین راهنمای پیاده سازی مقررات

# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت



# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- بررسی استانداردها/ به‌روش‌ها
- بررسی تجارب تنظیم‌گری
- تنظیم فرهنگ‌واژگان
- تدوین الزامات و گزارشات
- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما

۱-۵

تنظیم مقررات ناظر بر به اشتراک گذاری  
اطلاعات تهدیدات سایبری و نقل های بانکی

# شرح نیاز فناورانه

بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر

بررسی به روشها و استانداردها

بررسی نیازمندیهای داخلی

تدوین مقررات ناظر بر اشتراک گذاری تهدیدات سایبری و ثقلب های بانکی

تنظیم مقررات ناظر بر بازیگران

# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

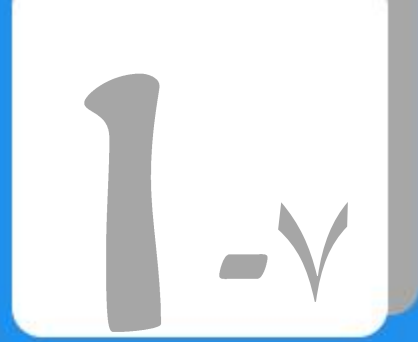
فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- بررسی استانداردها/ به‌روش‌ها
- بررسی تجارب تنظیم‌گری
- تنظیم فرهنگ‌واژگان
- تدوین الزامات و گزارشات
- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما  
راه‌حل‌ها و پیشنهادات



# طراحی و تدوین چارچوب مدیریت مقابله با تقلب‌های بانکی





# شرح نیاز فناورانه

بررسی تجارب سایر کشورها در حوزه تنظیم مقررات ناظر

بررسی به روشها و استانداردها

بررسی نیازمندیهای داخلی

تدوین چارچوب مدیریت مقابله با تقلب های بانکی

تنظیم مقررات ناظر بر بازیگران

تدوین راهنمای پیاده سازی این چارچوب در بانکها

# حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات

# حوزه صنعتی تقاضا

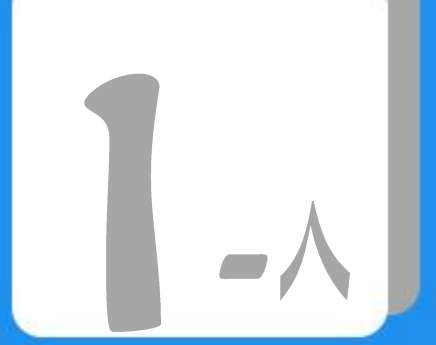
فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- - بررسی استانداردها/ به‌روش‌ها
- بررسی تجارب تنظیم‌گری
- تنظیم فرهنگ‌واژگان
- تدوین الزامات و گزارشات
- انتقال اطلاعات و دانش

# مدل همکاری مطلوب

تدوین تعاملی اسناد با دریافت بازخورد از کارفرما



تجزیه و تحلیل سریع و دقیق محیط انتشار پیام



# شرح نیاز فناورانه

یکی از فعالیت‌های محوری و مأموریتی روابط عمومی تولید و انتشار پیام‌ها با محتوای اطلاع‌رسانی و فرهنگ‌ساز است و برای دقت در این کار و کاهش هزینه، نیاز دارد که اولاً جامعه مخاطب پیام‌ها از ابعاد مختلف (سن، تحصیلات، سلیق، رسانه‌های مورد استفاده و...) شناسایی، طبقه‌بندی و تجزیه و تحلیل شود و دیگر اینکه بتواند بعد از انتشار پیام، با کمترین هزینه، بازخورد سریع و دقیقی از این پیام‌های منتشر شده در جامعه مخاطب دریافت کند.

چه در ایران و چه در دیگر کشورها این کار عمدتاً از طریق پرسشنامه‌ها و نظرسنجی‌ها و فعالیت‌های پیمایشی صورت می‌گیرد.

شرکت کاشف تاکنون در این زمینه فعالیت و اقدام خاصی نکرده است.

در صورت ارائه راهکار فناورانه‌ای برای تأمین این هدف، بررسی کارشناسی از سوی شرکت برای تأیید کفایت خواهد کرد.

