

# Rancangan Respon Fraud (Fraud Response Plan): Analisis Kasus Tesco

Ditulis oleh  
**Vauline Frilly**

# Daftar isi

I. Mengapa *Fraud Response Plan* Penting

---

II. *Fraud Response Plan*

---

III. Catatan Akhir

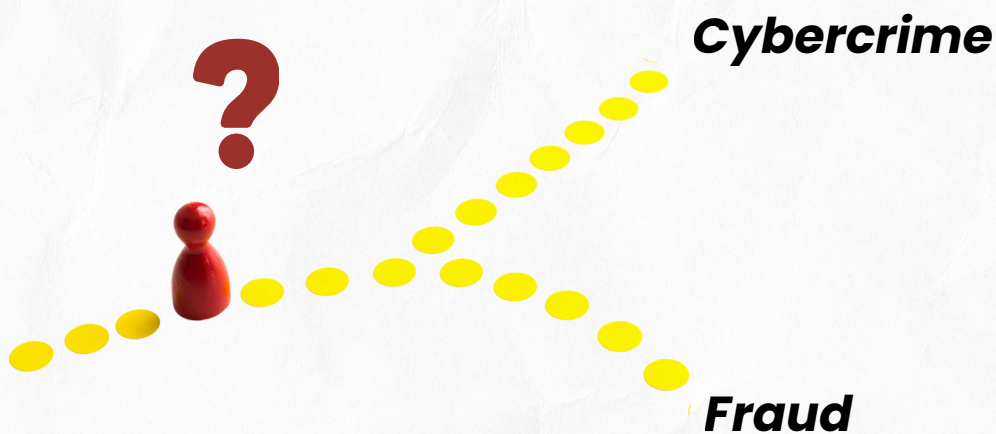
---



# Mengapa Fraud Response Plan Penting

"*Fraud*" mungkin sebuah kata yang terdengar kurang lazim bagi banyak orang, namun kata "*kejahatan siber*" atau "*cybercrime*", terdengar lebih sering digaungkan terutama di era digital saat ini. Lebih banyak orang yang familiar dengan *cybercrime* karena korbannya banyak ditargetkan kepada individu, berbeda dengan *fraud* yang lebih menasar pada perusahaan. Karenanya, persepsi atas urgensi penanganan *cybercrime* lebih terbentuk dan tersosialisasi dibandingkan dengan pentingnya merespon *fraud*.

Namun apakah tepat jika seorang pimpinan perusahaan dihadapkan untuk memilih prioritas antara *cybercrime* dengan *fraud*, selalu lebih baik mengedepankan *cybercrime* dan menaruh *fraud* di daftar paling belakang? Untuk menjawab pertanyaan ini, beberapa faktor di bawah merupakan poin kunci yang harus menjadi pertimbangan sebelum mengambil keputusan.



Salah satu faktor esensial dalam menentukan prioritas pengambilan keputusan adalah nilai kerugian finansial yang ditimbulkan oleh terjadinya insiden baik *fraud* maupun *cybercrime*.



Association of Certified Fraud Examiners (ACFE) dalam surveinya menyebutkan total rata - rata kerugian perusahaan akibat *fraud* bernilai US\$ 1,7 juta (Rp 28,25 miliar) tiap kasusnya,[i] *Federal Bureau of Investigation* (FBI) merilis laporan atas kejahatan internet (*cybercrime*) yang terjadi di Amerika dan menyebutkan nilai kerugian rata - rata tiap kasus adalah US\$ 19.372 (Rp 322 juta).[ii]

Nilai kerugian tersebut diperoleh berdasarkan analisis laporan kasus yang diterima, yang mana ACFE menerima 1.921 laporan kasus dengan tidak ada satupun kasus yang tidak mengakibatkan kerugian finansial,[iii] sedangkan FBI menerima 859.532 laporan kasus namun hanya 256.256 kasus yang memiliki kerugian finansial.[iv]



Selanjutnya, kasus *fraud* laporan keuangan, membutuhkan skema yang lebih kompleks dan terorganisir, namun tiap kasusnya menimbulkan kerugian paling besar bahkan dapat melumpuhkan perusahaan.[v] Sedangkan *cybercrime* yang paling tinggi nilai kerugiannya adalah penipuan investasi dengan korban individu, yaitu memanipulasi seseorang sehingga membeli suatu produk investasi dengan informasi yang salah.[vi]

Dari ketiga faktor tersebut, dapat disimpulkan bahwa seyogyanya sebuah perusahaan telah memiliki strategi penanganan *fraud* terlebih dahulu, baru kemudian mengembangkannya ke ranah *cybercrime*. Namun ironisnya, lebih mudah untuk menemukan pedoman metodologi respon insiden *cybercrime* (*cyber incident response*) yang terperinci dibandingkan pedoman metodologi respon *fraud* yang komprehensif.



### Fraud Response Plan

*Fraud response plan* seharusnya dibuat secara komprehensif mengingat krusialnya penanganan yang tepat sejak dini untuk mencegah kerugian yang lebih besar baik dari sisi finansial, operasional, reputasi, dan kontinuitas usaha; serta tidak berisiko pada hilangnya bukti *fraud* yang dapat digunakan di persidangan perdata maupun pidana.

Mengingat *fraud response plan* tidak hanya digunakan untuk mengidentifikasi kronologi peristiwa *fraud* namun juga skala pelaku yang terlibat dalam skema contohnya apakah melibatkan manajemen atas (*top management*); menilai skala dampak yang ditimbulkan seperti kerugian finansial, kerusakan citra perusahaan, timbulnya biaya konsultan hukum dan investigator eksternal; dan pertimbangan strategi *asset recovery* yang efisien dan efektif.





Dalam beberapa pedoman, *fraud response plan* tidak berdiri sendiri melainkan menjadi salah satu bagian dari rancangan yang lebih besar yaitu rancangan anti *fraud*. Beberapa negara seperti Inggris, Saudi Arabia, dan Indonesia, telah mewajibkan institusi perbankan di negaranya memiliki dan menerapkan strategi anti *fraud* (di dalamnya termasuk *fraud response plan*).

Contohnya POJK Nomor 39 /POJK.03/2019 telah mewajibkan bank umum untuk memiliki dan menerapkan strategi anti *fraud* (pasal 3), dengan deteksi dan investigasi termasuk 2 (dua) pilar utama yang harus dimuat di dalamnya (pasal 4). Namun bagi industri lain, tingkat terperinci metodologi respon *fraud* berbeda - beda di tiap institusi.

Karenanya, publikasi ini bertujuan untuk menyajikan poin - poin penting yang dapat dijadikan sebagai referensi awal bagi perusahaan dalam mengembangkan *fraud response plan*.

*Fraud response plan* yang disusun dalam publikasi ini dibuat dengan mengadopsi *Cybersecurity Framework* versi 2 (CSF v2) tahapan *Incident Response* yang dirilis oleh *National Institute of Standards and Technology* (NIST) Departemen Perdagangan Amerika[vii] dan Lampiran I - Pedoman Penerapan Strategi Anti *Fraud* bagi Bank yang dikeluarkan oleh Otoritas Jasa Keuangan dalam POJK Nomor 39 /POJK.03/2019.

Untuk memberikan gambaran aktual dari konsep *fraud response plan*, publikasi ini menggunakan contoh kasus *fraud* di Tesco.

# Fraud Response Plan

Merujuk kepada tahapan *Incident Response* dalam *Cybersecurity Framework* versi 2, terdapat 3 (tiga) bagian yang harus dilakukan yaitu Deteksi (*Detect*), Respon (*Respond*), dan Pemulihan (*Recover*). Ketiga aspek ini akan dijelaskan menggunakan analisis penulis terhadap tindakan respon *fraud* yang dilakukan oleh manajemen Tesco pada saat menghadapi skandal *fraud* di tahun 2014.

## II.1 Kasus *Fraud* Tesco



Tesco, perusahaan ritel terbesar di Inggris, melakukan *overstatement* (penggelembungan) terhadap nilai profitnya di tahun 2014.[viii] *Tesco Stores Limited*, salah satu anak perusahaan Tesco, membukukan *overstatement* nilai profit sebesar £326 juta (Rp 7,19 triliun)[ix] antara Februari dan September 2014.[x]

Akibat tindakan ini, Tesco harus membayar mahal tidak hanya denda, namun juga kerugian investor akibat salah saji laporan keuangan, biaya investigasi, dan biaya hukum lainnya. Meski demikian, Tesco dapat mempertahankan posisinya bahkan profitnya (*operating profit*) meningkat drastis dari £372 juta[xi] di 2015 (pasca insiden) menjadi £1,6 miliar di 2024.[xii]



## II.2 Fraud Response Plan: Detect



Bagian Detect mencakup tindakan identifikasi indikasi ketidakwajaran dalam suatu proses bisnis, transaksi, catatan keuangan, atau aspek lainnya dan menganalisisnya untuk menemukan potensi *fraud*.