# حوزه فناوری تقاضا

روابط عمومی

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت-تبلیغات

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

مطلوب آن است که روابط عمومی بتواند پیش از تولید محتوا برای اطلاع‌رسانی و فرهنگ‌سازی در گستره ملی یا منطقه‌ای سطح دانش امنیتی جامعه مخاطب و نحوه و مسیر دریافت اطلاعات توسط افراد این جامعه و سطح سواد و دانش عمومی آن‌ها را دریابد و به تبع این شناخت دقیق بتواند محتوایی کارساز و متناسب را تولید کرده و این محتواها را از طریق مجاری و رسانه‌های مناسب‌تر به بهترین وجهی به جمعیت هدف انتقال دهد.



# مدل همکاری مطلوب

به نظر می‌رسد، نحوه همکاری مطلوب، پس از ارائه راهکار فناورانه و بررسی شیوه استفاده، توانمندی‌ها و دیگر ابعاد و ویژگی‌های آن قابل ارزیابی و پیشنهاد خواهد بود.

۱-۹

طراحی، توسعه و راه‌اندازی سامانه  
اشتراک‌گذاری و تحلیل اطلاعات امنیتی

## شرح نیاز فناورانه

سامانه‌ای که توسعه آن مورد نظر است مشتمل بر چندین زیرسامانه بوده و مولفه فناوری مرکز اشتراک‌گذاری اطلاعات و هوشمندی تهدیدات بخش بانکی کشور است. از جمله مهم‌ترین مسئولیت‌های این سامانه می‌توان به اشتراک‌گذاری اطلاعات آسیب‌پذیری‌ها، تهدیدات، حملات و رخدادها به همراه به‌روش‌ها یا دانش مواجهه و پاسخ عملیاتی بین ذی‌نفعان و همچنین دریافت و تحلیل بلادرنگ آگاهی‌وضعیتی (وضعیت عملیاتی تهدیدات، رخدادها و مخاطرات) ذی‌نفعان، کمک به بروزرسانی آن و تعیین و بروزرسانی وضعیت لحظه‌ای آگاهی وضعیت بخش بانکی اشاره نمود. از سوی دیگر این سامانه می‌تواند نقش مهمی در مشارکت در تحلیل و برآورد لحظه‌ای تهدیدات و وضعیت مخاطرات و آگاهی وضعیت سایبری فرابخشی و ملی داشته باشد.

از نمونه‌های خارجی می‌توان به ابزارهایی همچون MISP، Soltra Edge، CRITs و ... اشاره نمود. همچنین لازم بذکر است شرکت کاشف پیش‌تر تلاشی جهت رفع این نیاز نداشته است.

## حوزه فناوری تقاضا

ارتقاء امنیت و تاب‌آوری در سطح نظام بانکی کشور

## حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

- سامانه باید یک کریدور اطلاعاتی حلقه بسته باشد. به عبارتی، اطلاعات از کلیه ذی‌نفعان مشارکت‌کننده و البته منابع هوشمندی سایبری بیرونی، دریافت می‌شود اما تنها در میان ذی‌نفعان مشارکت‌کننده و تعیین‌شده توزیع می‌شود.
- سامانه بهتر است مبتنی بر استاندارد NIST 800-150 با عنوان Guide to Cyber Threat Information Sharing باشد.
- سامانه نباید بدون هماهنگی و اجازه ذی‌نفعان و بدون رعایت الزامات حریم خصوصی کسب و کار آن‌ها عمل کرده و استفاده درست از گمنام‌سازی، اطلاعات اختصاصی و تحت مالکیت ذی‌نفعان را شامل شود.
- سامانه باید دریافت، نرمال‌سازی، جمع‌آوری و یکپارچه‌سازی اطلاعات دریافتی از منابع ذی‌نفعان مختلف و منابع خارجی هوشمندی را با علم به اینکه تفاوت سکوی منابع داده و قالب‌های آن‌ها مورد انتظار است؛ انجام دهد.
- سامانه باید توانمندی پذیرش مؤثر خوراک داده از چندین منبع بدون خطا یا خرابی در شرایط بار اضافی و اشباع ظرفیت را داشته باشد.

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

- سامانه باید تحلیل‌ها، ادغام /همبسته‌سنجی‌ها، دسته‌بندی‌ها و غنی‌سازی نشانگرهای تهدید را با استفاده از آخرین فناوری‌های موجود انجام دهد. ادغام /همبسته‌سازی خودکار باعث می‌شود تا ارتباطات میان خصیصه‌ها و شاخص‌های حملات برقرار شود.
- سامانه باید قابلیت ارسال هشدار و گزارش برای ذی‌نفعان براساس هشدارها یا متغیرهای از پیش تعریف شده را داشته باشد.
- بخش بصری سامانه باید وضعیت سایبری بخش بانکی کشور را به‌صورت شفاف، لحظه‌ای و با ماشین زمان قابل تنظیم مشاهده‌پذیر نموده و امکان اخذ گزارشات روند وضعیت سایبری را برای ذی‌نفعان لایه سیاست‌گذاری و تنظیم مقررات بخشی و ملی فراهم کند.