### II.2.1 Detect dalam Kasus Tesco

Pada kasus Tesco, indikasi *fraud* ditemukan dan diberitahukan oleh direktur keuangan bernama Amit Soni, kepada penasihat umum (*general counsel*) Tesco, yang selanjutnya diteruskan kepada CEO baru Tesco, Dave Lewis.[xiii]

Amit Soni selaku *whistleblower*, membuat laporan rahasia yang menyatakan bahwa telah dilakukan manipulasi profit dengan metode “*pulling forward*” yaitu membukukan pendapatan masa depan di periode akuntansi yang tidak seharusnya (lebih cepat).[xiv] Pada 22 September 2014, Tesco mengumumkan telah melakukan *overstatement* profit sekitar £250 juta.[xv]



### II.2.2 Detect dalam Pedoman *Fraud Response Plan*

Merujuk Lampiran I – Pedoman Penerapan Strategi Anti *Fraud* bagi Bank POJK Nomor 39 /POJK.03/201, mekanisme *Detect* dapat dilakukan dengan 3 (tiga) metode yaitu *whistleblowing* (pengaduan), *surprised audit* (pemeriksaan dadakan), dan *surveillance* (sistem pengawasan).

Agar *Detect* melalui *whistleblowing* efektif, perusahaan perlu menerapkan sistem yang dipercaya dapat melindungi *whistleblower* (pengadu), jalur yang aman dan efektif, dan kejelasan tindak lanjut atas aduan yang diberikan.

Surprised audit biasanya dilakukan dadakan pada proses bisnis yang berisiko tinggi, namun untuk meningkatkan kewaspadaan seluruh karyawan, dapat juga diterapkan pada proses bisnis yang berisiko lebih rendah meskipun dilakukan dengan frekuensi yang lebih rendah.

#### Mekanisme detect

POJK Nomor 39  
/POJK.03/201

**Whistleblowing**  
(pengaduan)

**Surprised audit**  
(pemeriksaan dadakan)

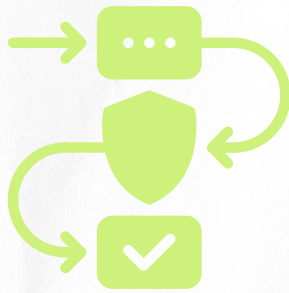
**Surveillance**  
(sistem pengawasan)

Surveillance dilakukan dengan diam – diam atau rahasia dan dapat melibatkan pihak ketiga untuk independensi.

Selain dari yang disebutkan, CSF v2 NIST juga memasukkan mekanisme pengawasan berkelanjutan yang dapat dilakukan dengan memasukkan pembelajaran dari kasus terdahulu.[xvi] Perlu dibuat log berisi informasi penting dari kasus fraud yang pernah terjadi, yang dapat membantu perusahaan untuk dapat mendeteksi *fraud* lebih cepat.



## II.3 *Fraud Response Plan: Respond*



Bagian *Respond* mencakup tindakan dan pilihan opsi yang dapat dilakukan sebagai tindak lanjut ketika ditemukannya potensi fraud dengan tujuan meminimalisir risiko kerugian yang diderita, preservasi (mengamankan) potensi bukti yang dapat digunakan di pengadilan, dan mencegah dampak yang lebih besar.

### II.3.1 *Respond* dalam Kasus Tesco

Setelah memperoleh *whistleblowing* atas dugaan manipulasi profit di hari Jumat siang, Tesco segera melakukan tindak lanjut dengan meneliti kembali unit bisnis yang diduga mengandung *fraud* di akhir pekan. Setelah dipastikan adanya potensi pelanggaran, Tesco menghentikan sementara kepala di unit bisnis Inggris dan segera memulai investigasi yang dilakukan oleh akuntan independen serta bekerjasama dengan konsultan hukum.[xvii]

Hasil investigasi mengungkap bahwa nilai *overstatement* profit akhir yang ditemukan, lebih tinggi dari dugaan awal yaitu senilai £263 juta, yang terdiri dari £118 juta berkaitan dengan profit *trading* periode awal (*first half trading*), £70 juta berkaitan dengan profit 2013/14, dan £75 juta berkaitan dengan profit di periode sebelumnya.[xviii] Tidak diketahui dengan pasti penyebabnya, namun nilai *overstatement* tersebut direvisi lagi menjadi £326 juta.[xix]

### II.3.2 Respond dalam Pedoman *Fraud Response Plan*

Lampiran I – Pedoman Penerapan Strategi Anti *Fraud* bagi Bank POJK Nomor 39 /POJK.03/201 mengatur bahwa tindakan *Respond* terhadap dugaan *fraud* adalah melakukan Investigasi. Poin penting dalam pelaksanaan Investigasi adalah menentukan pihak pelaksana dan mekanisme pelaksanaan, yang mana ditentukan berdasarkan pertimbangan:

- Independensi; dan
- Kompetensi yang mencakup keahlian dalam Analisis dan Investigasi, Forensik Akuntansi, Forensik Komputer, Pekerjaan Lapangan dan Wawancara.

CSF v2 NIST juga menekankan beberapa poin penting yang masuk dalam tahapan *Respond*: [xx]

- Tinjauan awal (*preliminary review*) untuk memverifikasi dugaan insiden (*fraud*).
- Investigasi, pengumpulan data, dan pendokumentasian dari seluruh hal yang terjadi dalam insiden dan tindakan yang dilakukan.
- Koordinasi dengan pihak - pihak terkait dan yang terkena dampak seperti pelanggan, penegak hukum, dan institusi terkait lainnya.
- Manajemen insiden yaitu dengan mengawasi perkembangan penanganan masing - masing insiden dan menentukan prioritas pengalokasian sumber daya.
- Evaluasi seluruh risiko yang timbul dari insiden.
- Penentuan prioritas yang tepat dalam setiap pengambilan keputusan.



## »» II.4 Fraud Response Plan: Recover



Bagian *Recover* mencakup tindakan restorasi terhadap aset dan operasional yang terkena dampak dari *fraud*. Aset dan operasional yang dimaksud dapat mencakup aspek finansial, organisasi, proses bisnis, citra perusahaan, dan kepercayaan pemangku kepentingan (*stakeholder*).

### II.4.1 Recover dalam Kasus Tesco

Atas kasus *fraud* yang terjadi, tuntutan pidana terhadap Tesco dibatalkan namun Tesco harus membayar penalti sebesar £128.992.500 dan biaya senilai £3.069.951 kepada *Serious Fraud Office* Inggris melalui mekanisme *Deferred Prosecution Agreement*.<sup>[xxi]</sup>

Tesco juga membayar ganti rugi senilai £85 juta kepada investor yang membeli saham atau bond antara 29 Agustus dan 19 September 2014.<sup>[xxii]</sup> Selain itu, 3 (tiga) direktur senior Tesco didakwa melakukan manipulasi akuntansi dan fraud dengan penyalahgunaan jabatan.<sup>[xxiii]</sup>

#### II.4.2 Recover dalam Pedoman *Fraud Response Plan*

Lampiran I - Pedoman Penerapan Strategi Anti *Fraud* bagi Bank POJK Nomor 39 /POJK.03/201 mengatur harus adanya tindak lanjut hasil investigasi berupa pengenaan sanksi yang setidaknya mencakup jenis sanksi sesuai tingkat *fraud* atau pelanggaran, mekanisme pengenaan sanksi, dan pengawas pelaksanaan pengenaan sanksi. Selain itu, juga penting adanya sistem pemantauan berkelanjutan yang mencakup proses evaluasi, perbaikan kelemahan, dan penguatan sistem pengendalian *fraud*.

CSF v2 NIST menyebutkan poin penting yang masuk dalam tahapan Recover adalah restorasi sistem sehingga berjalan normal dan perbaikan kerentanan untuk mencegah insiden serupa. Sistem yang dimaksud dapat mencakup aktivitas operasional, akuntansi, rantai pasokan (*supply chain*), citra perusahaan, hubungan dengan stakeholder, dan risiko hukum.[xxiv]



# Catatan Akhir

[i] ACFE, "Occupational Fraud 2024: A Report to The Nations." hlm. 4. Kurs BI tanggal 16 Mei 2025, US\$ 1 = Rp 16.617. Bank Indonesia, "Kurs Transaksi BI." <https://www.bi.go.id/id/statistik/informasi-kurs/transaksi-i/default.aspx>.

[ii] FBI, "Internet Crime Report 2024: Internet Crime Complaint Center." hlm. 4. Kurs BI tanggal 16 Mei 2025, US\$ 1 = Rp 16.617. Bank Indonesia, "Kurs Transaksi BI." <https://www.bi.go.id/id/statistik/informasi-kurs/transaksi-bi/default.aspx>.

[iii] ACFE, "Occupational Fraud 2024: A Report to The Nations." hlm. 4.

[iv] FBI, "Internet Crime Report 2024: Internet Crime Complaint Center." hlm. 4.

[v] ACFE, "Occupational Fraud 2024: A Report to The Nations." hlm. 4.

[vi] FBI, "Internet Crime Report 2024: Internet Crime Complaint Center." hlm. 10 dan 42.