# مدل همکاری مطلوب

محصول با انتقال دانش و فناوری همراه است.



# شناسایی مشتریان از راه دور e-KYC





## شرح نیاز فناورانه

شناسایی مشتریان (KYC) در نظام بانکی فعالیتی است که در آن نحوه شناسایی مشتری، تعیین سطوح خدمات بانکی متناسب با مشتری و مخاطرات رابطه تجاری با آن را مشخص می‌سازد. با ظهور خدمات مبتنی بر فناوری اطلاعات، این فعالیت نیز می‌تواند در قالب خدمتی الکترونیکی از طرف برخی از شرکت های فناورانه یا توسط خود بانک ها و مؤسسات اعتباری ارائه گردد. این خدمت به صورت از راه دور و مبتنی بر اسناد دیجیتال است که هزینه و بروکراسی اداری فرآیند شناسایی مشتریان را کاهش می‌دهد.

# حوزه فناوری تقاضا

امنیت اطلاعات بانکی

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

- امکان دریافت، ثبت، نگهداری، بروزرسانی و تبادل امن اطلاعات مرتبط با شناسایی مشتریان
- امکان اعتبارسنجی اطلاعات شناسایی مشتریان با مراجع ذی صلاحی همچون سازمان ثبت احوال، سازمان ثبت اسناد و املاک کشور، سازمان امور مالیاتی و ...
- بروزرسانی مستمر اعتبارسنجی‌ها از سازمان‌ها و مراجع ذی صلاح
- استفاده از فناوری‌های مبتنی بر زنجیره بلوک برای به اشتراک گذاری اطلاعات مرتبط با شناسایی مشتریان
- استفاده از فناوری‌های مبتنی بر هوش مصنوعی برای تشخیص تقلب در مدارک شناسایی دریافت شده

# مدل همکاری مطلوب

محصول با انتقال دانش و فناوری همراه است.



سامانه تشخیص هوشمند ابزارهای خودکار



# شرح نیاز فناورانه

با عنایت به حساسیت سامانه ها و خدمات بانکی و پرداخت، یکی از اقدامات پیشگیرانه مهم جهت جلوگیری از سوء استفاده ابزارهای خودکار، فراهم سازی سازوکار شناسایی چنین ابزارهایی با روشهایی نظیر «کپچای تعاملی»، «سامانه های هوشمند تشخیص رفتار کاربر» و ... می باشد. ایجاد زیرساخت بومی ارائه این خدمات به سازمان های داخلی از نیازهای احصاء شده در کشور می باشد.

# حوزه فناوری تقاضا

حوزه مطالعات و تنظیم مقررات

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

مستقل از زیرساخت‌های غیر ایرانی  
سازگاری با انواع فناوری‌های سمت کاربر نهایی  
نرخ قابل قبول خطای مثبت کاذب و منفی کاذب  
مقاوم در برابر روش‌های مختلف دور زدن همچون خودکارسازی مرورگر



# مدل همکاری مطلوب

قابلیت استقرار به هر دو صورت «SaaS» و «یا در محل مشتری»  
محصول با انتقال تکنولوژی همراه است.



سامانه شناسایی هوشمند سایت‌های فیشینگ



# شرح نیاز فناورانه

با عنایت به خدمات حساس ارائه شده بر روی درگاه‌های اینترنتی بانک‌ها و مؤسسات اعتباری، یکی از روش‌های رایج میان کلاهبرداران و سارقان اینترنتی، فیشینگ درگاه‌ها مانند اینترنت بانک‌های مؤسسات اعتباری می‌باشد. در این روش سارقان با استفاده از تبلیغات جستجوگرهای شناخته شده؛ نظیر گوگل و با ایجاد تارنماهای مشابه صفحات اصلی بانک، اقدام به ترغیب کاربران به ارائه اطلاعات حساس خود می‌نمایند. در این نیاز انتظار می‌رود با فراهم سازی امکان تعریف دامنه های مجاز بانکی و کلیدواژه‌های مرتبط، تارنماهای تقلبی را تشخیص و به سامانه های مسدود سازی بانک مرکزی جهت مسدودسازی ارسال نمایند.

# حوزه فناوری تقاضا

حوزه مطالعات و تنظیم مقررات

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

خزش گسترده صفحات وب

جستجوی انبوه در جستجوگرهای شناخته شده

امکان تعریف دامنه های مجاز

امکان تعریف کلیدواژه

# مدل همکاری مطلوب

محصول با انتقال تکنولوژی همراه است



سامانه شناسایی هوشمند سوءاستفاده از ابزارهای  
بانکی و پرداخت در کسب و کارهای  
غیرمجاز/مجرمانه و مقابله با آن ها



# شرح نیاز فناورانه

در حال حاضر برخی از گردانندگان کسب و کارهای غیرمجاز یا مجرمانه برای تبادلات مالی خود از ابزارهای بانکی و پرداخت استفاده می کنند از جمله استفاده از اطلاعات کارت بانکی یا حساب های کاربری ابزارهایی مانند اینترنت بانک، بسترهای مبتنی بر پیام رسان ها و ...

با عنایت به این موضوع شناسایی و گردآوری ادله متناسب برای برخورد قانونی با این نوع از سوءاستفاده ها در فضای مجازی نیاز به سازوکارهایی خودکار/نیمه خودکار با حداقل دخالت انسانی دارد. لذا نیاز است سامانه هایی توسعه پیدا کنند که در فضای مجازی در وهله نخست امکان شناسایی چنین کسب و کارهایی (از جمله سایت های قمار و شرط بندی یا فروش اقلام غیرمجاز) را داشته باشند و در گام های آتی قابلیت گردآوری ادله لازم را دارا باشند.



## حوزه فناوری تقاضا

حوزه رسیدگی به رخدادهای امنیت فضای تولید و  
تبادل اطلاعات بانکی

## حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

خزش گسترده صفحات وب

خزش گسترده در شبکه‌های اجتماعی

خزش گسترده در پیام‌رسان‌های رایج

جستجوی انبوه در جستجوگرهای شناخته شده

امکان تعریف مبادی رصد از جمله دامنه‌ها، حساب‌های کاربری در پیام‌رسان‌ها، صفحات ثبت شده در شبکه‌های اجتماعی و ...

امکان تعریف کلیدواژه

امکان تعریف پارامترهای لازم برای شناسایی کسب و کارهای غیرمجاز/مجرمانه

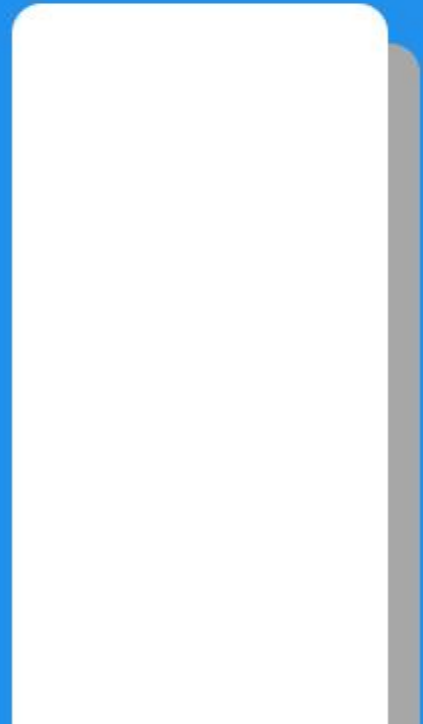
امکان ارائه گزارش‌های استاندارد به منظور تعامل با سایر سامانه‌های رسیدگی به رخداد

# مدل همکاری مطلوب

محصول با انتقال تکنولوژی همراه است



سامانه شناسایی هوشمند افشای اطلاعات حساس  
بانکی و رسیدگی به آن ها



# شرح نیاز فناورانه

یکی از مخاطرات همیشگی سازمان های مالی و اعتباری افشای اطلاعات حساس مرتبط با کاربران این سازمان هاست و سالانه ضرر های قابل توجهی از این موضوع متوجه آن هاست. جلوگیری از افشای اطلاعات حساس یکی از وظایف حیاتی این دسته از سامان ها محسوب می شود اما تجربه نشان داده است که علاوه بر جلوگیری از افشای اطلاعات حساس بایستی سازمان ها تدابیر لازم برای مواجهه با این نوع از رخدادهای امنیتی را داشته باشند و اولین گام برای مقابله با چنین رخدادهایی شناسایی سریع آن هاست.