[vii] NIST US Department of Commerce, "NIST Special Publication 800: NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management." hlm. 5. <https://doi.org/10.6028/NIST.SP.800-61r3>, diakses pada 19 Mei 2025

[viii] Financial Times, "Cost of Tesco Accounting Scandal Goes Beyond Fines." <https://www.ft.com/content/f50ca092-13ab-11e7-80f4-13e067d5072c>, diakses pada 19 Mei 2025.

[ix] Kurs BI tanggal 16 Mei 2025, £ 1 = Rp 22.052. Bank Indonesia, "Kurs Transaksi BI." <https://www.bi.go.id/id/statistik/informasi-kurs/transaksi-bi/default.aspx>.

[x] The Guardian, "Tesco to Pay £129m Fine Over Accounting Scandal." <https://www.theguardian.com/business/2017/mar/28/tesco-agrees-fine-serious-fraud-office-accounting-scandal>, diakses pada 19 Mei 2025.

BBC, "Tesco Fined £129m for Overstating Profits." <https://www.bbc.com/news/business-39415681>, diakses pada 19 Mei 2025.

[xi] Tesco, "Interim Results 2016/17." hlm. 2. <https://www.tesco plc.com/media/eyicwjfb/interim-statement-2016-17.pdf>, diakses pada 19 Mei 2025.

[xii] Tesco, "Interim Results 2024/25." hlm. 4. <https://www.tesco plc.com/media/qjeufm/tesco-plc-interim-results-2425-press-release.pdf>, diakses pada 19 Mei 2025.

[xiii] The Guardian, "Tesco Suspends Senior Staff and Starts Investigation Into Overstated Profits." <https://www.theguardian.com/business/2014/sep/22/tesco-investigators-overstating-profit-250m>, diakses pada 19 Mei 2025.

[xiv] Daily Mail, "Tesco Executives 'Inflated Profits by £250Million Because of Pressure from Budget Chains Aldi and Lidl'." <https://www.dailymail.co.uk/news/article-4951284/Tesco-bosses-inflated-profits-Lidl-pressure.html>, diakses pada 19 Mei 2025.

[xv] Daily Mail, "Tesco Executives 'Inflated Profits by £250Million Because of Pressure from Budget Chains Aldi and Lidl'." <https://www.dailymail.co.uk/news/article-4951284/Tesco-bosses-inflated-profits-Lidl-pressure.html>, diakses pada 19 Mei 2025.

[xvi] NIST US Department of Commerce, "NIST Special Publication 800: NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management." hlm. 23 dan 26. <https://doi.org/10.6028/NIST.SP.800-61r3>, diakses pada 19 Mei 2025.

[xvii] The Guardian, "Tesco Suspends Senior Staff and Starts Investigation Into Overstated Profits." <https://www.theguardian.com/business/2014/sep/22/tesco-investigators-overstating-profit-250m>, diakses pada 19 Mei 2025.

[xviii] Business & Accountancy Daily, "Deloitte Puts Tesco Accounting 'Black Hole' at £263m." <https://www.accountancydaily.co/deloitte-puts-tesco-accounting-%E2%80%99black-hole%E2%80%99-%C2%A3263m>, diakses pada 19 Mei 2025.

[xix] BBC, "Tesco Fined £129m for Overstating Profits." <https://www.bbc.com/news/business-39415681>, diakses pada 19 Mei 2025.

[xx] NIST US Department of Commerce, "NIST Special Publication 800: NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management." hlm. 27-33. <https://doi.org/10.6028/NIST.SP.800-61r3>, diakses pada 19 Mei 2025.

[xxi] Government U.K., "Notice of Discontinuance Tesco Stores Limited." [https://assets.publishing.service.gov.uk/media/67c0659ca0f0c95a498d207b/Notice\\_of\\_DPA\\_discontinuance\\_7.04.20.pdf](https://assets.publishing.service.gov.uk/media/67c0659ca0f0c95a498d207b/Notice_of_DPA_discontinuance_7.04.20.pdf), diakses pada 19 Mei 2025.

[xxii] The Guardian, "Tesco to Pay £129m Fine Over Accounting Scandal." <https://www.theguardian.com/business/2017/mar/28/tesco-agrees-fine-serious-fraud-office-accounting-scandal>, diakses pada 19 Mei 2025.

[xxiii] The Guardian, "Former Tesco Directors Charged with Fraud Over Accounting Scandal." <https://www.theguardian.com/business/2016/sep/09/sfo-charges-former-tesco-directors-with-fraud>, diakses pada 19 Mei 2025.

[xxiv] NIST US Department of Commerce, "NIST Special Publication 800: NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management." hlm. 33. <https://doi.org/10.6028/NIST.SP.800-61r3>, diakses pada 19 Mei 2025.