اطلاعات حساس بانکی و پرداخت عمدتاً شامل اطلاعات ابزارها و اعتبارنامه های صادر شده برای مشتریان بانکی به منظور احراز هویت است.

## حوزه فناوری تقاضا

حوزه رسیدگی به رخدادهای امنیت فضای تولید و  
تبادل اطلاعات بانکی

## حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

خزش گسترده صفحات وب

خزش گسترده در وب تاریک

خزش گسترده در شبکه‌های اجتماعی

خزش گسترده در پیام‌رسان‌های رایج

جستجوی انبوه در جستجوگرهای شناخته شده

امکان تعریف مبادی رصد از جمله دامنه‌ها، حساب‌های کاربری در پیام‌رسان‌ها، صفحات ثبت شده در شبکه‌های اجتماعی و ...

امکان تعریف کلیدواژه

امکان ارائه گزارش‌های استاندارد به منظور تعامل با سایر سامانه‌های رسیدگی

به‌خدا

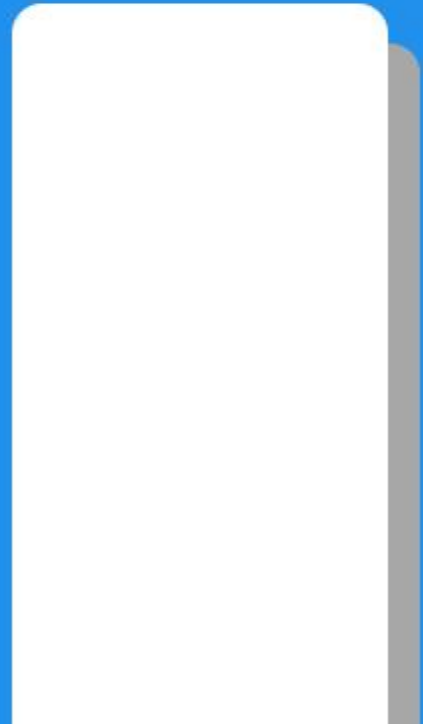
# مدل همکاری مطلوب

محصول امکان استفاده به صورت آزمایشی دارد  
محصول با انتقال تکنولوژی همراه است





سامانه شناسایی هوشمند ابزارهای بانکی و  
پرداخت جعلی و مقابله با آن ها



# شرح نیاز فناورانه

جعل ابزارهای بانکی و پرداخت به طور معمول برای گردآوری اطلاعات حساس یا سوءاستفاده از ابزارهای اصیل به کار می رود مصداق این موضوع می تواند ایجاد یک کپی (رونوشت) از ابزارهای ضعیف در برابر رونوشت شدن (برای مثال کپی کردن کارت های بانکی مغناطیسی)، دستکاری و انتشار برنامه های بانکی و پرداخت، مبادی ارتباطی با مشتریان (ایمیل، پیامک و ...) یا دستگاه های پوز جعلی باشد اما محدود به این موارد نیست.

شناسایی این موارد می تواند کمک به سزایی در مقابله با آن ها داشته باشد و ضررهای ناشی از آن ها را به حداقل برساند.

## حوزه فناوری تقاضا

حوزه رسیدگی به رخدادهای امنیت فضای تولید و  
تبادل اطلاعات بانکی

## حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

تعیین پارامترهای موردنیاز برای سنجش اصالت ابزارهای بانکی و پرداخت

پایش فضای مجازی برای شناسایی ابزارهای بانکی و پرداخت جعلی

امکان دریافت گزارش شناسایی ابزارهای جعلی

امکان اعتبار سنجی گزارش‌های دریافتی

امکان تعامل با شرکت‌های مخابراتی و اپراتورهای تلفن همراه برای شناسایی مبادی جعلی

ارسال پیامک‌های بانکی و پرداخت

امکان ارائه گزارش‌های استاندارد به منظور تعامل با سایر سامانه‌های رسیدگی به رخدادهای

# مدل همکاری مطلوب

محصول با انتقال تکنولوژی همراه است



# RegTech در حوزه امنیت اطلاعات بانکی



## شرح نیاز فناورانه

توسعه و نگهداری مجموعه قوانین، الزامات، دستورالعمل ها و رویه های اجرایی در حوزه امنیت فناوری اطلاعات بانکی نیاز به سازوکارهایی دقیق و قابل اتکا دارد تا ذی نفعان این حوزه بتوانند انتظارات تنظیم کننده مقررات را به خوبی درک کرده و اقدامات لازم برای تطابق با آن ها را به انجام رسانند و نتایج اقدامات را در فرمت های قابل به اشتراک گذاری در اختیار تنظیم کننده مقررات (بانک مرکزی ج.ا.ا) قرار دهند.

با توجه به گستردگی موضوعات مرتبط با مقررات تدوین و ابلاغ شده و تعدد نسخ آن ها لازم است سامانه ای اطلاعاتی، تولید، ثبت و نگهداری آن ها را به انجام رساند. همچنین این امکان فراهم باشد که نهادهای مکلف در قبال مقررات، میزان انطباق سازمان خود را با مقررات موضوعه، سنجیده و گزارش های موردنیاز تنظیم کننده مقررات را تهیه و ارسال نمایند.

## حوزه فناوری تقاضا

تنظیم مقررات امنیت اطلاعات، نظارت و ارزیابی امنیت اطلاعات

## حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت



# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

- امکان تعریف فرآیند توسعه مقررات
- امکان جلب مشارکت ذی نفعان در فرآیند توسعه مقررات
- نگهداری نسخ مختلف مقررات
- امکان تشخیص تضاد و تعارض میان مقررات مختلف
- امکان ارائه گزارش انطباق سنجی

# مدل همکاری مطلوب

محصول با انتقال دانش و فناوری همراه است.



نظام تولید، تبادل، ذخیره سازی و استفاده امن از  
گواهینامه های دیجیتال در ابزارهای همراه



## شرح نیاز فناورانه

استفاده از ابزارهای همراه توسط مشتریان در صنعت بانکداری الکترونیک رو به ازدیاد است و بسیاری از خدمات بانکداری و پرداخت الکترونیک بر مبنای ابزارهای همراه (مانند تلفن همراه، تبلت و ...) توسعه یافته اند. تبادل اطلاعات حساس میان خدمت دهندگان بانکی و چنین ابزارهایی نیازمند حصول اطمینان از اصالت ابزار همراه، حفظ محرمانگی داده های حساس ذخیره شده در ابزار همراه و تبادل امن اطلاعات است.

یکی از راه حل های رایج مسئله پیشگفته، ایجاد نظامی برای تولید، تبادل، ذخیره سازی و استفاده از گواهینامه های دیجیتال است.

# حوزه فناوری تقاضا

امنیت اطلاعات بانکی

# حوزه صنعتی تقاضا

فناوری اطلاعات-بانکی و پرداخت

# پارامترهای عملکردی لازم (الزامات) راه‌حل‌های پیشنهادی

- ایجاد محیط امن تولید، تبادل و نگهداری امن از کلیدهای مورد استفاده
- تعیین سازوکارهای استفاده از گواهینامه‌های صادر شده برای ذی نفعان
- تضمین عملکرد در مقیاس‌های متناسب با عملیات بانکی و پرداخت
- ایجاد ساختاری مقیاس پذیر برای پاسخگویی به نیازهای جدید

# مدل همکاری مطلوب

محصول با انتقال دانش و فناوری همراه است.



سامانه مدیریت حقوق اطلاعات  
RMS-IRM (Information Right  
Management Service)





# شرح نیاز فناورانه

یکی از دغدغه های هر سازمانی امنیت اطلاعات دارای طبقه بندی می باشد. طبیعتا اطلاعاتی ومستنداتی که در سطح هیات مدیره شرکت تولید می گردد می بایست از دید کارشناسان بخش های دیگر سازمان مخفی بماند. از سوی دیگر نگهداری این اطلاعات در سیستم های شخصی هم باعث عدم استفاده از امکانات شبکه ها می شود و هم امکان پشتیبان گیری از اطلاعات وجود نخواهد داشت. در دنیا سامانه های جهت Information Right Management وجود دارد که این امکان را فراهم می نمایند.

وجود سامانه ای بومی با این قابلیت ها و یکپارچه شدن با سیستم عامل های مختلف و نرم افزارهای آفیس بسیار مهم است.

# حوزه فناوری تقاضا

واحد فناوری اطلاعات - امنیت شبکه

# حوزه صنعتی تقاضا

فناوری اطلاعات

# پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

پشتیبانی از اکوسیستم میکروسافت

پشتیبانی از اکوسیستم ادوبی

# مدل همکاری مطلوب

محصول امکان تست داشته باشد.  
محصول دارای پشتیبانی قوی باشد و راه حلی سلسله مراتبی  
برای ریکاوری باشد.

# اطلاعات تماس

[info@kashef.ir](mailto:info@kashef.ir)

۰۲۱-۷۲۸۶۱۲۰۰